Encyclopedia of Security Management

Second Edition

J. Fay

B/H

Encyclopedia of Security Management

Second Edition

Encyclopedia of Security Management

Second Edition

Edited by

John J. Fay

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Butterworth-Heinemann is an imprint of Elsevier

Aquisitions Editor: Pamela Chester
Signing Editor: Jennifer Soucy
Assistant Editor: Kelly Weaver
Project Manager: Melinda Ritchie

Butterworth–Heinemann is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
Linacre House, Jordan Hill, Oxford OX2 8DP, UK

Library of Congress Cataloging-in-Publication Data
Application submitted

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN: 978-0-12-370860-1

For information on all Butterworth–Heinemann publications
visit our Web site at www.books.elsevier.com

Printed in the United States of America

07 08 09 10 11 12 10 9 8 7 6 5 4 3 2 1

Table of Contents

Contributing Authors

Sean A. Ahrens, CPP. Senior Security Consultant with Schirmer Engineering and has more than 16 years of security experience. Mr. Ahrens has provided security threat and risk analysis, contingency planning, loss prevention, force protection planning, and design and construction administration services for government, public, and private entities that encompass the areas of telecommunications, security, closed circuit television, and access control systems. He is well-versed in the various trade and local authority issues impacting projects, and has specialized professional competence in security, access control systems, and force protection systems. Known for his technical expertise, he has been asked to sit on a variety of standard-setting panels including Underwriters Laboratories (UL) and the Security Industry Association (SIA). Mr. Ahrens is a former and founding member of the American Society for Industrial Security International (ASIS) Commission on Guidelines, where he assisted in the development and promulgation of a variety of security-related guidelines. Mr. Ahrens currently participates as an active member of the ASIS Commercial Real Estate Council (CREC) and a committee to develop Physical Security Measures Guidelines.

Jill Allison, CISSP, MBA, MIM. Enterprise Security Risk Management Consultant; CEO, Allison Consulting and Fireworks Security Ventures, Chaska, MN; former Vice President, 4Ai International LLC, Chicago, IL; former Consultant, National Biometric Security Project (NBSP) Washington, D.C.; former Smart Card Solutions Product Manager, Datacard Group, Minnetonka, MN; former Graduate Program Manager, St. Thomas University, MBA Program, Minneapolis, MN; former Vice President, Business Development, Security Design International (Cylink subsidiary, merged with Counterpane,) Santa Clara, CA; former Vice President, Marketing & Business Development, CertifiedTime, Inc.; former PKI Consultant, Science Applications International Corp. (SAIC), Annapolis, MD; former Consultant, Intellitactics, Annapolis, MD; former Vice President, Business Development, Voltaire Advanced Data Security, Inc., Vienna, VA; former Vice President, Business Development, War Room Research, LLC, Annapolis, MD; former Director, Strategic Partnering and Solutions Marketing; Pinkerton's Inc., Encino, CA; former Director, Business Development, IriScan, Inc. (Iridian), Mt. Laurel, NJ; former Consultant, Monsanto Company, St. Louis, MO; former Business Planning Graduate Intern, Apple Computer, Cupertino, CA; former Product Marketing Manager; Hypro Corporation; former Security Program Analyst; Vitro Security Engineering, Mt. Laurel, NJ. Member, American Society for Industrial Security (ASIS) and former Conference Chair, ASIS IT Security Council; Bachelor of Arts, Economics, Gustavus Adolphus College, St. Peter, MN; Master of International Management, Marketing, American Graduate School of International Management (AGSIM/Thunderbird) Glendale, AZ; Master of Business Administration, Strategic and Entrepreneurial Management, the Wharton School, University of Pennsylvania, Philadelphia, PA.

Randall I. Atlas, PhD, AIA, CPP. President of Counter Terror Design, Inc. and Vice President of Atlas Safety & Security Design, Inc., Miami, FL; Adjunct Associate Professor of Architecture, Florida Atlantic University; Technical Assistance Consultant for the National Institute of Corrections, Longmont, CO. Member, American Institute of Architects—Architecture for Justice Committee; member, American Society of Industrial Security—Security Architecture Engineering Committee; member, American Correctional Association—Design & Technology Committee; member, American Society of Safety Engineers; member, National Safety Council; member, Environmental Design Research Association; member, National Fire Protection Association; member, American Society of Testing Materials; member, Human Factors Ergonomics Society; member, American Jail Association; member, National Institute of Justice—Leadership Position; member, Security by Design—Leadership Position; member, Advisory Task Group—Leadership Position. Doctorate of Criminology, Florida State University; Master of Architecture, University of Illinois; Bachelor of Criminal Justice, University of South Florida; Bachelor of Architecture, University of Florida. Author of "Crime Prevention Through Building Codes," *Building Security*, 1981; "Crime Site Selections for Assaults in Four Florida Prisons,"

Prison Journal, 1986; "Stairs, Steps, and Slipping," *Florida Architect Journal*, 1987; "Crime Prevention Through Building Codes," *Journal of Security Administration*, 1986; "Secure Homes: The Future of Anti-Crime Technology," *Futurist*, 1988; "Designing Security for People, Information, and Property," *Florida Real Estate Journal*, 1988; "How to Protect Your Home," 1988; "Just When You Thought It Was Safe," *Professional Safety*, 1989; "Building Design Can Provide Defensible Space," *Access Control*, 1989; "Design for Safety: Building Code Update," *Florida Architect Journal*, 1989; "Security Design," a monthly featured article in *Protection of Assets Bulletin*; "Pay It Now or Pay It Later," *Security Management*, 1990; "Architect Input Among First Steps in Design," *Access Control*, 1991; "Offensible Space: Obstruction of Law Enforcement Through Environmental Design," *Security Management*, 1991; "Handicap Accessibility Affects Security," *Access Control*, 1992; "Will ADA Affect Security?" *Security Management*, 1992; "Need for Involving Security in Building Planning," *Campus Security Report*, 1992; "Security for Buildings," *Architectural Graphic Standards*, Wiley Publishers, 1992; "Post-Occupancy Evaluation of Building Security," *Post-Occupancy Evaluations*, 1993; "Impact of ADA on Corrections," *Construction Bulletin*, National Institute of Corrections, 1993; "Environmental Barriers to Crime," Ergonomics in Design, October 1994; "The Impact on Crime of Street Closures and Barricades: A Florida Case Study." Security Journal; Vol. 5, No. 3, July 1994; Special Report: Defensible Space, Engineering New Record, May 1, 1995; "Designing for Security in Courthouses of the Future," Court Review Vol. 34, No. 2, Summer 1997; American Judges Association; "Designing Security in School Environments," Library Administration and Management Spring, Vol. 11, #2, 1997; "Designing for Crime and Terrorism: CPTED Training is Essential: Security Design and Technology magazine, June 1998; "Designing Against Crime: the Case for CPTED Training for Architects," Florida Architect, Summer 1998; "Stairwell Security," Door and Hardware Magazine, May 1999, p. 55; "Secure Facility Design, Environmental Design that Prevents Crime!" The Construction Specifier, *April* 1999; "Security Design: Access Control Technology," Door and Hardware magazine, *April* 1999, p. 49; "ADA: Proposed Final Regulations for Courthouses, Jails and Prisons," Corrections Today, *April* 2000; "Design Considerations: Setting Standards in Security Architecture," Door and Hardware magazine, June 2000; "Building Security Through Design," The American Institute of Architects, Washington, D.C., 2001; "Barry University: A CPTED Case Study," *Campus Law Enforcement Journal*, June 2002; "The Sustainability of CPTED: Less Magic More Science!" *The CPTED Journal*, Vol. 1, Issue 1, July 2002; "Planting and Shaping Security Success," Security Management magazine, August 2002; "The ABC's of CPTED," a Florida case study of Barry University, *Campus Safety Journal*, August 2002; "Creating Safety," Landscape Architect magazine, September 2002; "Designing Safe Campuses," *Campus Security and Safety Journal*, December 2002; "Loss Prevention Returns to Its Roots with CPTED," Plant Safety & Maintenance magazine, *April* 2003; "How Are Criminals Using CPTED? Offensible Space," Security Management magazine, May 2003; "Defensible Space: An Architectural Retrospective," *Master Builder*, September/October 2004, Vol. 1, Number 1; "Designing Safe Communities: Strategies for Safe and Sustainable Communities," Landscape Architectural Registrations Boards Foundation, Vienna, Virginia, 2004; "Security Design Concepts," Security Planning and Design: A Guide for Architecture and Building Design Professionals, American Institute of Architects, Wiley Publishers, Washington D.C., 2004; "The Security Audit and Premises Liability," Spotlight on Security for Real Estate Managers, 2nd Edition, IREM, 2005.

Ray Bernard, PSP, CHS-III. Founder and publisher of *The Security Minute* electronic newsletter; President and CEO of security management and technology consulting firm Ray Bernard Consulting Services of Lake Forest, CA; founder and former Principal Consultant of Ray Bernard Consulting and Design, Detroit, MI; current technical editor and columnist for *Security Technology & Design* magazine; Board Certified as a Physical Security Professional by ASIS International; Board Certified in Homeland Security (Level III) by the American College of Forensic Examiners International (ACFEI). Education Chair of the ASIS IT Security Council and Education Committee member of the ASIS Physical Security Council of ASIS; participating member of ASTM International standards organization, and member of the ASTM Technical Committee E54 on Homeland Security Applications; member of the International Association of Independent Security Consultants (IAPSC); member of the Information Systems Security Association (ISSA); member of the Information Systems Audit and

Control Association (ISACA); member of IEEE Computer Society; leading author and frequent presenter at security conferences on the subject of the convergence of physical security and IT; author of over 30 major articles for leading security industry and other industry journals including *Access Control & Security Systems, Buildings, Corporate Security News, Engineered Systems, Graduating Engineer, Hi-Tech Security Solutions, Security, Security Management Practices, Security Technology & Design, Seguridad Latina* and *Ventas de Seguridad.*

Bronson Steve Bias, CHS, CPP, CFE, CPO. Executive Director of Protective Services, Nova Southeastern University, Fort Lauderdale/Davie, FL; Adjunct Instructor, School of Justice and Safety Administration, Miami, FL; former Director of Loss Prevention, Bi-Lo Supermarkets, Inc., Greenville, SC; former Commander of Internal Affairs, Hollywood Police Department, Hollywood, FL; member, Board Member, and Executive Committee Member, American Society for Industrial Security; member, International Association of Campus Law Enforcement Administrators; member, National Association of Fraud Examiners; life member, Florida Association of Campus Safety and Security Administrators; life member, Florida Police Benevolent Association and the Fraternal Order of Police; Chairperson, Educational Institutions Standing Committee, ASIS; former Chairperson, Miami Chapter, ASIS; past President, Florida Chapter IACLEA (FACSSA); past President, Broward County Police Benevolent Association; past President, Hollywood Fraternal Order of Police; recipient of the ASIS Region XIII Award of Merit, 1991. Bachelor of Science, Nova University. Author of cover article, *Security, April*, 1991; "Behavioral Analysis," *Security New Canada*, "Recruiting Campus Public Safety Management," Campus Law Enforcement Journal; "Police Benevolent Centurion," *Campus Security Report*, December, 1991; *School Security Report*, September 1991; and *"Campus Crime Prevention,"* chapter, Handbook of Loss Prevention and Crime Prevention, 1996 and 2003.

Ken Bierschbach, CPP. Security Assessment & Development Specialist, Meijer Stores, Grand Rapids, MI; former Loss Prevention Manager, Meijer Stores, Grand Rapids, MI; Member, ASIS International; former Chapter Chairman, Western Michigan Chapter of ASIS; former Chapter Vice Chairman, Western Michigan Chapter of ASIS; Member, Editorial Advisory Board, Private Security Case Law Reporter; Associate of Arts, Grand Rapids Community College, Grand Rapids, MI.

James F. Broder, CPP. Consultant, Confidential Management Services, Inc., San Dimas, CA; former Security Consultant, Marsh and McLennan, Inc.; former Special Agent, U.S. State Department; former Assistant and the Chairman, Investigations Sub-Committee, U.S. House of Representatives. Member, American Society for Industrial Security; member, Society of Former Special Agents of the FBI; member, Association of Former Intelligence Officers; past member, Congressional Staff Association, U.S. House of Representatives; past member, International Association of Professional Security Consultants; Legion of Merit, Vietnam; Bachelor of Arts, Criminology, University of California; author of *Risk Analysis and the Security Survey*, Butterworth-Heinemann; *Investigation of Substance Abuse in the Workplace*, Butterworth-Heinemann; *Resources Control in Counter-Insurgency*, Agency for International Development, U.S. State Department; "Case Management and Control of Undercover Operations for Business and Industry," *Professional Protection*; contributing author, *Effective Security Management*, Butterworth-Heinemann.

Lonnie R. Buckels, CPP. Deceased. Before his death, Mr. Buckels was Head, Information Security, Telecommunications and Space Sector, Hughes Aircraft Company, El Segundo, CA; former Branch Manager, Industrial Security, McDonnell Douglas Corporation, Huntington Beach, and Long Beach, CA; former part-time Instructor, Golden West College, Huntington Beach, CA; former substitute Instructor, California State University at Long Beach; member, American Society for Industrial Security; Chapter Chairman, Greater Los Angeles Chapter, ASIS; National General Chairman, 20th Annual Seminar and Exhibits, ASIS; member, National Classification Management Society; member, Research Security Administrators; member, California Association of Administration of Justice Educators; recipient of the James S. Cogswell Award, Douglas Aircraft Company, Long Beach, CA,

and Hughes Aircraft Company, Torrance, CA; Silver Beaver and District Award of Merit, Boy Scouts of America; Associate in History, El Camino College, Torrance, CA; Bachelor of Arts in History, California State College at Long Beach; Bachelor of Science in Criminal Justice (Security Adminstration Option), California State University at Long Beach; Douglas Management Institute Certificate; co-author of "Is an Ex the Best Candidate?" and "The Security Manager's Apprentice," *Security Management*; author of "A Murphy's Law Corollary in Personnel Selection," "The Perils of 'P'," "The Plague of Security Misconceptions," and "Professionalism—An Impossible Task?" *Security Management*, "While Waiting for the Call That Never Came," *Greater Los Angeles Chapter Newsletter*.

Joseph P. Buckley, III. President, John E. Reid and Associates, Inc., Chicago, IL; past and present Lecturer, Northwestern School of Law, Federal Law Enforcement Training Center, Institute of Internal Auditors, American Society of Industrial Security, and numerous other professional groups; licensed Detection of Deception Examiner Committee, 1978–1982; Vice President, Illinois Polygraph Society, 1981, President in 1982 and 1983, and Chairman of the Board in 1984 of the Illinois Polygraph Society; Chairman, Public Relations Committee, American Polygraph Association, 1979–1980 and 1984–1990; member Investigations Committee of the American Society of Industrial Security, member of various professional associations including International Chiefs of Police, American Management Association, Chicago Crime Commission, Special Agents Association, Federal Law Enforcement Officers Association, International Association of Directors of Law Enforcement Standards and Training, and American Academy of Forensic Sciences; Bachelor of Arts, Loyola University; Master of Science in the Detection of Deception, Reid College of Detection of Deception; co-author of *The Investigator Anthology*, 1999; co-author of *Criminal Interrogation and Confessions*, 4th Edition, 2001; co-author of *The Essentials of The Reid Technique*, 2004; co-author "Abdominal and Thoracic Respiration Recordings in the Detection of Deception," *Polygraph*, 1972; "Relative Accuracy of Polygraph Examiner Diagnosis of Respiration, Blood Pressure and GSR Recordings," *Journal of Police Science and Administration*, 1975; "The Nine Steps of Interrogation," *Security Management*, 1983; "The Use of Behavior Symptoms in the Search for the Truth: A Tool for the Prosecutor," *Prosecutor*, 1985; "The Influence of Race and Gender on Pre-employment Polygraph Examination Results," *Polygraph*, 1991; "The Influence of Race and Gender on Blind Polygraph Chart Analysis," *Polygraph*, 1991; "Criminal Interrogation Techniques on Trial," *Prosecutor*, 1991; author of "Polygraph Technology" a chapter in the text *Modern Legal Medicine, Psychiatry and Forensic Science*, 1980; "The Use of Polygraphs by the Business Community," *Management Review*, 1986; "How Do I Know if They Told Me the Truth?" *Internal Audit Advisor*, 1986; "Nobody's Perfect," *Security Management*, 1987; "Interrogation," a chapter in the text, *The Encyclopedia of Police Science*, 1989; "The Behavioral Profile of a Liar," International Association of Credit Card Investigators NEWS, First Quarter, 1991; "The Behavior Analysis Interview," International Association of Credit Card Investigators NEWS, Second Quarter, 1991.

Robert Capwell. Founder and President, Comprehensive Information Services, Inc. (CIS). Mr. Capwell is considered one of the leading experts in the background screening industry with over 17 years of experience in the field. Mr. Capwell is a founding member and currently sits on the Board of Directors of NAPBS, National Association of Professional Background Screeners, and is also Co-Chair of the Board of Directors for the 2006 fiscal year. Robert has chaired the Public Awareness and Communications Committee and sits on the Government Affairs Committee. He has made industry presentations to various public entities and trade organizations including The Federal Trade Commission, The Department of Transportation, and Sub-Committee on Aviation. Mr. Capwell has also testified to the Pennsylvania Court Administrators and Senate Judiciary Committee staff regarding consumer privacy and data breach legislation. Robert is also the Managing Editor of an industry newsgroup. He was also employed with Equifax, Inc., serving as production supervisor, regional sales representative and field liaison before founding CIS. Mr. Capwell has a Bachelor of Science in Business Administration with a concentration in Management from Penn State University, The Behrend College. He has also served as a part-time high school economics teacher through Junior Achievement and sits on the board of the CIS corporate philanthropic initiative SymbioCIS.

James S. Cawood, CPP, PCI, PSP, CFE. President of Factor One; worked in the area of threat assessment, violence risk assessment, behavioral analysis, violence prevention, security analysis, and incident resolution for more than 20 years, and has successfully assessed and managed over 3,000 violence related cases for federal and state government agencies, public and private corporations, and other business entities throughout the United States; current Association President of the Association of Threat Assessment Professionals (ATAP); former Association 2nd Vice President and President of the Northern California Chapter (ATAP), Former Secretary of ASIS International Foundation Board, Former Chairman of the Board of the California Association of Licensed Investigators (CALI); has served on the faculties of Golden Gate University, in their Security Management degree program and the University of California, Santa Cruz extension, teaching Threat Management; first concurrent holder of all three ASIS International certifications: Certified Protection Professional (CPP), Professional Certified Investigator (PCI), Physical Security Professional (PSP), also a Certified Fraud Examiner (CFE), Certified Security Professional (CSP), Certified Professional Investigator (CPI), Certified International Investigator (CII), and Diplomate, American Board of Forensic Examiners (DABFE); authored articles and book chapters for various professional publications including *Security Management* magazine, as the original author of A Plan for Threat Management (Chapter 40) of the *Protection of Assets Manual*; Chapters 24 – Personnel Screening and Chapter 32 – Arson, Sabotage, and Bomb Threats in the *Accident Prevention Manual for Business & Industry – Security Management* volume; Chapter 32 – Security for *Safety, Health, and Asset Protection: Management Essentials, 2nd Ed*; and a co-authored chapter: Threat Management of Stalking Cases in *The Psychology of Stalking: Clinical and Forensic Perspectives*, published by Academic Press in 1998. He has also co-authored a book, *Violence Assessment and Intervention: The Practitioner's Handbook*, CRC Press 2003.

Russell L. Colling, CPP, CHPA, MS. Executive Vice President, Hospital Shared Services of Colorado, Denver, CO; Adjunct Professor, Security Management, Webster University, Denver, CO; former Assistant Vice President, Chicago Wesley Memorial Hospital, Chicago, IL; former Security Compliance Officer, Martin Marietta, Denver, CO; former Police Officer and Chief of Police, Saugatuck, MI; member, American Society for Industrial Security; founding president, charter member and life member, International Association for Healthcare Security and Safety; past Chairman/member, Metropolitan Law Enforcement Association, Denver, CO; past Chairman/member, Colorado Law Enforcement Memorial Committee; member, American Hospital Association, Ad Hoc Security Committee; member, Board of Directors, School of Criminal Justice Alumni Association, Michigan State University; member, Editorial Advisory Board, *Security Journal*; Editorial Advisory Board, *Hospital Security and Safety Management*; recipient of first Russell L. Colling Literary Award, International Association for Healthcare Security and Safety; Bachelor of Science, Michigan State University; Master of Science, Michigan State University; Editor, *Security Officer Basic Training Manual*, International Association for Healthcare Security and Safety; Editor, *Supervisor Training Manual*, International Association for Healthcare Security and Safety; author, "Hospital Security: Is the Patient at Risk," *Journal of Healthcare Protection Management*; author of *Hospital Security*, 3rd Edition, Butterworth-Heinemann.

Geoff Craighead, CPP. Head of High-Rise and Real Estate Security Services, Securitas Security Services USA, Inc., an organization that provides support for high-rise facilities throughout the United States. He has been involved in the security and life safety operations of industrial and high-rise facilities for over 20 years. He has conducted extensive security surveys and training programs, developed security policies and procedures, and written building emergency plans. Mr. Craighead is a member of the Building Owners and Managers Association (BOMA) Greater Los Angeles Board of Directors and chair of the ASIS Commercial Real Estate Council. He is certified by the Los Angeles Fire Department to provide high-rise life safety services and serves on the National Fire Protection Association (NFPA)'s High-Rise Building Safety Advisory Committee. Mr. Craighead is board-certified in security management (CPP) by ASIS International and a past president of the ASIS Professional Certification Board that administers certification programs for security professionals throughout the world. Mr. Craighead is author of *High-Rise Security and Fire Life Safety, Second Edition*, published by Butterworth-Heinemann. It is a comprehensive reference for security and

fire life safety operations within commercial office buildings/skyscrapers. In addition, he has had numerous articles published in industry magazines on office security, high-rise emergency planning, and contract security for high-rise buildings. Mr. Craighead has spoken on security and emergency planning for high-rise buildings at BOMA International and the Institute of Real Estate Management (IREM) workshops. He has also spoken and at national conventions of ASIS International, the Risk and Insurance Management Society (RIMS), and The Council on Tall Buildings & Urban Habitat.

Sidney W. Crews. Adjunct instructor with the Texas Engineering Extension (TEEX), and a member of the Texas A&M University system. Mr. Crews travels the country teaching Enhanced Threat and Risk Assessment courses focusing on potential threat elements, security concepts, building systems, physical security practices and devices, and preparation/conduct of vulnerability assessments. Prior to joining TEEX, Mr. Crews was a U.S. Army Special Forces officer who served in various assignments over his 20-year career. He has been responsible for developing programs of instruction and training for approximately 5,000 personnel in seven nations. He has instructed on such topics as physical security planning and oversight, risk management, critical infrastructure and personnel protection, surveillance/surveillance detection, anti/counterterrorism procedures, dispute mediation, and intelligence gathering/investigative procedure. While serving as a Special Forces Operational Detachment–Alpha (A-team) commander Mr. Crews was hand-picked to recruit, outfit, and train a one-of-a-kind team that was responsible for conducting clandestine operations of the highest sensitivities. During Operation Iraqi Freedom, he led the detachment into Iraq, well in advance of any U.S. ground or air presence, to conduct extremely sensitive operations deep behind enemy lines. These operations included both targeting and security assessments of various operationally important compounds and facilities, as well as instructing Kurdish forces in physical security improvement measures and other operations. For his actions in Iraq, he was awarded the Bronze Star with "V" (for valor) by President George H.W. Bush. He also organized and led area studies and security assessments in other permissive and semi-permissive environments. Prior to his retirement from the Army in 2005, Mr. Crews was an Assistant Professor of Military Science at Texas A&M University. There, as a Course Director, he completely redeveloped course curriculums, training schedules and programs of instruction for the largest U.S. Army Reserve Officer Training Corps in the nation consisting of 600 students and 20 cadre members. He managed a ROTC instructional training staff that instructed approximately 200 hours of undergraduate coursework per student while personally conducting approximately 1,000 hours of classroom/lab presentations and stand-up training. Mr. Crews is a graduate of the University of Washington, where he received a Bachelor's Degree in International Study and was on the Dean's List for academic excellence for all terms and he has earned a Project Management Certificate from the University of Washington. He has received numerous military honors and is a graduate of both the U.S. Army Ranger and Special Forces qualification courses as well as many others. He holds a Department of Defense Top Secret security clearance and is a member of the American Society for Industrial Security (ASIS).

Dennis Dalton, DPA. Former Director of Academic Affairs for the University of Phoenix's Sacramento Campus. He teaches primarily for the Colleges of Graduate and Undergraduate Business and Management. He holds a Doctorate in Public Administration from the University of Southern California, a Master's Degree in Adult Education, and a Bachelor's Degree in Criminal Justice from Michigan State University. In 1987 he founded Dalton Affiliates, an international security management consulting firm for Fortune 500 companies. He is recognized as one of the country's foremost security experts, having been retained in over 250 cases, serving as the lead consultant for the World Trade Center bombing, the Empire State Building Palestinian shooting, and the Atlanta Day-Trader mass shooting. He is a former police officer, educator and administrator and served as Vice President and Director of Corporate Security for three large multinational companies. He is the author of many manuals, articles, and videos, and is a well-known speaker on management subjects. He has authored three very successful books on security management. His most recent is entitled: *Rethinking Corporate Security in the Post 9/11 Era: Issues and Strategies for Today's Global Business Community*. He is also a winner of Security Magazine's "Executive Achievement Award" and is the only person to have appeared

on the magazine's cover twice. He has appeared on MSNBC, Fox News, the BBC, several radio stations, and is considered an industry spokesperson for several leading newspapers, including the Wall street Journal, the Los Angeles Times, and the San Francisco Chronicle.

Sandi J. Davies began her career in contract security in 1980 with a primary focus on personnel administration. She became deeply involved in training and was instrumental in developing Security Officer training programs for a major guard company. Her interest in security training grew, and in 1988 she joined the newly formed International Foundation for Protection Officers (IFPO) as a program administrative assistant. In 1991 she was elected executive director of the International Foundation for Protection Officers. She became a member of the American Society for Industrial Security (ASIS) in 1985 and has served in executive positions at the chapter level. Ms. Davies is also a Member of the Technical Advisory Board for the Canadian General Standards Board on Security Officer Training Standards. In addition, she is a Member of the Advisory Board for the Northwest Territories Security Officer Certification Committee. In 1999 Sandi agreed to serve on the Advisory Board of the International Foundation for Cultural Property Protection. Since 1994 Sandi has been the Chairperson for the Asset Protection Advisory Board for Mount Royal College in Calgary, Alberta Canada. Most recently, Sandi has been involved as an Associate Member of the Private Security Services Council of ASIS International. She has had numerous articles published in security publications relating to certifications and training of security personnel. In the early 1990s Ms. Davies in a cooperative effort with the IFPO Founding Director; Ronald R. Minion, co-edited the *Protection Officer Training Manual,* published by Butterworth-Heinemann. That text is now in its 7th edition. In 1994 she contributed a chapter relating to crime prevention in Canada in the *Handbook of Loss Prevention and Crime Prevention,* published by Butterworth-Heinemann. In 1995, again in a cooperative effort, Ms. Davies and Mr. Minion co-authored a Butterworth-Heinemann text entitled *The Security Supervisor Training Manual.* In July 1999 the second edition of this text was released as, *Security Supervision: Theory and Practices of Asset Protection,* again published by Butterworth-Heinemann. Sandi also edits "Protection Officer News," published by the International Foundation for Protection Officers, now in its 13th year of publication.

Andrés de la Concha Bermejillo, DVM, MS, PhD. Pathologist, Texas Veterinary Medical Diagnostic Laboratory, Texas A&M University, College Station, Texas; Consultant, National Emergency Response and Rescue Training Center, Texas Engineering Extension Service (TEEX), Texas A&M University; Associate Professor, Department of Veterinary Pathobiology, College of Veterinary Medicine, Texas A&M University; Assistant Professor and Research Project Leader, Department of Pathobiology, Texas A&M University's Agricultural Research and Extension Center, San Angelo, Texas; post-doctoral trainee, Department of Pathology, College of Veterinary Medicine and Biomedical Sciences, Colorado State University; post-graduate researcher and resident in diagnostic pathology, Department of Pathology, School of Veterinary Medicine, University of California, Davis; Professor and Chief of Service, Department of Pathology, School of Veterinary Medicine and Animal Science, National Autonomous University of Mexico, Mexico City; member of the American Society for Virology; awards and distinctions include the 2004 Robert & Virginia Lectureship, Western College of Veterinary Medicine, University of Saskatchewan; Member, Editorial Review Board, Clinical & Diagnostic Laboratory of Immunology; Member, Scientific Panel, Premio Canifarma "Dr. Alfredo Tellez Giron Rode," Consejo Nacional de Ciencia y Tecnologia (CONACYT), Mexico; National Institutes of Health Minority Investigator Award; peer-reviewed publications include *Genetic Characterization of Viruses Isolated from Various Ruminant Species of a Zoo, Genomes of Parapoxviruses, Virus and Bovine Papular Stomatitis Virus, Construction and Characterization of a Recombinant Ovine Lentivirus Carrying the Optimized Green Fluorescent Protein Gene at the dUTPase Locus,* and a book chapter of *Maedi-visna and Ovine Progressive Pneumonia.*

Sal DePasquale, CPP has over 25 years experience in the physical security field and has gained special expertise in vulnerability analysis and long term strategic planning. He is a former manager

of security at Georgia Pacific and is presently a security consultant for CH2MHill, an organization that provides services to the chemical industry. In the past, he has consulted with the Department of State, Department of Energy, Honeywell, W.R. Grace, Aetna, American Airlines, AT&T, Atlanta Gas and Light, General Electric, Georgia Power, University of Virginia, Tampa International Airport, Kraft Foods, New Jersey Institute of Technology, Phillip Morris, and Spartanburg County, SC. Mr. DePasquale instructs at Georgia State University and has taught at Polytechnic University and the American Institute of Chemical Engineers (AIChE). He holds a Master of Business Administration, Mercer University, and a Master of Science, University of South Carolina. His memberships include the Physical Security Council, ASIS International; Site Security Committee, American Chemistry Council; Center for Chemical Process Safety; and a American Institute of Chemical Engineers. He has authored numerous security-related articles and has presented at a great number of seminars and workshops. Mr. DePasquale served with the U.S. Marine Corps in Vietnam.

Michael Erbschloe. Information technology consultant, educator, and author. He has taught graduate level courses and developed technology-related curricula for several universities and speaks at conferences and industry events around the world. Michael holds a Master Degree in Sociology from Kent State University. He has authored hundreds of articles on technology and several books, including *Physical Security for IT (Elsevier Science); Trojans, Worms, and Spyware (Butterworth-Heinemann); Implementing Homeland Security in Enterprise IT (Digital Press); Guide to Disaster Recovery, Course Technology,* and*Socially Responsible IT Management (Digital Press); Information Warfare: How to Survive Cyber Attacks (McGraw Hill); The Executive's Guide to Privacy Management (McGraw Hill); Net Privacy: A Guide to Developing & Implementing an e-business Privacy Plan (McGraw Hill).*

John J. Fay, CPP is the owner/operator of The Learning Shop, a provider of online courses and tests for security professionals and private investigators. He is also an Adjunct Instructor at Texas A&M University. Prior employment includes Adjunct Instructor, DeKalb Institute; Security Manager, British Petroleum Exploration; Adjunct Professor, University of Houston; Director of Corporate Security, The Charter Company; Director, National Crime Prevention Institute; Chief of Plans and Training, Georgia Bureau of Investigation; Chief of Training Standards, Georgia Peace Officer Standards and Training Council; Special Agent, U.S. Army Criminal Investigation Division; Lecturer, Police Science Division, University of Georgia; and Adjunct Professor, University of North Florida. Associate Member, Georgia Association of Professional Private Investigators. Former Certified Protection Professional (CPP), Regional Vice President, Chapter Chairman, and member of the CPP Board, American Society for Industrial Security International; Association of Chiefs of Police; Peace Officers Association of Georgia; Texas Police Association; and Houston Metropolitan Criminal Investigators Association. Honor Society, University of Nebraska at Omaha; Bronze Star Medal with Oak Leaf Cluster (Vietnam); Meritorious Service Medal (Vietnam); and U.S. Army Commendation Medal. Bachelor of General Education, University of Nebraska at Omaha and Master of Business Administration, University of Hawaii. With Butterworth-Heinemann, author of *Contemporary Security Management; Model Security Policies, Plans, and Procedures; Encyclopedia of Security Management; Drug Testing;* and *Butterworth's Security Dictionary.* Other books include *Security Dictionary,* American Society for Industrial Security International; *The Alcohol/Drug Abuse Dictionary and Encyclopedia,* Charles R. Thomas; *The Police Dictionary and Encyclopedia,* Charles R. Thomas; and *Approaches to Criminal Justice Training,* University of Georgia.

Eugene F. Ferraro, CPP, CFE, PCI. President and Chief Executive Officer, Business Controls, Inc., Littleton, CO; former chairman of the Workplace Substance Abuse Council, American Society for Industrial Security International (ASIS) and current Program Advisor for the ASIS Asset Protection Course II; former military pilot, intelligence officer and a graduate of the Naval Justice School; author of eight books, including *Undercover Investigations in the Workplace* and *Investigations in the Workplace;* past and current affiliations with professional associations include ASIS International, Association of Certified Fraud Examiners, Professional Private Investigators Association of Colorado, National

Council of Investigative and Security Services, National Association of Professional Process Servers, and California Association of Licensed Investigators.

Mary Lynn Garcia received a Bachelor of Arts in Biology from the State University of New York at Oswego, a Master of Science in Biomedical Sciences from the University of New Mexico, and a Certificate in Electronics Technology from the Albuquerque Technical-Vocational Institute. Ms. Garcia is a Senior Member of the Technical Staff at Sandia National Laboratories where she has worked for the past 16 years in international safeguards and physical security. Her past projects include development of an automated video review station, video and lighting design for a demonstration physical security system at a major U.S. airport, and project management of an integrated alarm communication and display system. She has taught classes at U.S. universities to initiate new programs in security engineering, internationally in the People's Republic of China, and to other government and industry groups. Ms. Garcia has written a textbook on the design and evaluation of physical protection systems for use in university security courses and is currently writing another text on vulnerability assessment of physical protection systems. Ms. Garcia is a member of the American Society for Industrial Security, is a Certified Protection Professional, and serves as a member of the ASIS Standing Committee on Academic Programs and the Security Architecture and Engineering Committee.

Richard P. Grassie, CPP is President of TECHMARK Security Integration, Inc., a Boston-based security design and integration firm with a wide range of Fortune 500, institutional, and government clients both in the United States and abroad. Mr. Grassie has designed and implemented complete asset protection programs for manufacturing and industrial sites, internet service provider hardware and service providers, internet start-up companies, biopharmaceutical companies, private residences, international petroleum terminals, transportation complexes, commercial office complexes, medical and educational institutions, college and university campuses, aerospace firms, publishing companies, communications centers, high rise commercial office, food processing, tobacco and pharmaceutical plants, international airports, government intelligence gathering and radar sites, military air bases and installations, court houses, vaccine research centers, high schools and middle schools, banks, and industrial parks. His systems design and integration expertise includes environmental designs, facility access controls, electronic intrusion detection, closed circuit television surveillance and assessment, local and remote site communications, networking remote sites over LAN/WAN, and computer-based central monitoring systems. He is equally well versed in security technology, crime prevention, security awareness, policies and procedures, and security personnel. During the early stages of his career, he was a sworn police officer, an urban crime analyst and manager of technical assistance to police and prosecutor agencies for the U.S. Department of Justice's Integrated Career Criminal Apprehension Program. Mr. Grassie also served for 15 years as Director of Project Development for one of the world's leading security systems integrators and managed security design and installation projects in the Pacific Rim, South America, Middle East, and Europe.

George D. Haddow. Principal, Bullock & Haddow LLC, Washington, D.C.; Adjunct Professor, Institute for Crisis, Disaster and Risk Management, George Washington University, Washington, D.C.; former Deputy Chief of Staff and White House Liaison, Federal Emergency Management Agency (FEMA), Washington, D.C.; Bachelor of Arts, Washington College, Chestertown, MD; Masters of Urban and Regional Planning (MURP), University of New Orleans; co-Author of *Introduction to Emergency Management,* Butterworth-Heinemann; co-Author of *Introduction to Homeland Security,* Butterworth-Heinemann.

Richard J. Heffernan, CPP, CISM. President of R.J. Heffernan and Associates, Inc., Guilford, CT. Senior advisor and consultant to business and government on risk management of information, products, and people; member of Information Systems Security Association, Information Security Audit and Control Association and American Society for Industrial Security International (ASIS); Past Chairman, ASIS Information Asset Protection Council; and former member, National Counter

Intelligence Center Advisory Board; author and principal investigator of the ASIS Trends in Intellectual Property Theft Survey Report, and the ASIS Proprietary Information Loss Survey Reports. 1991–2006. Mr. Heffernan has testified before the U.S. Congress concerning espionage targeting and best practices in information security. Representing the 30,000+ members of ASIS before the U.S. Congress, his testimony was a key element in defining the need for and shaping the Economic Espionage Act.

Robert B. Iannone, CPP. President, Iannone Security Management, Inc., Fountain Valley, CA; former Adjunct Professor, School of Business, California State University, San Marcos, CA; former Adjunct Professor, Department of Criminal Justice, California State University, Long Beach, CA; former Adjunct Professor, Administration of Justice, Golden West College, Huntington Beach, CA; former Manager of Security, Hughes Aircraft Company, Torrance, CA; former Manager of Security and Investigations, Rockwell International Corporation, El Segundo, CA; former Security Inspector, Douglas Aircraft Company, Long Beach, CA; Member, American Society for Industrial Security; former Chapter Chairman, Greater Los Angeles Chapter, American Society for Industrial Security; Member, Board of Directors, Research Security Administrators; Member, International Association of Professional Security Consultants; Recipient of the James S. Cogswell Award, Department of Defense; bachelor of Science, California State University, Long Beach, CA; Master of Science, LaVerne University, LaVerne, CA; co-author of "Security, Higher Training, and Internship," *Security Management* and "Is an Ex the Best Candidate?" *Security Management*; contributing author, "Requirements Specification For An Integrated Electronic Security System," *"Risk Analysis and The Security Survey."*

Steven R. Keller, CPP is a Certified Protection Professional, and with 36 years in security related positions, he is Board Certified in Security Management. He is the former Executive Director of Protection Services and Construction Projects Advisor for the Art Institute of Chicago. Steve is the author of over 40 articles in professional publications, and is a frequent speaker at AAM and regional museum conferences. His written contributions include sections of "The Encyclopedia of Security" and sections pertaining to security technology for Microsoft's "Encarta Encyclopedia." He is a former chairman of ASIS International's Committee on Museums, Libraries, and Cultural Properties and has been a member of AAM's security committee for over 20 years. He has taught museum burglar and fire alarm design seminars at numerous venues including New York University, and was an author of "The Suggested Guidelines for Museum Security," the prevailing standard. He has been interviewed by all major TV networks, National Public Radio, and BBC on museum security issues. He is the recipient of the ASIS International's President's Award of Merit and "Security" Magazine's Executive Achievement Award. He has been a speaker at the Smithsonian's National Conference on Cultural Property Protection 19 of the past 25 years. He is Principal Consultant of Steve Keller and Associates, Inc. He recently authored "The Instant Museum Security Department Policy Manual" and a software package for managing a museum security operation, "The Security Department Knowledge Base." In 2006, Mr. Keller was inducted into the Centennial Honor Roll of the American Association of Museums.

Daniel B. Kennedy, PhD, CPP. Professor, Department of Sociology and Criminal Justice, University of Detroit Mercy, Detroit, MI; Consulting and testifying expert in premises liability, negligent security litigation, and use of force Issues; former Probation Officer and Police Academy Director. Member of American Society for Industrial Security, International Association of Chiefs of Police, and International Society of Crime Prevention Practitioners; former Chairman, Academic Programs Committee of American Society of Industrial Security; recipient of Chairman of the Year, American Society for Industrial Security; Faculty Award for Excellence, University of Detroit; Bachelor of Arts, Master of Arts, and Doctor of Philosophy, Wayne State University, Detroit, MI; graduate of the National Crime Prevention Institute and the author of seven books and over 80 professional articles appearing in such periodicals as *Security Journal, Journal of Security Administration, Security Management, Journal of Police Science and Administration, Justice Quarterly, Journal of Criminal Justice, Professional Psychology, Journal of Social Psychology,* and *Journal of Business and Psychology.* Dr. Kennedy

is currently active in the design of computer security and intelligence analysis curricula in response to the war on terrorism.

Carl E. King. Chief Executive Officer, President, Akers Biosciences Houston, TX; Chief Executive Officer, Insights Corporate Selection Systems, Houston, TX; Chief Executive Officer WNCK, Inc., Houston, TX; Major, U.S. Marine Corps, Retired. Member of International Association of Chiefs of Police; American Society for Industrial Security; Private Security Services Council of American Society of Industrial Security; FBI National Academy; National Order of Battle Field Commissions; listed in *Who's Who in Finance and Industry, 1989–1992;* listed in *Who's Who in Security, 1989–1992;* named to *Inc.* magazine's 1990 list of 500 Fastest Growing Companies; finalist for Houston's Entrepreneur of the Year; recipient of two Purple Hearts, the Bronze Star, Presidential Unit Citation, and other Vietnam awards. Bachelor of Science in Criminal Justice, University of Nebraska at Omaha; Bachelor of Laws, Lasalle Extension University, Chicago, IL; Master of Arts in Business Management, Central Michigan University; graduate of the Federal Bureau of Investigation National Academy, Quantico, VA; graduate of the Military Police Officers Advanced Course. Author of "Why Test for Alcohol?," "When Is a Drug Not a Drug?," and "Alcohol Abuse on the Job," *Security Management.*

Glen Kitteringham, MSc, CPP, FIISec. Senior Manager, Security & Life Safety, Brookfield Properties Corp., Calgary, Alberta; former Internal Investigator, Hudson Bay Company; former Loss Prevention Officer, Hudson Bay Company; Member, ASIS International, International Foundation for Protection Officers (IFPO), National Fire Protection Association, BOMA Canada, International Institute of Security; former Chair, Calgary/Southern Alberta Chapter of ASIS; former Vice-Chair, Commercial Real Estate Council, ASIS; member Business Practices Council, ASIS; Vice-Chair International Advisory Board, IFPO; former Chair, BOMA Calgary Public Safety Committee, BOMA; member BOMA Canada Public Safety Committee; Director, BOMA Calgary; Fellow, International Institute of Security. Obtained Diploma in Criminology from Mount Royal College, Calgary, Alberta, 1992; Security Management Certificate from University of Calgary, Alberta, 1998; Masters of Science Post Graduate Degree from University of Leicester, United Kingdom, 2001; General Management Certificate, University of Calgary, Alberta, 2005; awarded Crime Prevention Award from Province of Alberta Solicitor General's Office, 2003; written, published or presented more than 80 times on various aspects of security management and/or life safety including six training videos with the Professional Security Training Network (PSTN); author of *Environmental Crime Control Theory; IFPO Certified Protection Officer Training Manual, 7th Ed,* Butterworth-Heinemann; contributing member *Threat Advisory System (TASR) Guideline: Guideline for Preparations Relative to the Department of Homeland Security Advisory System,* ASIS International; author of the soon-to-be published *Security Management Guidance for the Commercial Real Estate Industry,* ASIS International; author of Dissertation entitled, "A study of two types of vertical crime pattern analysis in the commercial multi-tenanted high-rise structure" for a Masters degree in Security and Crime Risk Management, March 2001. This dissertation currently resides within the National Criminal Justice Reference Service Database, a division of the United States Department of Justice. Member of a team researching Canadian Shoplifting Offenders Study, coordinated through PRCI Ltd. (U.K.) as part of a four-country study (Spain, Brazil, England, Canada).

Robert L. Kohr, CSP, CPP. Senior Consultant, Arthur D. Little, Inc., Cambridge, MA; Principal, Kohr & Associates, Mt. Airy, MD; Director of Design and Director of Technical Services for Loss Prevention, Marriott Corporation, Washington, D.C. Member, American Society of Safety Engineers; member, American Society for Industrial Security; member, American Society for Testing and Materials; member, National Safety Council; member, National Fire Protection Association; member, Building Officials and Code Administration International; member, American Hotel and Motel Association; Secretary, ASTM F13 and C21.06. Bachelor of Science, Geology, Virginia Polytechnic Institute and State University. Author of *Accident Prevention for Hotels, Motels, and Restaurants,* Van Nostrand Reinhold; "Washroom Safety, Things to Consider," and "Slip, Slidin' Away," *Safety & Health;* "Safety Factor in Bathroom Design," "Recognizing and Preventing Slip and Fall Accidents," "How Safe Are Marble

Floors?," and "It Could Be A Crime," *Lodging*; "Security By Design" and "Mastering the Challenge of Securing a Budget Motel," *Security Management*; "A Study of the Comparative Slipperiness of Floor Cleaning Chemicals," "Worker Safety in the Kitchen: A Comparative Study of Footwear versus Walking and Working Surfaces," and "Bucknell University F-13 Workshop to Evaluate Various Slip Resistance Measuring Devices," *Standardization News*; "Slip Resistance and the Designer," *Progressive Architecture*.

Herman A. Kruegle. President, Avida Inc., former President, Visual Methods, Inc.; former Section Head, Electro-Optics Division, ITT Avionics, Clifton, NJ; former Manager, Laser and Electro-Optical Systems Division, Holobeam, Inc., Paramus, NJ; former Assistant Chief Engineer, Spectroscopic and Electro-Optical Laboratory, Warner and Swasey Co. Member, Institute of Electrical and Electronic Engineers (IEEE); member, American Society for Industrial Security (ASIS); Chairman, 1992, 1993, Closed Circuit Television Manufacturers Association (CCTMA); awarded six patents in security, electro-optical, and laser fields; Bachelor of Science in Electrical Engineering, Brooklyn Polytechnic Institute; Master of Science in Electrical Engineering, New York University; Licensed New York State Professional Engineer; author of numerous publications in professional security and electro-optics journals; contributing author, *Handbook of Loss Prevention and Crime Prevention, Controlling Cargo Theft, Museum, Archive and Library Security,* Butterworth-Heinemann; author of *Lens Primer Series,* CCTV Source Book; author of *CCTV Surveillance,* Elsevier, Butterworth-Heinemann.

William A. "Tony" Lavelle. Consultant, TYH Police & Military Canine Services, Sacramento, CA; Vice President, Detection Support Services, Walnut Creek CA; Lobbyist, International Explosive Detection Dog Association, Wilmington, DE; Adjunct Professor, Division of Criminal Justice, California State University, Sacramento ("CSUS"), CA; Director of Force Protection, Travis AFB, CA; Deputy Chief of Police, Osan Air Base, Republic of Korea and Rhein-Main Air Base, Germany; National Chairman, International Explosive Detection Dog Association; Member, International Association of Bomb Technicians & Investigators, American Society for Industrial Security, Military Officers Association of America, U.S. Air Force Security Police Association, American Legion, China Post 1, Disabled American Veterans Association, International Chiefs of Police Association, and American Society of Law Enforcement Trainers. Significant career achievements include being handpicked to command a prototype force-protection rapid deployment unit created to support worldwide military special missions, with responsibilities for anti-terrorism actions and force protection command and control, safeguarding U.S. and Allied Armed Forces aircraft and ground personnel, including missions to Somalia, Haiti, and South America, Africa, and Southwest Asia. At CSUS, developed the criminal justice division's first web-based course program and the division's first professional speakers bureau; selected as the top faculty associate in the 45 member Criminal Justice Division. Established and made operational Detection Support Services (DSS), an organization that provides explosive detection services. DSS deployed 20 bomb-dog teams to Iraq to support U.S. Forces during *Operation Iraqi Freedom*. Master of Science Degree, Criminal Justice, CSUS; author of *State Terrorism and the Death Squad: A Study of the Phenomenon*, Air Force Institute of Technology, Wright-Patterson Air Force Base and University Publications of America, Bethesda, MD, 1993; co-author of *Global Mission Standard for Explosive Detection Dog Teams,* International Explosive Detection Dog Association, 2004. Infantryman, U.S. Army Airborne, with one combat tour in Vietnam; commissioned officer, U.S. Air Force Security Police. Decorations include the Bronze Star medal with "V" device; Purple Heart; U.S. Air Force Meritorious Service Medal; and the U.S. Army Combat Infantry Badge.

Lindsey M. Lee, BS, MA is an Investigative Consultant for the Investigations Department, forensic clinician on the Behavioral Sciences Team, and Account Manager for Business Controls, Inc.'s Anonymous Incident Reporting Systems, MySafeWorkplace and MySafeCampus. She is responsible for consulting and supporting undercover and special investigations, as well as the training, implementation, and supervision of undercover operatives. Additionally, Ms. Lee is assisting in the development and expansion of the Behavioral Sciences Department to include forensically-related evaluations, trainings, and

other activities. She furthermore manages and supervises the call center representatives responsible for the intake of highly sensitive reports on the MySafeWorkplace and MySafeCampus systems. Related to her call center management, Ms. Lee conducts training, oversees the quality assurance program, and provides general support for all agents. She also guides the training, implementation, and rollout of the MySafeWorkplace and MySafeCampus systems for many premier organizations. Ms. Lee is a contributing editor for *Security Newsletters*, published by Business Controls, Inc. In 2002, Ms. Lee obtained a Bachelor of Science in Experimental Psychology from Millikin University in Decatur, Illinois and a Master of Arts in Forensic Psychology from the University of Denver, Denver, Colorado, in 2005. She completed a nine-month clinical internship with the Division of Youth Corrections at Mount View Youth Services Center, Denver, Colorado. Her responsibilities included assessing committed youth offenders for the presence or absence of mental health impairment, making recommendations for appropriate placement, and scheduling and conducting follow up therapeutic sessions with the most disturbed. Additionally, she wrote evaluation reports to guide the placement board in their decision-making. Prior to her arrival in Denver, Ms. Lee worked in the Division of Women and Family Services for the Illinois Department of Corrections at Lincoln Correctional Center (LCC), a medium security women's prison. At LCC, she assisted in release planning, interviewed female offenders for appropriate class placement, and co-facilitated psychoeducational groups, such as anger management and writing expression. Furthermore, Ms. Lee has extensive experience in conducting original psychological research and developing computer-based psychological experiments. Ms. Lee's professional affiliations include: The Association of Threat Assessment Professionals (ATAP) and Phi Kappa Phi National Academic Honor Society.

Liz Martínez. Author of *The Retail Manager's Guide to Crime and Loss Prevention: Protecting Your Business from Theft, Fraud and Violence* (2004, Looseleaf Law); "Using the Internet to Get a Job in the Criminal Justice Field," Chapter 12 of *Career Planning in Criminal Justice, 3rd Ed.* (1998, Anderson Publishing); editor of *Public Safety Funding Solutions* Newsletter and *Beyond the Badge* Magazine. Fiction credits include editing and contributing to the anthology *Cop Tales 2000* (2000, .38 Special Press); as well as short stories in the anthology *Manhattan Noir* (2006, Akashic Books); *COMBAT Literary Journal*; OrchardPressMysteries.com; *Civil Service Journal*; and *Police Officer's Quarterly*. Long-time contributor to domestic and international publications, including Law Enforcement Technology, Loss Prevention, Security Technology & Design, SecurityInfoWatch.com, Security Today (India), TheBackup.com, and many others; instructor, security and criminal justice, in the security management degree program at Interboro Institute, a two-year college in New York City, NY State Certified Security General Topics Instructor; retail security/loss prevention consultant and trainer; lecturer on the topics of organized crime, criminal justice, security and publishing for ASIS International, Contingency Planning Expo, Interboro Institute, John Jay College of Criminal Justice, Learning Annex, New Jersey Opticians Association, Police Writers Conference, and Vision Expo West; trained USMC officers to deal with the media during the 1994 East Coast Commanders Media Training Symposium. Former NYPD; Auxiliary Police Officer; formerly with Pre-Trial Services, Fairfax County, Virginia; Bachelor of Arts in Criminal Justice, John Jay College of Criminal Justice, New York, NY; Master of Arts in writing popular fiction, Seton Hill University, Greensburg, Pennsylvania; memberships in ASIS International, Criminal Justice Educators Association of New York State, National Native American Law Enforcement Association, Mystery Writers of America, Public Safety Writers Association, and Sisters in Crime.

Brad Mathers, MA is an Investigative Consultant and Forensic Clinician in the Behavioral Sciences Department at Business Controls, Inc. He is involved in the development and expansion of the Behavioral Sciences Department, which includes conducting forensically-related evaluations, trainings, pre-employment screening, fitness-for-duty evaluations, threat assessments, and police psychology. He is involved in the Special Investigations division at Business Controls, Inc., to include workplace investigations and corporate consulting. He is the primary editor for Security Newsletters, Business Controls, Inc.'s monthly newsletter. Mr. Mathers earned his Bachelor of Arts

in Psychology from the University of Colorado, Boulder in 1999 and later earned his Master of Arts in Forensic Psychology at The University of Denver in 2002. He has been a Neighborhood Justice Coordinator for the Denver District Attorney's Office, during which his duties included the mediation of victim-offender conferences stemming from juvenile court. He has been a Forensic Clinician for the Colorado Department of Corrections in Denver County. His responsibilities included the treatment and evaluation of a population of individuals with criminal involvement and a psychological disposition. From this experience, he brings specialized knowledge concerning the psychological machinations of the criminal mind, violence and risk assessment, appropriate implementation of psychological interventions, keen diagnostic interpretation, and suicide and crisis intervention. Mr. Mathers has also been a Litigation and Jury Consultant for Courtroom Performance, Inc., a Colorado-based litigation consulting firm. As a Litigation and Jury Consultant, he assisted attorneys in developing effective presentation styles and litigation strategies, as well as selecting favorable juries. Mr. Mathers' previous clinical experiences have included administering psychological assessments and conducting clinical interviews for the purposes of creating a diagnostic model for clientele, assessing violence and risk potential, and coordinating treatment efforts with psychiatrists, psychologists, hospital staff, and correctional staff. In addition, Mr. Mathers has provided expert testimony and has participated in parole, probation, and disability hearings. Mr. Mathers' professional affiliations include the American Society of Trial Consultants and the Association of Threat Assessment Professionals.

Leon C. Mathieu, CFE. Security Director, Conocophillips Global Security, Houston, TX; former Chief of Investigations, The Charter Company, Jacksonville, FL; former Detective, Metropolitan Dade County Police, Miami, FL; former Insurance Adjuster, Employer's Service Corporation, Coral Gables, FL; former Instructor, Miami-Dade Community College, Miami, FL; member, American Society for Industrial Security; former Chapter Chairman, Jacksonville, Florida, Chapter of ASIS; Certified Fraud Examiner (CFE) member, International Society of Crime Prevention Practitioners; member, Energy Security Council, Houston, TX. Bachelor of Science, Florida International University; and Master of Science, Nova University.

Robert D. McCrie, PhD, CPP. Professor of Security Management, John Jay College of Criminal Justice, the City University of New York; founding editor and now editor emeritus of *Security Journal.* Founder and editor of Security Letter; member, ASIS International; recipient of President's Award of Merit, Urban History Association; Breslin Award, International Security Management Association; John J. Duffy Award, National Council of Investigation and Security Services; and Harvey J. Watson Award, National Association of Security Companies; Certified Protection Professional; author of *Security Operations Management,* Butterworth-Heinemann; *Readings in Security Management,* ASIS International; and numerous articles in the field.

Chris E. McGoey, CPP, CSP. President, McGoey Security Consulting, Phoenix, AZ; Publisher of security books, Aegis Books, Oakland, CA; former Security Manager, Neiman-Marcus, San Francisco, CA; former Corporate Loss Prevention and Region Security Manager, Southland Corporation, Dallas, TX; former Security Consultant, Big Bear Markets, San Diego, CA; former Security Manager, S.S. Kresge Corporation, San Diego, CA; former Criminal Investigator, Santa Clara County Public Defender's Office, San Jose, CA; member, International Association of Professional Security Consultants; member, American Society for Industrial Security; member, Retail Security Association of Northern California; member, California Crime Prevention Officers Association; member, California Association of Licensed Investigators; member, National Association of Legal Investigators; Board of Directors, International Association of Professional Security Consultants; District Governor, California Association of Licensed Investigators. Recipient of the President's Award for District Governor of the Year, California Association of Licensed Investigators; and recipient of the Governor's Crime Prevention Award, State of Nevada; associate of the Arts, Police Science, Chabot College, Hayward, CA; Bachelor of Science, Criminal Justice Administration, San Jose State University; Master of Science,

Criminal Justice Administration (12 units completed), San Jose State University; author of "Security; Adequate...or Not?," "The Complete Guide to Premises Liability Litigation," and "Premises Liability Investigation," *CALI*; "A Model of Management," and "Effective Security Design Must be Flexible," *Access Control*.

Steven W. McNally, MA, CPP, PSP, PCI, CFE. Director of Public Safety and Security, Williams Island Club and Property Owner's Association, Aventura, FL; University Adjunct Professor and Program Developer; former Deputy Administrator/Chief of Security, Wackenhut Corrections, Pompano Beach, FL; former Independent Security/Investigative Consultant/President, IntelQuest, Inc., Miami FL; former South Florida and Caribbean Regional Security Manager, McDonalds Corporation, Boca Raton, FL; former Miami-Dade County Police Officer and Detective, Miami, FL; former Corrections Officer, Michigan Department of Corrections, Plymouth, MI; former United States Air Force, Aircraft Armament System Specialist, Strategic Air Command, Wurtsmith AFB; member ASIS International, National Association of Chiefs of Police, Association of Certified Fraud Examiners, International Association of Protection Officers, Academy of Criminal Justice Sciences, and the National Fire Protection Association; Bachelor of Science in Criminology and Criminal Justice—Cum Laude, Eastern Michigan University; Master of Arts in Business and Organizational Security Management—Academic Honors; ASIS triple board certified in security management (Certified Protection Professional); physical security (Physical Security Professional), and investigations (Certified Professional Investigator); Certified in fraud examination (Certified Fraud Examiner) by the Association of Certified Fraud Examiners.

William R. McQuirter, CPO, CPOI. General Manager, Iron Horse Security, National Capital District, Ottawa, Ontario; former District Manager, Securitas Canada Limited, National Capital District, Ottawa, Ontario; former Security Manager, Digital Equipment of Canada Limited, Ottawa, Ontario; former Technical Services Manager, Atomic Energy of Canada Limited, Chalk River Nuclear Laboratories, Chalk River, Ontario; former President of Community Sentinels Company Limited, Ottawa, Ontario; former Police Officer, Ontario Provincial Police, Killaloe, Ontario; member of Algonquin College Security Management and Law and Security Program Advisory Council, charter member and Chairman of Ottawa Chapter of ASIS; former Regional Vice President of ASIS for Canada; member of CSIS; guest lecturer and presenter to RCMP, BOMA, CSIS and ASIS on various security related topics including Public and Private Policing; Certified Protection Officer Instructor with IFPO; member of Greater Ottawa Chamber of Commerce; author of a contract security article pertaining to public policing published in "Papyrus," a newsletter for the International Association of Museums and Galleries, Graduate of Law and Security, Ottawa, Ontario.

Adolfo Meana, Jr., Capt, USAF. Security Inspector, Defense Threat Reduction Agency (DTRA), Albuquerque, NM; former Chief of Concepts Division, Air Force Force Protection Battlelab, Lackland AFB, TX; former Operations Officer, 39th Security Forces Squadron (SFS), Incirlik AB, Turkey; lifetime member of the Air Force Association; Joint Service Commendation Medal with Oak Leaf Cluster; Air Force Commendation Medal with three Oak Leaf Clusters; Joint Meritorious Unit Award; Bachelor of Arts, Geography, University of Florida, Gainesville, FL.

Robert W. Miller, PhD. Dr. Miller has more than 20 years training and training development experience within Government and commercial sectors. In addition to serving as Advanced Systems Technology's Chief Knowledge Officer, he is currently serving as an Adjunct Professor and Corporate advisor at Cameron University, Lawton, Oklahoma. In that role he is providing instruction to undergraduate students in the application of distance learning technologies to governmental and commercial training situations. He is also advisor to the Multimedia Departments Curriculum committee. He has developed more than 40 computer-based training, web based training and performance improvement products. Dr. Miller holds a PhD in Instructional Psychology & Technology from the University of Oklahoma and a Master of Behavioral Science (Human Relations) from

Cameron University, Lawton, Oklahoma. Dr. Miller's publications and presentations include: *Keeping Captains "On Track": Support for the U.S. Army Combined Arms & Services Staff School Advanced Distance Learning Program (CAS3 ADL)*, Centra Summit 2004, Boston, MA, March, 2004 (co-authored with Daniel O. Pupek and Frank Colletti); *Internet-based Distance Learning: Implications of Emerging Technologies for Public Safety Training*, 2002, The Executive Forum, Illinois Law Enforcement Executive Institute 2(3), pp. 109–120; *The Shareable Content Object Reference Model (SCORM): A Primer for Small Businesses*, Oklahoma Distance Learning Association, *April* 2002 (co-authored with Dale Wheelis and Donald Aguilar); *Configuration Management for Web-Based Instructional Content*, Centra Summit '99, Boston, MA, October, 1999; *Integrating Environmental Tasks Into Job Performance*, National Association of Environmental Professionals, 1998 (co-authored with Barbara O'Keeffe); *Using Internet-Based Training to Integrate Environmental Compliance into Job Performance*, 1998, IX Congreso Internacional Sobre Tecnologia Y Educacion a Distancia, Consorcio Red De Educacion a Distancia, San Jose, Costa Rica; *Field Manual FM 20-400, Military Environmental Protection* (co-authored with Chris Conrad, Dave Neeley, Charles Okrassa, and Dana Merkoulov); *Training Circular TC 20-401, The Soldier and the Environment* (co-authored with Dana Merkoulov).

Richard L. Moe, CPP. Former Director of Assets Preservation for S&A Restaurant Corp., Dallas, TX; former Director of Assets Protection for Metromedia Steakhouses, Inc., Dayton, OH; former Security Manager for Argonne National Laboratories-West, Idaho Falls, ID; former Director of Security for Sambo's Restaurants, Inc.; Lieutenant Colonel, U.S. Army (Retired); member, American Society for Industrial Security; member, International Security Management Association; member, National Food Service Security Council (NFSSC); member, International Association of Chiefs of Police; Chairman, National Food Service Security Council; Chairman, Food Service Security Standing Committee, ASIS; Chairman, Santa Barbara Chapter, ASIS. Recipient of ASIS Standing Committee Chairman of the Year Award, recipient of NFSSC Award for Life Time Achievement in Food Service Security; Bachelor of Science, University of Arizona; and Master of Science, George Washington University.

John R. Morris. President, VIDEOTRONIX, Inc., Burnsville, Minnesota and Denver, Colorado; former Vice President of North American Video Corporation; member, American Society for Industrial Security International and Minnesota Association of Parking Professionals; author of "Plugging into the Systems," *Security Management*.

John A. Nolan, III, CPP, OCP, is a retired operational intelligence officer who served in Asia, Central Europe, and the U.S. During his 22-year career, his assignments included intelligence collection, counterintelligence and Special Operations projects. He co-founded the Phoenix Consulting Group in 1990, which provides CI collection and analysis, Competitive Assurance™ and professional development programs for client firms worldwide. Client firms range from the Fortune 50 to the Inc. 500, in electronics, utilities and telecommunications, defense and aerospace, manufacturing, food products, pharmaceuticals, and financial services. Government agencies in the U.S. and several allied countries also avail themselves of the expertise of the Phoenix cadre in efforts ranging from specialized training to studies and analyses. He and his firm have been profiled in many leading business journals, and he is a frequently invited guest speaker both here and abroad. He serves as adjunct faculty at the Defense Intelligence College and the University of Alabama. Multilingual, he received his undergraduate degree from Mount Saint Mary's College, and his graduate degrees from Central Michigan University and the University of Southern California. Military decorations include the Legion of Merit, Bronze Star Medal (2nd Oak Leaf Cluster), Air Medal, and numerous other commendation and service decorations from the U.S. and foreign nations. He has authored nearly one hundred articles and monographs, has contributed chapters to six different books, and has authored four books of his own. His professional affiliations include the Society of Competitive Intelligence Professionals (Member, Board of Directors and President), the Association for Psychological Type, American Society for Industrial Security (former chapter chairman and other offices), OPSEC Professionals Society (Member, Board of Directors), National Military Intelligence Association, and the Association of Former Intelligence Officers.

Robert L. Oatman, CPP retired as Major and Chief of Detectives from Maryland's Baltimore County Police Department. During his long and varied career, he acquired a broad range of training and experience in crisis management leadership, executive protection, and criminal investigation. He developed and commanded the first Hostage Negotiation Team formed in the State of Maryland, successfully concluding over 100 hostage taking incidents. United States Secret Service training provided the foundation of his executive protection skills, which he used to administer protective operations for a variety of local, national and international officials and dignitaries. His command of the Criminal Investigative Division gave Major Oatman the opportunity to utilize the investigative and management skills acquired during a distinguished 20-year career. Since entering the private sector, Bob Oatman has provided consulting advice, management services, expert protective and investigative support and training to multi-national corporations both in the United States and abroad. Frequently called upon to analyze standing executive protection operations, he has been responsible for restructuring major corporate security programs. He managed executive protection operations for NBC during the Olympic Games in Seoul, Korea in 1988, Barcelona, Spain in 1992, Atlanta, Georgia in 1996 and Sydney, Australia in 2000. An expert on protective operations, Mr. Oatman is the author of *The Art of Executive Protection* (Noble House, 1997) and co-author of *You're the Target*, (New World Publishing, 1989). He was also a contributing author to Volumes I and II of *Providing Protective Services*, (Winchester Printers, 1991–1994). Mr. Oatman holds a Bachelor of Science in Criminal Justice from the University of Baltimore and is a graduate of the FBI National Academy and the Federal Executive Institute. He is a Certified Protection Professional and long standing member of the American Society for Industrial Security, FBI National Academy Associates, American Society of Law Enforcement Trainers and the Maryland Chief's of Police Association.

Denis O'Sullivan, CPP. President and CEO of PPM 2000, Inc. Formerly Corporate Security Advisor to the City of Edmonton; Unit Commander, Alberta Highway Patrol; Special Branch detective with An Garda Siochana (the Irish National Police Force); Instructor University of Alberta; holds memberships in IACLEA, IAHSS, and ASIS International. With ASIS International, he held the positions of Chapter Chair, Regional Vice President, Trustee of the ASIS Foundation, member of the Professional Certification Board, member of the Board of Directors and International Vice President on the Executive Committee. Most recently served as the ASIS Senior Regional Vice President for International Development. Awarded the ASIS Canadian Region Pioneer Award and most recently received the Edmonton Chapter Chairman's Recognition Award.

Raymond Payne, CPP has 25 years experience in senior management for major Physical Security manufacturers. In these leading companies, he was responsible for product development and product management teams. Ray has been a visionary in new product solutions for physical security. In the capacity of product development, Ray has been involved in the design of security systems for major government facilities in Washington, as well as worldwide government organizations. He has been intimately involved in the requirements and design of many fortune 100 enterprise solutions. Some of the major contributions to the physical security market are first to introduce IP Video/Audio Security; integrated PC Security System; GUI interface for CCTV control systems; Solid State Cameras in CCTV Security; first to implement VPhase Switching in the industry, and numerous New Product awards through SIA, ASIS, etc. His areas of interest and expertise include transitioning facilities from analog to IP Video, evaluating existing security systems for flaws and/or improvements, IP Video and IP Audio, Video Object Processing (extracting intelligence from video and audio), integrating all aspects of Physical Security through AI to prevent security risks, solving challenging problems in Physical and IT Security, and dedicated to advancing the technology and solutions to Physical and IT Security. Mr. Payne has been intimately involved in the design of security systems for many facilities in the government and commercial sectors. Some of the government projects are the U.S. Capitol Building, White House, Secret Service Headquarters, CIA Headquarters, TVA, Panama Canal, FBI, and NSA. In the commercial sector he has worked with John Deere, Caterpillar, American Express, Apple Computer, and Compaq.

Kimberly L. Pfaff, BS, MA is the Director of Operations and Behavioral Sciences Department at Business Controls, Inc. She is responsible for managing the consultative and special investigations division relating to forensic psychology, as well as defining and enhancing the forensic assessment program to include pre-employment screening, fitness-for-duty evaluations, threat assessments, and police psychology. She has built a team of three forensic clinicians who actively assist and direct the above services. Ms. Pfaff often trains on workplace violence, substance abuse, and mental illness in educational and organizational settings. Ms. Pfaff is also responsible for the continual enhancement and management of the implementation and customer service program relating to the Anonymous Incident Reporting Systems provided by BCI, as well as directly training and monitoring the call center representatives responsible for handling MySafeWorkplace calls. Ms. Pfaff is currently working toward her doctorate in Clinical Psychology at The University of Denver. Ms. Pfaff received a Bachelor of Science in psychology with a minor in biology from Indiana University. She received a Master of Arts in forensic psychology from the University of Denver. She completed a 12-month clinical internship at The Federal Correctional Institute (FCI) in Englewood, Colorado. From this prison environment, she brings specialized knowledge concerning the psychological functioning of the criminal mind, conflict management and resolution, life-skills training, and suicide and crisis intervention. Ms. Pfaff worked as part of the psychology team that engaged daily with medium-to-high security male inmates. Her clinical duties included pre-screening (consisting of clinical interviews and/or cognitive and personality assessments) of new inmates, individual therapy (cognitive-behavioral in nature), and group therapy (stress management and relaxation training). Other duties included formulating treatment plans for chronic care patients and making referrals to health services for possible psychotropic medications. Ms. Pfaff's previous clinical experiences include working as a victim's advocate in the Douglas County Probation Department in Castle Rock, Colorado. Working as a liaison between perpetrators and their victims, she informed victims of current changes in perpetrator status and answered questions pertaining to the criminal justice system. Ms. Pfaff also worked as a co-facilitator of male domestic violence perpetrator groups, providing therapy and assessment of their psychological needs through testing and interviewing. Ms. Pfaff's professional affiliations include: American Psychological Association, ASIS International, and the Association of Threat Assessment Professionals.

Philip P. Purpura, CPP. Director, Security and Criminal Justice Institute, Florence-Darlington Technical College, Florence, SC; Expert Witness; Security Consultant; former Security Manager and Investigator; member, Academic Programs Council, American Society for Industrial Security; master of Science, Criminal Justice, Eastern Kentucky University; and Bachelor of Science, Criminal Justice, University of Dayton; author of *Terrorism and Homeland Security: An Introduction with Applications* (2006), Elsevier Pub.; *Security & Loss Prevention: An Introduction*, 5th Edition (2007), Elsevier Pub.; *Security Handbook*, 2nd Edition (2002), Delmar, Butterworth-Heinemann Publishers; *Police & Community: Concepts and Cases* (2001), Allyn & Bacon; *Criminal Justice: An Introduction* (1997), Butterworth-Heinemann Publishers; *Retail Security & Shrinkage Protection* (1993) Butterworth-Heinemann Publishers; and *Modern Security & Loss Prevention Management* (1989), Butterworth-Heinemann Publishers.

James T. Roberts, Jr., CPP, CFE. United States Marshal, United States Marshals Service, Savannah, GA; former Director, Criminal Justice Technology Studies, Augusta Technical College; former adjunct instructor in Criminal Justice, Augusta State University; former adjunct instructor, Security Management Studies, Park College; former security and emergency management consultant, Odgen Environmental and Energy Services; former emergency management consultant, Westinghouse Savannah River Company; former emergency preparedness planner, Advanced Systems Technology; former senior staff member, security protection team, Science Applications International Corporation; former law enforcement management consultant; former director of law enforcement and security, U.S. Army Medical Command; former district commander, director of investigative operations, and deputy commander, U.S. Army Criminal Investigation Command; former physical security staff officer, Office of the Chief of Army Law Enforcement; former team member and designated team chief, Commission on Accreditation for Law Enforcement Agencies; numerous presentations on emergency

management and security subjects; former book manuscript reviewer, Butterworth-Heinneman, publisher; author, Military Policeman's Handbook (three printings), Tuttle, publisher; numerous articles for professional journals; Master in Education, Georgia Southern University, Bachelor in Public Administration, Virginia Tech University; former member, Professional Certification Board, former Regional Vice President and Chapter Chairman, American Society for Industrial Security; member, education and training committee, International Association of Chiefs of Police, former member, Board of directors, International Foundation of Protection Officers; member, American Society for Law Enforcement Trainers; board-approved Certified Protection Professional; Certified Fraud Examiner.

Lester S. Rosen is an attorney at law and President of Employment Screening Resources, a national background screening company located in California. ESR was rated as the top screening firm in the U.S. in the first independent industry study. He is the author of *The Safe Hiring Manual—Complete Guide to Keeping Criminals, Impostors, and Terrorists Out of Your Workplace*, Facts on Demand Press, the first comprehensive book on employment screening. He is also the author of the first professional development education course on safe hiring and background screening, including 30 hours of online training. He is also a consultant, writer, and frequent presenter nationwide on pre-employment screening and safe hiring issues. He has qualified and testified in the California and Arkansas Superior Courts as an expert witness on issues surrounding safe hiring and due diligence. His speaking appearances have included numerous national and statewide conferences. He is a former deputy District Attorney and criminal defense attorney and has taught criminal law and procedure at the University of California Hastings College of the Law. His jury trials have included murder, death penalty, and federal cases. He graduated UCLA with Phi Beta Kappa honors, and received a JD degree from the University of California at Davis, serving on the Law Review. He holds the highest attorney rating of AV in the national Martindale-Hubbell listing of American Attorneys. He is also a licensed Private Investigator in California. Mr. Rosen was the chairperson of the steering committee that founded the National Association of Professional Background Screeners (NAPBS), a 400-member professional trade organization for the screening industry. He was also elected to the first board of directors NAPBS and served as the co-chairman in 2004.

Charles A. Sennewald, CPP, CSC, CPO. Independent Security Management Consultant in Esco-ndido, CA; former Security Director for the Broadway Department Stores; former Chief of Campus Police, Claremont, CA; former Deputy Sheriff, Los Angeles County; former assistant Professor at California State University at Los Angeles; founder and first President, International Association of Professional Security Consultants (IAPSC); and former Standing Committee Chairman and member of the American Society for Industrial Security; recipient of *Security World* magazine's Merit Award and the IAPSC'S Distinguished Service Accolade; twice designated by the U.S. Department of Commerce as the Security Industry Representative on missions to Sweden, Denmark, Japan, China, and Hong Kong. Bachelor of Science, California State University at Los Angeles; author of various Butterworth-Heinemann-Elsevier books: *Effective Security Management*, 4th Edition, *The Process of Investigation*, 3rd Edition, *Security Consulting*, 3rd Edition, and *Shoplifting*. In production at the time of this writing is one ASIS book: *Shoplifting: Managing the Problem*.

Amy L. Slettedahl, BA, MA. Forensic Clinician on the Behavioral Sciences Team at Business Controls, Inc. and is responsible for helping in the development and expansion of forensic psychology related services, including assessment and training. She is also a senior coordinator of special investigations and undercover investigations, respectively. Additionally, Ms. Slettedahl manages client accounts for both MySafeWorkplace and MySafeCampus systems at Business Controls, Inc. (BCI). Ms. Slettedahl has been employed at BCI for two years and is responsible for training and managing high-caliber organizations prior to, during, and following implementation of anonymous incident reporting systems for the MySafeWorkplace and MySafeCampus. Ms. Slettedahl is a contributing editor for *Security Newsletters*, published by Business Controls, Inc. She obtained a Bachelor of Arts in psychology, with an emphasis in legal studies in 2002 from the University of Northern Colorado, and

graduated with a Master of Arts in forensic psychology at the University of Denver in 2005. She completed a nine-month clinical internship with the Colorado Department of Corrections at the Denver Women's Correctional Facility (DWCF) in Denver, Colorado. Her clinical interaction with substance abusing female offenders as well as acute mentally ill offenders gives her specialized knowledge in the psychological functioning of the female criminal mind and addiction. Ms. Slettedahl was trained in the assessment and evaluation of substance abusing offenders, made treatment recommendations for incarcerated offenders, and facilitated a cognitive-behavioral/psychoeducational group with special-needs offenders. Her other clinical duties included assisting in the determination of risk/custody levels for incoming offenders, formulating community based treatment recommendations for the parole board and working with perpetrators and victims of sexual abuse. Ms. Slettedahl has specialized training in disaster response and has also worked at an inpatient, locked psychiatric facility in Greeley, Colorado. She co-facilitated inpatient treatment groups, monitored psychotropic medications and related effects, and developed discharge treatment plans. Ms. Slettedahl's professional affiliations include: Psi-Chi, National Honor Society in Psychology, and she is a Board Member for the Association of Threat Assessment Professionals (ATAP)-Colorado Chapter.

Don Sturgis, CPP. Physical Security Consultant; Senior Consultant, Ray Bernard Consulting Services; former Product Manager, Cardkey Systems, Simi Valley, CA; former Director of Marketing–Access Control Products, American Magnetics Corporation, Carson, CA; former Manager, Product Management, Rusco Electronic Systems, Inc., Glendale, CA; member, American Society for Industrial Security; Chapter Treasurer, California Inland Empire Chapter of ASIS; Mentor, ASIS Region III CPP Review Class; 2005 Recipient, Minot Dotson Award, ASIS Region III; Omicron Delta Kappa Honor Society and Student Body President, American University, Washington, D.C. Specialist, 3rd Class, U.S. Army, Scientific and Professional Program, Army Ballistic Missile Agency, Huntsville, AL; Bachelor of Arts, American University, Washington, D.C.; Master of Science and Master of Business Administration, West Coast University, Los Angeles, CA; co-inventor on three patents: bi-directional communication protocol used between computer systems and intelligent terminals; degraded mode operations for card readers; and self-contained programmable terminal for security systems; articles published in *Access Control & Security Systems Magazine*: "Product Overview—Magstripe Access Cards Attract Users," and "Security Technology Defeats Vehicle Theft and Driver License Fraud in Mexico," plus an eight-part series of articles on security system testing.

Kathleen M. Sweet is currently an Associate Professor in the Department of Aviation Technology at Purdue University, where she teaches courses in Aviation Security, Terrorism, and Strategic Intelligence. She is CEO and President of Risk Management Security Group, and is certified by the UK and Irish Department of Transport to teach air cargo security. Dr. Sweet received her undergraduate degree from Franklin and Marshall College in Lancaster, Pennsylvania, in Russian Area Studies and she has a Master's Degree in history from Temple University. She also has been admitted to the bar in Pennsylvania and Texas after graduating from Beasley School of Law, and Temple University in Philadelphia, PA. She is a graduate of many Air Force and civilian training programs. After graduating from law school, Dr. Sweet joined Wyeth International Pharmaceuticals as a legal specialist focused on licensing agreements between Wyeth and international agencies. She later joined the U.S. Air Force and initially was a member of the Judge Advocate General's (JAG) Department. She frequently served as Director of Military Justice at the Base and Numbered Air Force level. After 15 years as a JAG officer, and generally engaged in prosecuting cases on behalf of the military, she transferred to the 353rd Special Operations Wing as a military political affairs officer. She was later an intelligence officer assigned to HQ AMC as an executive officer and briefer. In 1995, she became an Assistant Air Attaché to the Russian Federation. As an attaché, she was engaged in liaison work not only with the Russian Air Force but also the Federal Security Bureau, at which time she became interested in counter terrorism efforts. Her final Air Force assignment was as an instructor at the Air War College where she taught in the International Security Studies division. She later became an Associate Professor at St. Cloud State University in the Department of Criminal Justice and an Associate Professor at Embry Riddle Aeronautical University, teaching security and intelligence related courses. She is the author

of four books: *Terrorism and Airport Security*, Edwin Mellen Press, March 2002; *Aviation and Airport Security: Terrorism and Safety Concerns*, Prentice Hall Publishers, November 2003; *The Transportation Security Directory*, Grey House Publishing, January 2005; and *Transportation and Cargo Security: Threats and Solutions*, (Prentice Hall Publishers, August 2005). She is considered an expert in the field of airport, aviation, and air cargo security and has been well published in the fields of international space programs and associated treaties, space based offensive weapons, bio-terrorism, and aviation security. Her company, Risk Management Security Group (RMSG), doing business in Ireland as RMSG Ireland Ltd., engages in all aspects of consulting in transportation-related security including the preparation of threat and vulnerability assessments and security awareness training. As CEO of RMSG, she is certified by the United Kingdom and Irish Department of Transport to teach air cargo security. RMSG and RMSG Ireland Ltd. engage in all aspects of consulting in transportation-related security, including the preparation of threat and vulnerability assessments and security awareness training. She is the author of *Terrorism and Airport Security; Aviation and Airport Security: Terrorism and Safety Concerns; The Transportation Security Directory;* and *Transportation and Cargo Security: Threats and Solutions*. She has been well published in the fields of international space programs and associated treaties, space-based offensive weapons, bio-terrorism, and aviation security.

Peter E. Tarlow, PhD. Expert specializing in the impact of crime and terrorism on the tourism industry, event risk management, tourism, and economic development; PhD in sociology from Texas A&M University. Teacher of courses on crime and terrorism and tourism development; security consultant to numerous U.S. government agencies such as U.S. Bureau of Reclamation, U.S. Customs Service, U.S. National Park Service, and U.S. Bureau of Prisons; lecturer at major universities around the world. Consultant to the Royal Canadian Mounted Police, United Nation's WTO (World Tourism Organization), and the Centers for Disease Control and Prevention; speaker throughout North and Latin America, the Middle East and Europe on the sociology of terrorism, its impact on tourism security, and risk management; trainer of numerous police departments throughout the world on TOPS (Tourism Oriented Policing Skills); publisher of numerous academic and applied research articles, books, and chapters of books on security; writer and publisher of "Tourism Tidbits," an electronic newsletter on tourism and travel that appears in English, Spanish, and Turkish editions; contributor to the joint electronic tourism newsletter (ETRA) that is published jointly by Texas A&M University and the Canadian Tourism Commission; writer and publisher of numerous professional reports for U.S. governmental agencies and for businesses throughout the world. Guest on nationally televised programs such as Dateline: NBC and Dateline: CNBC; organizer of conferences around the world dealing with visitor safety and security issues. Founder and President of Tourism & More Inc. (T&M).

Eugene L. Tucker, CPP, CFE, CBCP. President, Praetorian Protective Services® LLC, Orinda, CA; Senior Consultant, The Steele Foundation; former Security and Safety Manager for several High Technology and Biotechnology Fortune 500 companies; former West Coast Practice leader for Minet Insurance Services; former coordinator of the Emergency Management program at Santa Clara University; former Director of Student Services and Head Professor for the Security and Investigations program at Barclay College, former Associate Manager for Global Business Continuity Planning, The Clorox Services Company. Mr. Tucker has appeared as a security expert in TV news interviews and was commended by the City of Berkeley, CA. Member, Physical Security Committee, American Society for Industrial Security; Board of Directors, Business Recovery Managers Association; High Technology Crime Investigation Association, Association of Certified Fraud Examiners; California Emergency Services Association; co-author of the second and third editions of *Risk Analysis and the Security Survey* by James F. Broder, CPP, CFE, ACFE, Butterworth-Heinemann; contributing author to the *ASIS Professional Practices* book, and has been quoted in, and written articles for *Security Management Magazine*.

Karim H. Vellani, CPP, CSC. Independent Security Consultant and President, Threat Analysis Group, LLC, Houston, TX; Adjunct Professor, College of Criminal Justice, Security Management Department, University of Houston—Downtown. Member, American Society for Industrial Security International

(ASIS), International Association of Professional Security Consultants (IAPSC), International Association of Crime Analysts (IACA); Professional Certification Committee Chairman for IAPSC; and Certifications Chairman for the Houston, TX, Chapter of ASIS; former CPP Chairman for Houston, TX, Chapter, of ASIS and Director of the Board for IAPSC; Bachelor of Criminal Justice, Sam Houston State University and Master of Criminal Justice Management, Sam Houston State University; author of *Applied Crime Analysis* and numerous articles, white papers, and case studies on crime analysis, threat assessment, and risk management; board certified in Security Management by ASIS; Board Certified as an Independent Security Consultant by IAPSC; and licensed as a security consultant.

Scott A. Watson, MCJ, MEd, CPP, CFE. Principal Consultant & CEO, S.A. Watson & Associates LLC, Dover NH; Executive Director, Christian Emergency Response Volunteers (CERV), Dover, NH; Adjunct Professor, Boston University, Metropolitan College, Boston MA. Adjunct Professor, American Military University, Charles Town, WV: Physical Security Specialist, TD Banknorth Corporate Security, Bedford, NH; Senior Risk Management Analyst, Liberty Mutual, Regional Area Markets, Keene, NH; Security Manager, Liberty Mutual, Special Operational Services, Boston, MA: Investigative Analyst, Fidelity Investments Corporate Security, Boston MA, Business Security Representative, Fidelity Investments Corporate Security, Boston, MA; Senior Security Representative, Fidelity Investments Corporate Security, Boston, MA; Security Representative, Fidelity Investments Corporate Security, Boston, MA: Investigator, Pinkerton Security & Investigations, Burlington, MA:, Security Officer, Pinkerton Security, Boston, MA. Senior Security Officer, Boston University's Mugar Memorial Library, Boston, MA; Security Officer, First Security Services Corporation, Boston, MA. Editorial Chairman of the ASIS Crisis Management Council, Member of the Association of Certified Fraud Examiners, Member of the New England Disaster Recovery Information Exchange (NEDRIX); Frequent speaker at professional conferences including ASIS Annual Seminar, ASIS Crisis Management Workshops, City of New York Employee Emergency Preparedness Manual Workshop, CPM East and NEDRIX. Bachelor's Degree in Political Science, Long Island University, Southampton, NY: Masters Degree in Criminal Justice Administration, Boston University, Boston, MA; Masters Degree in Education/ Instructional Design, University of Massachusetts, Boston, MA; Author of *A Lesson in Training*; Security Management October 2002; Author of *Buildings with Bull's–Eyes*, Contingency Planning & Management, 2 Part Series-July/August & September/October Issues 2003; Author of *Emergency Preparedness in Nine Steps*, Continuity Insights, March/April Issues 2004; Author of: *How To Steer Your Company to Emergency Preparedness*, Continuity Insights, May/June Issue, 2004.

James J. Zirkel, Maj, USAF. Security Inspection Team Chief, DTRA, Albuquerque, NM; former Operations Officer, 377 SFS, Kirtland AFB, NM; former Chief of Security, 425th Air Base Squadron, Izmir AB, Turkey; former Missile Field, Convoy, and Training and Resources Flight Commander, 91 SFS, Minot AFB, ND; 2005 Air Force Commander-in-Chief's Special Recognition Award winner; 2004 DTRA Field Grade Officer of the Year award winner; Meritorious Service Medal with one Oak Leaf Cluster; Air Force Commendation Medal with one Oak Leaf Cluster; Joint Service Achievement Medal with one Oak Leaf Cluster; Air Force Achievement Medal with two Oak Leaf Clusters; Army Achievement Medal; Bachelor of Science, Economics, United States Air Force Academy, CO; Master of Arts, Security Management, Webster University, St. Louis, MO.

Dick Zunkel. Mr. Zunkel has been involved with electronic locking and access control systems since their development in the 1960s. He was a product designer and later an Engineering Manager in the builders' hardware industry. In the early 1980s he was General Manager of two start-up companies specializing in design-built door automation and access systems. He joined Recognition Systems, Inc. in Campbell, CA in 1995 where he was involved in sales of access controls in domestic and international markets. He is currently a security consultant with Ingersoll Rand Security Technologies in Pleasanton, CA. He wrote the chapter on hand geometry and access control in the book *Biometrics, Personal Identification in Networked Society*, published by Kluwer Academic Publications. His articles on locks, hardware, access control and biometrics appear frequently in trade journals.

Foreword

The security industry, aside from a handful of 19th century private sector investigators performing limited protective functions, didn't really come into its own until World War II, with the need to protect the war industry. Security was more commonly called "plant protection" and was an operational function, a process relatively restricted to "guarding" facilities and their contents, including war-related secrets. Following the war, the need for protection continued to grow in our industrialized society and the name evolved from plant protection to industrial security. In 1955 the American Society for Industrial Security was founded, adopting a name which generally reflected the industry's heritage, i.e., industrial.

One essential element of a "profession" is the presence of scholarly works, namely books. The earliest book on security I can find is titled *Practical Plant Protection and Policing*, written by G.W. Gocke for Charles C. Thomas Publishers in 1957, which was identified as a Monograph in *The Police Science Series*, edited by V.A. Leonard, a professor of Police Science and Administration at Washington State College. This is important because university undergraduate degree programs were emerging in this same period, which resulted in security being relegated to the backwaters in favor of a growing recognition of "police science," later to be named "criminal justice" degrees. Charles C. Thomas captured the public sector police book market and also recognized the growing security market in the private sector; as a result, *Modern Retail Security*, by S.J. "Bob" Curtis, was published in 1960. A few more security books found their way into print during that decade, but it wasn't until the 1970s that the security industry started to emerge as a true and rewarding profession. It was then that Security World Publishing Company, a division of Security World Magazine, came on the scene dedicated to publishing books for the industry.

The books during that decade included such works as Berger's *Industrial Security*, Carson's *Managing Employee Honesty*, Buzby & Paine's *Hotel & Motel Security Management*, and Blackwell's *The Private Investigator*, to name a few.

The management of people, as a unique and separate discipline, was not the focus of the industry. It was industry performance standards in the nuts and bolts of security as it related to specific environments, institutions, and enterprises that were in demand, and it wasn't until the late 1970s that the first purely *management* book was published.

With the growth of the security industry came the growing need not for security technicians but for the management of those technicians.

In the following decades, quality books on virtually every security-related topic imaginable have been produced, enhancing and upgrading our industry.

Then, in 1993, along comes John J. Fay with his *Encyclopedia of Security Management*, which immediately became recognized as an abbreviated synthesis of all our earlier works. I view his work as one of the leading contributions to the ever-growing professionalization of our industry, and this newly revised, enhanced, and expanded second edition is equally, no, more important than the original. One man, one author, John Fay, has captured and presented many voices sharing their views of our business for the edification of us all! No other singular work can be of greater value to the effective security manager of today.

Charles A. "Chuck" Sennewald, CPP, CSC, CPO
Security Management Consultant and Author

Preface

The security field continues to evolve rapidly, becoming broader and more complex with each passing year. The single common thread tying the field together is the discipline of management. This book is for and about security managers, the practitioners whose innovativeness and energy are fueling the great changes of our age.

Security management must be applied wherever protective effort is to be organized on a significant scale—in government, the military, or the business sector. The security manager in one arena can take advantage of technical advances in other arenas when the advances have been described in a useful format. This book is dedicated to that purpose.

The product of rapid evolution is specialization, which can be both positive and negative. The manager who specializes in computer security, for example, may possess great knowledge about electronic data bases but not know very much about the behavioral sciences or the traditional management functions. While this can be accepted as the price tag of progress, it presents a real problem in a discipline committed to control, direction, and elimination of complexity.

As specialization increases, the generalists decline—not because they are unneeded, but because the broadening opportunities are not present in the workplace. The usual experience of a security practitioner is to spend formative years in a relatively specialized area, such as supervising contract guard services, conducting investigations, or installing alarm systems. When promoted to a managerial level, the individual brings to the new job a limited, one-dimensional viewpoint. Saddled with enlarged responsibilities that call for proficiency in many aspects of managing, the individual is suddenly in a sink or swim situation. Some survive, in a sense overcoming the weight of specialization, to become generalists. The few that reach the very top often owe their success to personal efforts on a grand scale. We observe that these are individuals who have acquired a broad understanding of the profession and have developed strong skills in planning, organizing, directing, and controlling.

Continuous learning is required of a security manager who is determined to stay current. The area of electronic technology, with myriad security applications, has practically exploded in recent years. At the same time, steady advances have been made in the time-honored ways that human and financial resources are harnessed to the work of security organizations. The professional security practitioner needs an authoritative reference source to keep abreast.

This encyclopedia offers to the aspirant, student, or practitioner, whether at the entry or senior executive level, a collection of authoritative information that impinges directly upon the security management function as it is performed in many different industries. It proposes, for example, to make the novice aware of the opportunities that are presented in the diverse nature of security jobs; to make the retail store investigator aware of cash register auditing techniques used by his or her counterpart in the lodging industry; to make the electronic access control designer aware of group dynamics; to make the consultant knowledgeable about finance; and to give the top security executive improved insights into the work of the front-line technicians. In addition, this book endeavors to make all security practitioners aware of the truly remarkable strides that have been made in electronic technology, the forensic sciences, human motivation, and the like.

Authoritativeness has been assured by the professional standing of the individual contributing authors. The editor's contacts with professionals engaged in the subjects presented have made possible original contributions by leading authorities. In many cases, a contributing author is also the author of a recognized text or is a frequent contributor of articles to the security trade magazines and professional journals.

To the extent feasible, the authors have followed a prescribed editorial formula designed to tell the reader what the topic is all about, how it works, what it does, how it is used and the problems it solves or creates. A reader who has no substantive knowledge of a topic will, after referring to the article, obtain the basics, i.e., purpose, objectives, modes of operation, and scope. A reader whose education and experience provide at least a peripheral understanding of a topic will gain an appreciation of the potentials for applying the information to the reader's own job, business, or industry.

John J. Fay

I: Business Principles

AGE DISCRIMINATION

The Age Discrimination in Employment Act of 1967 (ADEA) protects individuals who are 40 years of age or older from employment discrimination based on age. The ADEA's protections apply to both employees and job applicants. Under the ADEA, it is unlawful to discriminate against a person because of his/her age with respect to any term, condition, or privilege of employment, including hiring, firing, promotion, layoff, compensation, benefits, job assignments, and training.

It is also unlawful to retaliate against an individual for opposing employment practices that discriminate based on age or for filing an age discrimination charge, testifying, or participating in any way in an investigation, proceeding, or litigation under the ADEA. The ADEA applies to employers with 20 or more employees, including state and local governments. It also applies to employment agencies and labor organizations, as well as to the federal government. ADEA protections include:

Apprenticeship Programs

It is generally unlawful for apprenticeship programs, including joint labor-management apprenticeship programs, to discriminate on the basis of an individual's age. Age limitations in apprenticeship programs are valid only if they fall within certain specific exceptions under the ADEA or if the EEOC grants a specific exemption.

Job Notices and Advertisements

The ADEA generally makes it unlawful to include age preferences, limitations, or specifications in job notices or advertisements. A job notice or advertisement may specify an age limit only in the rare circumstances where age is shown to be a "bona fide occupational qualification" (BFOQ) reasonably necessary to the normal operation of the business.

Pre-Employment Inquiries

The ADEA does not specifically prohibit an employer from asking an applicant's age or date of birth. However, because such inquiries may deter older workers from applying for employment or may otherwise indicate possible intent to discriminate based on age, requests for age information will be closely scrutinized to make sure that the inquiry was made for a lawful purpose, rather than for a purpose prohibited by the ADEA.

Benefits

The Older Workers Benefit Protection Act of 1990 (OWBPA) amended the ADEA to specifically prohibit employers from denying benefits to older employees. Congress recognized that the cost of providing certain benefits to older workers is greater than the cost of providing those same benefits to younger workers, and that those greater costs would create a disincentive to hire older workers. Therefore, in limited circumstances, an employer may be permitted to reduce benefits based on age, as long as the cost of providing the reduced benefits to older workers is the same as the cost of providing benefits to younger workers.

Waivers of ADEA Rights

An employer may ask an employee to waive his/her rights or claims under the ADEA either in the settlement of an ADEA administrative or court claim or in connection with an exit incentive program or other employment termination program. However, the ADEA, as amended by OWBPA, sets out specific minimum standards that must be met in order for a waiver to be considered knowing and voluntary and, therefore, valid. Among other requirements, a valid ADEA waiver must:

- Be in writing and be understandable.
- Specifically refer to ADEA rights or claims.
- Not waive rights or claims that may arise in the future.
- Be in exchange for valuable consideration.
- Advise the individual in writing to consult an attorney before signing the waiver.

- Provide the individual at least 21 days to consider the agreement and at least seven days to revoke the agreement after signing it.

If an employer requests an ADEA waiver in connection with an exit incentive program or other employment termination program, the minimum requirements for a valid waiver are more extensive.

Source The U.S. Equal Employment Opportunity Commission. 2006. <http://www.eeoc.gov/types/age.html>

BEST PRACTICES

Pursuing quality requires making a commitment to doing things in the best possible way. In today's organizational environment we would call this "pursuing best practices." But what does this mean exactly? To properly understand the context of best practices we need to consider three fundamental realities:

- There are no absolute criteria for defining best practices within security today.
- Best practices do not have to be measurable by empirical means.
- Best practices can be common practices.

On the surface, each of the three considerations appears to fly in the face of the very essence of what best practices should be all about. Yet ironically all three embody the very essence of best practices for a security manager. Let's examine each briefly.

First, security is a non-codified profession. Unlike corporate safety with its guidelines as set forth by underwriters and regulators, the security industry has not subscribed to a set of standards. Consequently, security professionals are pretty much driven by the codes of other professional business counterparts, an occasional state requirement, an underwriter prescription, or a court decision.

Even though there may be no prescribed, empirical criteria for measuring the attainment of best practices, decision makers can determine if they are on the right track when such practices:

- Directly contribute to the bottom line.
- Add value in a demonstrable way.
- Maximize efficiency and effectiveness.

Established practices can become best practices. For example, requiring employees to display a photo identification badge is an established practice that is not always done well. When an organization enforces the established practice by use of a system of incentives and disincentives, and when statistical evidence shows that the practice contributes to cost savings, such as preventing theft, the common practice becomes a best practice.

A security manager can evaluate security practices by asking a simple question: "Am I getting the job done?" If the security manager's responsibilities include criminal investigations, the evaluation criteria can be how quickly the investigation was completed, whether the investigation succeeded in solving a crime or correcting a crime condition, the cost of the investigation, recovery of property, and a settlement from or restitution made by the offending party. In looking at the totality of investigations, the security manager can compare total costs against total recoveries and also use historical data to demonstrate that crime-related losses in previous years were higher than crime-related costs currently.

Challenging Basic Assumptions

Are the common assumptions associated with staffing levels and deployment, allocation of security systems and devices, and operating practices relevant in today's organizational culture? Or are there other opportunities available to be pursued that will yield the same result at a lower cost while actually maintaining or increasing the quality of the service delivered? As an example, with respect to criminal investigations, is it better to create a prosecutorial threshold (that is, no loss under an established value will be criminally pursued) rather than using civil litigation as a means of seeking appropriate remedies for all losses? By establishing such thresholds, both the manner in which investigations are pursued and the allocation of resources could vary significantly. Only those incidents involving a loss equivalent to a significant monetary value would be pursued from a criminal perspective, and those investigations would require an adherence to a higher standard of

investigational pursuit. It is important to note that the best practice here is the establishment of a value threshold. The actual value you establish will vary depending on the type of organization and value of the assets.

Allocating Staff Resources

To "get the job done" how many staff people do you require? This is much different from the traditional approach of seeking authorized levels based on "the great what-if." Security executives, like many of their counterparts in other service-related industries, have traditionally defined levels above what is actually required. They want "the coverage." Usually they justify this judgment by pointing to their ability to provide a more rapid response or by giving the assurance that selected posts will not be left open. Unfortunately, neither of these "justifications" falls within the definition of services as "required."

Employing best practices means analyzing what it takes to meet the routine assigned tasks and then creatively identifying strategies to accomplish the non-routine incidences. To address the issue of rapid response, you may need to develop a mutual response program with neighboring facilities or organizations, similar to what is done in the public sector.

Using Appropriate Technology

Accomplishing most assigned security tasks requires the use of some technology. Against the backdrop of today's continuum of available security devices, it is easy to fall into the trap of believing that the more sophisticated and electronic the security device is, the better it is. The best practice approach speaks to addressing the problem at hand with the technological resource commensurate with resolving the need. If a simple mechanical lock and key can suffice to prevent unauthorized access into an area, as opposed to an electronic card-access system, then the use of the lock and key should be pursued. Though locks and keys may not be as "sexy" as access cards and electronic readers, there are applications where locks and keys are more cost-effective and, therefore, demonstrate a commitment to quality assurance and best practices.

Conversely, attempting to address a security issue using outmoded technology when state-of-the-art devices are available is equally inappropriate. An example would be the use of radio frequency controlled closed-circuit television surveillance systems as opposed to hard-wired configurations in selected applications. The wireless devices may be more expensive initially, but the cost of installing the wiring (that is, across parking lots, in marina locations, and so forth) for the other configuration may be more.

Challenging Basic Operating Practices

To get the job done using best practices also requires that the decision maker (e.g., generally the manager) challenge basic operating practices, especially when the common response from employees is "We've always done it this way." The best of a best practices approach recognizes that employing security's operating procedures is often the most effective and least costly way of accomplishing the security mission. By shifting the responsibility for good security practices to end users, the security management team is able to redirect limited resources to other areas requiring specific attention. Meanwhile, business unit managers and non-security employees can not only be held accountable for the security and safety of those assets charged to them, but also share in the knowledge that they have promoted the well-being of their colleagues.

Is the Service Being Delivered Effectively?

Best practices demand that the intended results be achievable. A gap can lie between what senior management expects and what the security manager can deliver. To eliminate the gap, or at least keep it from widening, the security manager has to be in tune with the expectations of senior management and the overall corporate culture. Determining what their perception of effectiveness is and how this translates into security's service delivery is critical. Not only must the end result be clearly defined by security best practices but it must also be perceived by senior management as being in accordance with cultural values. All too often the result is accomplished, but the methodology or personalities involved have

alienated enough key players so as to render the actual results less obvious.

Best practices means looking for new ways to be effective. In using this strategy you assume nothing is so sacred that it cannot be improved upon—even if it means taking radical action. An example is the 180-degree rule. It says that effectiveness can be improved by approaching the problem from exactly the opposite direction. Often we find that by simply looking at the problem from a different perspective, an answer will arrive and it turns out to be better than what we might otherwise have come up with through conventional evaluation.

Is the Service Being Delivered Efficiently?

Efficiency is often synonymous with cost. Whether cost is measured in terms of time, dollars, or both, the hard fact is that dollars are spent to achieve results. Efficiency naturally translates into bottom-line performance. The best practices approach involves obtaining the best possible value in exchange for the "best" dollars spent. By definition, efficiency means "the best way of doing something in the best utilization of time." Time, of course, equates to cost such as paying people to do a job that should have been finished in a lesser period of time.

Pursuing Best Practices

Do One Thing Well. One of the myths about pursuing best practices is that to be a world-class organization all your departmental activities must be carried out from a best practices perspective. The pursuit of best practices is evolutionary. It begins with concentrating on one particular activity and doing it very well. As you develop a best practices proficiency in any one area, the lessons learned can then be carried over to other areas. In time, if you pursue best practices diligently, several, if not all, aspects of your security program will be classified as best practices.

Leverage the Good, the Bad, and the Ugly. While there are many ways to measure the activities in your organization, it is not uncommon to describe tasks as those being done well (the good); those that were initially good but for any number of reasons have failed (the bad); and those that seem to "get the job done," but you're mystified about how it is accomplished (the ugly). Regardless of a particular outcome, there are lessons to be learned. The astute manager maintains the broad-based perspective and seeks to find the opportunities in each situation.

Develop and Maintain Employee Loyalty. In addition to empowering people, there are other techniques you can use to build employee loyalty, particularly when third-party providers are involved.

- Develop a "we will" package. Items to be included might be a packet for newcomers including coupons for discounts offered by the company, a WELCOME ONBOARD card signed by other employees, a company T-shirt, a certificate suitable for framing or a plaque for posting, promoting the idea of the employee belonging to the company family, and so forth.
- Recognize a security officer and his or her contribution with a gift certificate for $50 at Christmastime either to the nearest toy store to be spent on the officer's children or to a nearby department store.
- Give a gift certificate for two to the security officer to a local medium-priced restaurant. Include an extra $15 to $20 for babysitting money for those officers with children to assure that they will be able to take advantage of the gift certificate.
- Allow employees to leverage on your volume discounts for the laundering and dry cleaning of their uniforms by offering them discounted fees for the care of items in their personal wardrobes.
- Extend employee award programs to staff members normally not eligible, such as administrative staff and security branch officers, as a way of recognizing their support and contribution to the security program.
- Pay officers for as many as two hours per month for helping in community school activities or other charitable work programs.
- Create employee support groups, such as parents with teenagers, dealing with aging, and so forth.
- If security vehicles are used, stencil the name of the security officer of the year on the side of his or her vehicle.

These are all small examples of affordable options, yet they demonstrate to employees that management is willing to make an investment in them. Such gestures allow employees, proprietary or contract, to develop a measure of loyalty because they get a feeling of both acceptance and respect for the contribution they are making.

Quality Should Be Cultural—Not Supplanted. Quality, and therefore the pursuit of best practices, is not something that can be forced on an organization. It is something that is embraced naturally by both management and line staff. For them quality is a matter of identity and not just the latest management fad.

"We've Always Done It That Way" Is Changed to "We've Never Done That Before." The pursuit of best practices is a journey involving the pursuit of alternative ways of doing things. In the process you challenge traditional methods, not for the sake of eliminating them, but in an effort to seek other ways that are better suited for the current climate. "We've always done it this way" is an organizational cancer that needs to be surgically removed because it is indicative of complacency, a major obstacle to pursuing best practices.

Challenge Every Existing Assumption. Challenge does not necessarily equal change. Challenging the status quo simply shows a willingness to break away from the temptation to protect sacred cows or territorial boundaries that can get in the way of pursuing efficiency and effectiveness.

Define Your Operation as World-Class. Behaviorists have long taught us that you can only achieve that level to which you aspire. By defining yourself as a world-class organization you force new perspectives and a willingness to ask yourself questions such as:

- "How would a world-class organization respond?"
- "Would a world-class organization pursue this?"
- "If we do not pursue it this way, are we running the risk of losing our status as a world-class service organization?"

Only when you begin to define yourself as a world-class organization can you start to act like one.

Conclusion

The achievement of best practices requires a commitment from senior management. Without their sign-off there will be an absence of budgetary support and a lack of leadership by example. Yet, the actual implementation of best practices is the functional responsibility of those at the bottom of the organization. Without their willingness to implement and actively participate, best practices remain only a concept. In short, success can only be achieved when there is a convergence of involvement from both the top and the bottom levels of the organization.

Dennis Dalton

Sources

Dalton, D. 1995. *Security Management: Business Strategies for Success*. Boston: Butterworth-Heinemann.

Gulick, L. and Urwick, L. eds. 1937. *Papers on the Science of Administration*. New York: Institute of Public Administration.

Morehouse, D. 1992. *Total Quality Management: A Supervisor's Handbook*. Shawnee Mission: National Press Publications.

BUDGETING

A budget is a forecast of expenditures and revenues for a specific period of time. Because a budget sets priorities and monitors progress toward selected goals, it is a basic planning tool. A budget helps a Chief Security Officer make informed decisions on the management of people and assets in the Security Group. Typically, the CSO prepares the budget on the basis of estimates to meet priorities for the next fiscal year. The estimates reflect inflationary pressure and current year spending. The budget is presented to the CSO's supervisor who may modify the estimates and rearrange priorities. The supervisor delegates to the CSO formal authority to enter into financial obligations at certain agreed dollar levels. An independent body within the company, such as a financial control group, generally monitors security

expenditures to ensure they are consistent with organizational objectives.

In any operation of size and complexity, budgeting will be a routine, yet essential, element of planning from year to year. Three purposes stand out:

- Estimate the costs of planned activities.
- Provide a warning mechanism when variances occur in actual costs.
- Exercise uniformity in the matter of fiscal control.

The budgeting process has four distinct stages: preparation, authorization, execution, and audit.

Preparation

An annual budget places on the CSO the responsibility for preparing Security Group estimates and coordinating them with overall company planning. The CSO and his/her supervisor meet, sometimes with key Security Group staff present, to discuss planned activities. It is not unusual to begin as early as six months in advance of the next fiscal year.

Security budget preparation begins with targets and ends with binding commitments. Outlays and spending authority are usually categorized by functions such as security officer operations, investigations, and physical security inspections. New spending requests, even when approved at the next higher level, tend to be very critically examined.

Preparation includes obtaining buy-in from groups dependent on or affected by Security Group activities. Garnering buy-in is typically informal: phone calls, e-mails, memoranda, and one-on-one meetings. The CSO's primary aim is to identify essential security services that have not already been addressed. A secondary aim is to identify objections that may surface later, when the time for patching up has passed.

Authorization

Authorization begins by obtaining supervisory approval. Preceding approval may be meetings with peers. Peers head up groups and report to the same supervisor. It is very likely that a peer will be a security services customer and therefore will have a stake in the security enterprise and a right to offer input.

The next step is to present the proposed budget to a budget review committee composed of specialists from the company's finance group. The review committee typically asks to receive the proposed budget for study in advance of one or more discussion meetings to follow. The CSO's budget proposal is detailed item by item and thoroughly documented. Details address projected activities, purposes and benefits, and likely consequences if activities are not funded adequately.

When the CSO presents the proposed budget in person, he/she uses a mild combination of negotiation and persuasion. Several such meetings ensue before the budget review committee sends the proposed budget to a higher level for final decision. The decision will certainly involve the chief financial officer (CFO) and possibly others on the executive team.

Execution

The budget begins at the start of the fiscal year. The CSO's responsibility is to ensure effective and efficient performance of Security Group functions while at the same time keeping costs in line with the budget.

At one point or another, the CSO may find it necessary to amend the budget; for example, when an unanticipated event requires the expenditure of unbudgeted funds. In the business of security, unanticipated events are the norm rather than the exception. The CSO will send a funding request up the chain of command.

Other amendments can occur. Unspent funds in one account can be moved to another account short of funds, not unlike a shopper that moves money from one pocket to another. In some cases in some organizations, the CSO can make such transfers on his/her authority. They must, however, be documented.

Although formal and closely managed, a budget is in a constant state of change and not all changes bring added funds. In times of economic stress, the CSO may be required to cut spending.

Audit

A budget is audited during execution by the CSO and the company's accounting group. The CSO keeps track of spending almost as it occurs. Every invoice or bill signed by the CSO is copied and placed in a file.

Auditing by the accounting group is largely a matter of recording payments made to fund Security Group activities. A record is prepared monthly. When significant variances appear, the accounting group informs the CSO. When variances increase or are not corrected, the accounting group notifies the CSO's supervisor.

The Security Group's budget can also be examined by the company's audit office for one of two reasons: as a routine control measure or as a formal investigation of suspicious irregularities.

Budget Director

A budget director brings all group budgets into a comprehensible whole called the master budget. It is an overall forecast of transactions within a given period, set up in a manner that delivers to senior management timely reports of financial results. The master budget enables the preparation of financial statements such as the income statement and balance sheet.

The process of budget preparation at the group level adheres to a methodology specified by the budget director. Group leaders identify and justify their planned activities and estimate costs. The format and dollar figures of proposed budgets are developed according to a common framework. Without it, the auditing function would be hampered and the master budget difficult to comprehend.

The prescribed methodology of the common framework and the actual budget are two different things: the first is a tool and the second is the object crafted by the tool.

A budget is purpose driven and function conscious. The form of budgeting specified by the budget director will correspond to organizational goals and the functions necessary to reach them. Selection of the budgeting approach can be influenced also by history and experience (the way we've always done it), tax implications, and the preferences of the executive team and the board of directors. Major spending decisions can be made at the board level but are most often made by the executive team. The budget director reports to the chief financial officer, a member of the executive team.

Zero-Based Budgeting

Zero-based budgeting starts with an assumption that zero dollars are available. Dollars become available when proof is presented that an activity is necessary to the business. Implied in the approach is a requirement to explore alternatives for achieving the same or similar results at a lower cost. Group leaders, including the CSO, make their case by answering three questions: What is the purpose of the activity? What will it cost? What is the added value? Benefits that can be derived from the activity are weighed against cost. The CSO makes the argument that benefits will be lost or that undesirable consequences will come about if an activity is not funded or funded at a lesser level.

Zero-based budgeting forces the CSO to look at different levels of effect for performing an activity. The levels may range from minimum to optimum. At each spending level, the CSO would show the costs of the activity, the predicted value, and the effects likely to be experienced by increases or decreases in spending. The CSO could be required to describe the probable outcomes of operating a guard force at different spending levels.

Flow Directions

Directions on major budget issues flow from the top down and requests for funding flow upward. Directions passed downward tend to deal with both administrative and substantive matters. Administrative matters provide guidance as to the format of the budget document, the placement of particular costs into particular categories, the attachment of supporting documentation, and the deadlines for submitting drafts.

Limitations

Substantive matters can include limitations, such as no new hires, no purchases without prior authority, and no increase of the group budget

beyond a certain level (e.g., not more than 5 percent above the total budget of the current year).

A down and then up again pattern is usually the case before a group's budget is set in stone. The CSO meets multiple times with multiple functionaries. At one meeting, the budget is okay; at the next meeting it is not okay. At every meeting, the CSO pleads his/her case. Nearly every meeting is called the "final" meeting, which turns out not to be the case. Because the CSO never knows if the next meeting will be the final meeting, he/she has to approach it as if it were a "last chance."

Cost-Benefit Ratio

A request for a major purchase may require approval by a spending authority separate from the budget committee. A major purchase not reflected in a budget is called an "exception to the budget." A preparatory step in considering a large expenditure is to determine the cost-benefit ratio, a figure computed by dividing costs by benefits. To illustrate:

- An access control system costs $500,000 to purchase.
- The service life of the system is 10 years.
- Guards replaced by the system result in a saving of $100,000 per year.
- The cost-benefit ratio is therefore 0.5:1, meaning that the cost of the purchase is half of the benefits or that the benefits are twice as great as the costs.

The ratio was arrived at by multiplying the annual guard cost savings by the number of years of useful service of the access control system. This figure ($1,000,000) represents the benefit, and is divided into the cost of the system ($500,000). Benefit versus cost is 0.5. When the ratio is less than 1, it is favorable; and unfavorable when it is higher than 1.

Controlling Costs

Apart from the process of budget preparation and approval is the day-to-day task of maintaining a budget folder. This folder is informal and a device of convenience. Placed into the folder are invoices, statements, price quotes, purchase orders, sales receipts, notes and memos concerning expenditures, and like tems. Monthly, the accounting group sends to the CSO a computer-prepared summary that (1) reflects spending for the previous month and year-to-date, (2) compares those figures against the budget's planned expenditures, and (3) highlights variances. The CSO is expected to take action when actual spending exceeds planned spending by a significant amount. The action is to put a brake on spending, if possible; if not possible, the CSO submits a request to increase the budget, a request that is never warmly received.

Overspending

Overspending is frequently the result of poor planning. Failing to anticipate rises in the costs of essential products and services or incorrectly calculating how many and how much of each will be needed is somewhat forgivable. Underspending for a budget item is rarely a problem; overspending is an indication of poor money-managing skill.

John J. Fay

Source Fay, J. *Contemporary Security Management, 2nd Edition*. 2006. Boston: Butterworth-Heinemann.

BUDGET PLANNING

Management is the coordinated application of resources to accomplish objectives. In this definition, managers carry out the functions of planning, organizing, directing, and controlling. The work activities of these functions consume resources that are purchased and are therefore measurable in dollars. The dollars planned to be expended are shown in budgets. There are many types of budgets. They can be used to show expenditures for projects that start and end, processes that never end, capital equipment purchases, a department's monthly activities, or the total organization's yearly activities. Budgets come in all sizes and shapes, serve a variety of purposes, and involve many different techniques.

All budgets have one thing in common, however; they have a close relationship with the planning function. This is so because the work activities planned to occur must be funded by dollars set aside in the budget. A budget can be viewed as:

- A plan stated in financial terms.
- An allocation of funds to meet planned objectives.
- A record of work activities in terms of monies appropriated.
- A tool for measuring the success of planned activities.

Let's use a simple situation to illustrate the relationship between planning and budgeting. Assume the security manager, in planning for the next fiscal year, concludes that a valuable work activity of the department will be to operate a rape avoidance program. The objective of the program is to minimize loss to the company resulting from lower productivity of employees who miss work or are distracted at work due to actual or perceived rape incidents. The security manager's plan is to conduct one rape avoidance presentation each quarter of the next year; the presentations will be made by a rape avoidance expert; a video tape on the topic will be purchased; and the presentations will be held in the company's learning center, using in-house audiovisual equipment. The presentations will be announced by posters placed in the coffee bars and each attendee will receive a booklet that is available for sale from the community rape crisis center. The security manager estimates that 100 employees will attend each presentation. The budget might look like this:

TABLE 1 A Very Simple Example of Computing Costs

Speaker fees	
Four @ $200 each	$ 800
Film purchase	$ 250
Posters	
Artwork	$ 150
Printing	$ 100
Booklets	
400 @ .50 each	$ 200
Total	$ 1500

This simple illustration does not take into account other costs, such as the security manager's time in managing the program, and the cost of the learning center and audiovisual equipment. Those costs might be rolled into other categories in the security manager's overall budget, and within that overall budget the rape avoidance project would be a very small item.

Forecasting

Work activities of today are based on yesterday's plans and tomorrow's expectations. Plans cannot be made without forecasting the future and what the future will bring. For example, a security manager's projection of growth in the company's employee population is a forecast of increased pre-employment screening activity; increased vehicle and pedestrian movement into, within, and from the premises; and increased pressure on the pass section to issue new access control badges.

It is well recognized that while forecasting is important in making rational decisions, the activity itself is more art than science. The value of a forecast is not in its relative accuracy, but in the fact that the activity requires the manager to give balanced consideration to factors that might influence the future. Because the past has never been a perfect predictor of the future, the manager is on mushy footing when making plans based solely on historical data.

Success at forecasting usually rests on a competency to judge under what conditions past occurrences can be relied upon. The manager must also be able to differentiate between new facts that are important and those that are irrelevant. The security manager cannot plan for the unknown or the unpredictable, but must instead concentrate on making an intelligent assessment of probabilities.

While the average line employee is thinking of work in terms of today, the manager is thinking about work stretched across substantially larger blocks of time. Thinking ahead is not necessarily a measure of intelligence, but of the conditioning effects of experience in meeting life's responsibilities.

Charles A. Sennewald

Source Sennewald, C. 1985. *Effective Security Management, 2nd Edition.* Boston: Butterworth-Heinemann.

BUSINESS ETHICS

Ethics in business are the standards of conduct and judgment in respect to what is perceived as right and wrong. An intrinsic element of ethics is the specification of responsibility for human actions. Ethical standards go beyond merely describing conduct that we habitually accept;

they seek to define higher goals and the means for attaining them.

The Chief Security Officer (CSO) encounters ethics in two dimensions: first, as the employer's instrument for developing business conduct policy and investigating improper conduct by others; and second, as an employee who is personally obligated to conduct business in accordance with the established policy.

The CSO knows well such unethical practices as misuse of proprietary information, kickbacks, and conflicts of interest. The controls for preventing and detecting offenses are clear cut and easily understood administrative mechanisms. It may be less clear to the CSO the expectations of senior management regarding the manager's decisions and conduct that impact the company's bottom line. For example, a CSO whose principal duties involve selling a security product may be caught between the choices of using persuasive, but deceptive, selling techniques and being scrupulously honest. How does senior management view the situation? Does the promise of profit take precedence over truth?

The continued deterioration of ethics in business should lead us to a closer examination of personal and corporate morality. Mainstream ethicists believe that an act is either intrinsically correct or incorrect, and that we have a duty to always act correctly. Others argue, however, that the reality of the human condition is that we all seek to engage in acts that derive pleasure, and acts that produce the greatest amount of pleasure for the greatest number of people are morally correct.

Code of Ethics

A traditional approach for promoting ethical conduct is the adoption of a code of ethics. Problems arise, however, due to concerns about who will create the code, who will be affected by it, what it will cover, and the sanctions that may be applied to violators.

In attempting to reconcile the various concerns about a code under development, the drafters may produce an ineffectual document. On the one hand it may be so watered down as to have no real impact on behavior, or on the other hand, include unattainable principles. In many cases it is impossible to select between competing and sometimes incompatible interests when moral questions are being examined.

A great difficulty lies in reconciling morality and profit. Realistically, a moral principle is not acceptable if it condemns business activity; as a result there is a natural tendency within business to see profit-making as a legitimate, if not moral, end in itself.

Principles of Business Conduct

A business is driven by the forces of economic reality, is constrained by the limits of custom and law, and is shaped by the human values of its workforce. A business, then, is an institution of people and ethics as well as an enterprise of profit and loss.

The ethical performance of a business is a matter of spirit and intent, as well as a matter of law. A company's business practices are the expression of management's philosophy and will often contain these basic principles:

- Businesses that succeed are those that conduct their affairs with honesty and integrity. These qualities are characterized by truthfulness and freedom from deception.
- There is no conflict between pursuit of profit and attention to ethics. Business generally will prosper in an environment that is fair, open, and morally secure.
- Employees are the key to ethical business conduct, and their behavior is strongly influenced by the way they are treated and how they view management. Ethics flourish in an environment that fosters individual self-respect, loyalty, and dedication.
- A business ethics policy will usually express these overriding principles in a more specific format, setting out personal standards, responsibilities, and sanctions. The policy provides a framework against which individual employees can measure their own personal conduct and management can establish a supportive climate by communicating the principles and setting the example.

John J. Fay

Source *Principles of Business Conduct*. 1991. Cleveland: British Petroleum America.

BUSINESS ETHICS POLICY

(SAMPLE)

General. The Company has a policy of strict compliance with laws which are applicable to its businesses, wherever conducted. In some instances, law and regulations may be ambiguous and difficult to interpret. In such cases we would seek legal advice to which we have access in each business and at the corporate level in order to assure that we are in compliance with this policy and are observing all applicable laws and regulations. Compliance with the law means not only observing the law, but conducting our business affairs so that the Company will deserve and receive recognition as a law-abiding organization.

Entertainment, Gifts, Favors, and Gratuities. The Company's guidelines governing levels of entertainment, gifts, favors, and gratuities, whether offered by employees or extended to them, are acceptable if:

- They cannot be construed as intended to affect the judgment of the recipient so as to secure preferential treatment and
- They are of such limited nature and value that they could not be perceived by anyone to affect the judgment of the recipient and
- Public disclosure would not be embarrassing to the Company or the recipient. All relations with government or public officials should be conducted in a manner that will not adversely reflect on our reputation or the official's integrity and with the expectation that all such actions will become a matter of public knowledge.

Political Contributions. Corporate contributions, direct or indirect, and of whatever amount or type, to any political candidate or party, or to any other organization that might use the contributions for a political candidate or party, are illegal at the federal level and in some states. In those states where such contributions are legal, they should be made only upon the approval of the Director, State Government Affairs. In addition, political contributions at the federal or state level by any employee who is a "foreign national" (i.e., an employee who is not a citizen of the United States or has not been admitted for permanent residence) are illegal.

We may from time to time take stands on issues of public policy, particularly those that affect the Company's interests or those of its several constituencies. In such cases, we may elect to express our views publicly and spend company funds to ensure that our position is broadly disseminated. We may also provide financial support to groups that advocate positions essentially consistent with our own. The Company encourages individual employees to participate in the political process, including voluntary contributions to the Company's political action committee and to candidates and parties of their choice. However, no influence shall be exerted by any employee on another employee to make any personal political contribution or to engage in any political activity inconsistent with that employee's own personal inclination.

Accountability. The law requires that the Company and the businesses for which it is responsible keep accurate books, records, and accounts to fairly reflect the Company's transactions and that we maintain an adequate system of internal accounting controls. Therefore, it cannot be over-emphasized that our books and records should have the highest degree of integrity. Employees should fulfill their responsibilities to assure that books, records, and accounts are complete, accurate, and supported by appropriate documents in auditable form.

All vouchers, bills, invoices, expense accounts, and other business records should be prepared with care and complete candor. No false or misleading entries and no undisclosed or unrecorded funds or

assets should be permitted for any reason. No payment is to be made for purposes other than those described in the documents supporting the payment.

Antitrust Laws. The Company endorses the view that a viable free-enterprise system rests upon the fundamental proposition that free and open competition is the best way to assure an adequate supply of goods and services at reasonable prices. Therefore, in carrying out his or her duties, every employee shall strictly adhere to the letter and spirit of the antitrust laws of the United States and with competition laws of any other country or any group of countries that are applicable to our business.

It is recognized that the antitrust laws are complex and difficult to interpret. They also have application to a very broad range of activities. In these circumstances, employees should take the initiative to consult the Law Department whenever the proper course of action is in doubt. We consider compliance with the applicable antitrust laws so vitally important that neither claims of ignorance and good intentions, nor failure to seek timely advice will be accepted as an excuse for noncompliance.

Conflict of Interest. The term "conflict of interest" describes any circumstance that could cast doubt on our ability to act with total objectivity with regard to interests of our business. We not only want to be loyal to the Company, we want that loyalty to come easily, free from any conflicting interests.

While we fully respect the privacy of employees in the conduct of their personal affairs, we insist that each employee fully discharges his or her obligations of faithful service to the business. Activities which involve the unauthorized use of time, equipment, or information, which significantly interfere with business interests will be avoided. Of particular concern are situations in which our personal interests may conflict with the interests of our business in relations with present or prospective suppliers, customers, or competitors.

The use of an employee's position or the assets or influence of the organization for personal advantage or for the advantage of others is prohibited. In order to avoid potential conflicts with regard to accepting outside employment regarding consultancies, directorships, part-time or freelance activities, the employee should discuss the particulars with his or her immediate supervisor prior to accepting employment.

Generally, it is our policy that employees may not, except at the direction of the Company, undertake any discussions or activities with potential participants, lenders, advisors, or attorneys relative to the possible purchase of any business for which the Company is responsible. This applies whether or not that business has been applied for divestiture.

If an employee desires to undertake any such activity on his or her own behalf or on behalf of others, before doing so he or she should advise the Chief Financial Officer of the Company who will determine in each case whether such activity can be conducted in such a way so as to protect the best interests of the Company.

Prohibited Investments. The Company prohibits employees from purchasing or dealing, either directly or indirectly, in any:

- Interest (or option to purchase or sell interest) in any organization or concern that the employee knows is a candidate for acquisition by the corporation or is under consideration for some other business arrangement with the corporation. This provision, however, does not apply to ownership of stock or securities amounting to less than one-half of one percent of the outstanding stock of any publicly

held corporation. For purposes of this policy, a "publicly held corporation" is one whose shares are listed on a recognized stock exchange or are included in the daily over-the-counter list of quotations of the National Association of Securities Dealers and published in the Wall Street Journal.
- Interest in any supplier, competitor or customer with whom we do business.
- Contracts, options, or any other form of participation in the commodities' futures or trading markets and in any commodity which we sell.

These prohibitions apply to purchasing and dealings by members of the employee's household or by a third party if intended to benefit the employee. They apply only to "purchasing and dealing" and do not apply to acquisitions by inheritance or gift nor do they apply to employees who are members of collective bargaining units. Managers are requested to take necessary actions to ensure their employees are aware of these prohibitions.

Employees should also be urged to discuss any questions they may have pertaining to prohibited investments with their immediate supervisor or designated ethics coordinator within their operating company or staff department.

Other prohibitions, in addition to those above, may be prescribed by individual business who will make these prohibitions known to affected employees.

Use of Classified Information. Company classified information is found in many types, forms, and locations. Security measures applicable to the protection of information are to be followed.

It is our policy that all classified business information is used solely for our own purposes and is not to be provided to unauthorized persons or used for the purpose of furthering a private interest or making a personal profit.

We would ensure that all material non-public information concerning the securities, financial condition, earnings, or activities of the Company remain protected until fully and properly disseminated to the public. Examples of areas of particular sensitivity are current interim earnings figures or trends, possible acquisitions or divestitures, exploration and production plans, and new plants, products, or processes.

Procurement. We require that our employees maintain the highest ethical principles in the acquisition of goods and services. Procurement practices and procedures should:

- Provide equal opportunity to all qualified firms wanting to do business with us.
- Treat all suppliers and contractors fairly and consistently.
- Be meticulously applied.

During the bidding process, difficulties may arise when bidders offer unsolicited price reductions or other concessions after bid submission, or attempt to enter into other post-bid negotiations which go beyond the normal bid clarification process. Acceptance of such unsolicited offers during bidding is contrary to our procurement policy.

Bids are considered confidential and are never to be provided to anyone outside the Company, and, within the Company, only to authorized personnel. Further, pains must be taken to treat all bidders equally during the bid period, especially with respect to bid document interpretations and clarifications.

The Company procurement policy, reflecting ethical business practice, is issued by the Corporate Materials and Contracts Department. Businesses and staffs are expected to establish their own procedures consistent with such policies.

Non-Compliance. Compliance with this Policy carries the highest priority throughout the Company. Failure to comply with the principles of business conduct may unnecessarily expose us and our employees to risks in the form of administrative sanctions, civil proceedings, and/or criminal prosecution.

Management is responsible for instituting preventative measures, ensuring that violations of Policy are thoroughly investigated by competent professionals experienced in ensuring equal respect is given to the rights of employees and objectives of the Company and the business for which it is responsible, and taking the appropriate administrative and/or disciplinary actions consistent with the infraction.

Legal Violations. Diversion of Company assets, fraud embezzlement, theft, and intentional damage to equipment and similar events all represent criminal actions against the Company. It is our policy to seek and assist the prosecution of persons who are believed to have committed criminal acts against the Company. Particulars of the case will be presented to the appropriate law enforcement agency for a determination in pursuing prosecution. In addition, any criminal loss exceeding $75,000 requires an investigative audit with assistance from Internal Audit and Corporate Security.

Policy Violations. Violations of this policy on business conduct more often will not result in violations of law; however, they result in violating the spirit and intent of ethical behavior. These may include: unauthorized use or disclosure of classified information; accepting gifts or entertainment of material value that affects our ability to be impartial; records manipulation; and conflict of interest. Management's response to such cases usually will be handled internally and disciplinary procedures will be applied where deemed appropriate.

Follow-Through. There are two broad actions we can take to ensure that our written commitment to ethical business conduct pays off in practice.

The first is to provide a mechanism that will help us handle difficult judgment decisions in those "gray areas" where it is often hard to pinpoint right from wrong. None of us should be uncomfortable in handling a question of ethics.

When such situations arise, we must seek counsel. The system is very simple. Ask the person to whom you report.

All managers are to maintain an open-door policy with regard to questions of ethics. They are to make themselves easily available to any of us who have such questions. We are reminded that the time to bring up a question of moral standard or ethical behavior is before the fact, rather than after the fact. We must never hesitate to talk to our supervisors about a question of business conduct, no matter how small or insignificant it may seem to be.

The second action consists of several steps that will make attention to this policy an integral part of managing our business. These steps are as follows:

- The Chief Security Officer is assigned oversight of a follow-through program.
- Each business and staff group will establish a procedure to ensure that at least once a year these principles of business conduct are reviewed with their managerial employees. Additionally, each business

and staff group will designate at least one person to whom any employee may communicate freely on matters concerning the interpretation, application, or suspected violation of these principles. Such designees will, routinely, keep the Chief Security Officer apprised of activities/inquiries with respect to these principles which arise in the ordinary course of business.

- Urgent issues of this nature will be immediately communicated to the Chief Security Officer, who will consult, as appropriate, with the Audit and Law Departments as to the appropriate course of action.
- Any allegation or suspicion that unethical or illegal activities are taking place will be reported to Corporate Security and, where appropriate, will be thoroughly investigated in a competent, fair, and confidential manner, with equal respect being given to the rights of the employee and the objectives of the Company.
- The General Auditor will establish procedures to monitor management's compliance with our principles of business conduct and will annually report the results of this effort to the Chief Executive Officer of the Company and to others as he or she may direct.

CORPORATE SECURITY AND THE PROCESSES OF CHANGE

At least since the end of World War II, the security industry has been radically and rapidly evolving. The main driving forces of change have been the steady escalation of crime and the increasing inability of law enforcement to be effective in dealing with crimes against businesses. A whole new industry has risen up to meet market demands fueled by business fears, and with it we have seen the maturation of an entity that has come to be called the proprietary security organization or simply corporate security.

Corporate security's *raison d'être* has been the protection of the employer's assets against threats of crime, and the methods of protection have relied to a great extent on concepts borrowed from other fields. Intelligence gathering, crime analysis, investigating, and target hardening are examples of methods acquired from law enforcement; and from sister organizations in the business environment. Corporate security has learned how to conduct audits and inventories, how to secure confidentiality agreements, and how to track and control the movement of people and property. Corporate security has also necessarily developed an expertise in the application of electronic technology to the tasks of assets protection.

In other words, corporate security is the child of change and the product of its environment. It was born out of a need and grew up learning how to cope and survive. It is what it is and does what it does because of the dictates of external and internal forces. Carried with this condition is the inherent danger that change can become so demanding that corporate security may be unable to cope and therefore unable to survive.

A New Form of Change

A change with profound and sweeping proportions is in fact brewing now. The change has to do with human values, but first a little background.

Business organizations are turning up the pressure to improve results. It is not just that results matter more today, because results have always mattered, but what we are seeing is a shift in the way results are delivered. To be sure, change is essential if organizations are to succeed in a tough, competitive world, and organizations are being judged more harshly than ever before, both by their managements and shareholders.

Change is turning organizations into clusters of clever people doing clever things, and clever people have to be handled rather more sensitively than was the case in the good old days. The tried and true concepts of control and supervision are giving way to persuasion and to leadership. Business managers now speak of visions and empowerment. An entirely new rationale is taking shape in which traditional controls are increasingly unwelcome.

For the Chief Security Officer, the mandate is to achieve the same or a higher level of results, except go about it differently. This is neither simple nor easy. On the one hand, the organization's top leadership wants the CSO to embrace bold new concepts, yet on the other hand wants no dilution in the protection of assets. Whether the CSO likes it or not, he or she is caught up in a process of learning, adapting, and, above all, accepting the proposition that the change which has begun will continue well into the foreseeable future, and that corporate security must be a constructive part of the process.

Being a part of the process is another way of saying that the CSO will continue to adapt. Successful adaptation is to continue to be effective in protecting the organization's assets, but to apply techniques that fit the ways of the new organization. But what does the new or evolving organization look like, and what are its ways?

The Shamrock Organization

Some insights can be found in Charles Handy's excellent book, *The Age of Unreason*. Handy describes what he calls the shamrock organization. The first leaf of the shamrock is the core of professional workers. These are the managers, the high fliers, the skilled technicians, and key professionals who are absolutely critical to the organization. Without them, the business cannot possibly succeed. They work hard and long, and are paid well.

Life in the professional core is collegial, resembling that in a consultancy or a professional partnership. The core structure is relatively flat, with few layers of rank. The concept of superiors and subordinates has been replaced by that of colleagues and associates.

The size of the professional core in many corporations has gotten smaller and is continuing to shrink. Two cost-driven reasons stand out: a preference for a flat organizational structure is making many positions redundant, and more and more professional core functions are being assigned to outside contractors.

The second leaf of the shamrock organization is contractors; generally, people who do specialized work. While the work may have value, it is not necessarily critical or central to the business. Contractors are able to perform these jobs better and at lower cost than regular employees, requiring less management time and attention in the bargain.

The third leaf is the flexible labor force, the part-time and temporary workers. They move in and out of the company as the needs of the business expand, contract, and evolve. The services are not always done conveniently and to great satisfaction, but they are economical. In many U.S. corporations, flexible labor is the fastest growing segment of their workforces.

Shamrock types of organizations have been emerging at least since the early 1980s when downturns in profits forced many major corporations to make significant reductions in human-power. Hit hardest were the professional cores. When times improved, businesses were determined not to be caught the same way twice. Work that in earlier times would have been returned to the professional core was farmed out to contractors, and some of the lower-level jobs were converted to part-time and temporary status.

Instead of one workforce, many corporations now have three. Each workforce has a different contribution to make, a different commitment to the organization, a different scheme of remuneration, and a different set of expectations. Clearly, there are a number of interesting problems associated with delivering security services in such an arrangement.

Security Problems in the Shamrock Organization

In the professional core we see more people conferring and sharing information across large expanses of geography, and the information they work with has been pulled from many centers of expertise. A greater amount of sensitive information is being generated and opened to a larger number of key players in many parts of the globe.

Business information, including the most sensitive possessed by an organization, is valuable to the extent it is put to work. Although the CSO's instinct is to keep sensitive information under lock and key, the reality is that sensitive information is widely scattered and in flux at any given time for the simple reason it is in use. Information in movement is most vulnerable to loss and compromise. The utilitarian value of the information at the moment of use may only be fractional by comparison to the cost of its loss.

In the professional core we are also seeing more people making spending decisions. This is called trust and empowerment, but the CSO knows that more hands on the purse strings can lead to spending that is dishonest.

In the second of the three-leaved workforce, corporate security has to be concerned when the organization makes sensitive materials available to contractors, especially when contractors work for competitors. Sensitive materials include things like business plans, trade secrets, proprietary processes, customer lists, and executive salaries.

There is the possibility of contractors learning how to pass through protected computer gateways that lead to valuable data or to third parties connected to the system. When the know-how of access is in the hands of a disgruntled contractor, the organization can be damaged severely. Hacking, viruses, worms, and Trojan horses are possibilities, as well as disablement of a critical system by the support contractor as the result of a contractual dispute.

With regard to the third part of the workforce, there are few reasons to believe that the part-timers and temporaries who replaced regular employees are of the same caliber. One should anticipate in this group a higher level of drug-related accidents and incidents, pilferage, vandalism, confrontational behavior, and acts of violence. The vendors of flexible labor are focused on providing human-power, not on conducting pre-employment background checks. Without screening, the professional core is likely working shoulder-to-shoulder with people that cannot be trusted.

Controls Based on Motivation

The motivations that supported ethical business conduct in the old organization are changing in the shamrock organization. A concern for assets, for example, is not a motivator to people who get their paychecks elsewhere. The sense of mutual interest found in the employee/employer relationship may not be present in service arrangements, and it would be foolish to believe that vendors will place the client's economic good ahead of theirs. While persons in the professional core may have careers, love the challenge of their work, and take pleasure when the organization succeeds, the people who work on an outsourced basis look at things much differently.

The traditional techniques of organizational control, such as locking things away, compartmentalizing information, and limiting spending authority, lose their effectiveness in organizations with cultures that stress individual trust. This is not to say, however, that all of the traditional controls will disappear. It is more likely they will be modified and new controls invented as the organization continues to evolve. A good guess is that the successful controls will be founded on principles of motivation, such as the influence of peers and informal groups. Motivation may be the only means of bridging the gap between rules and the desired human behavior.

The rapidly expanding work practices that rely on desktop computing are a case in point. The provision of personal computers (PCs) to employees is the giving of trust and empowerment to a large portion of the workforce. The autonomy inherent in desktop operations, combined with the power and flexibility of the technology, present new problems in control. Mainframe computers with large databases have physical, procedural, and technical safeguards, but this is not always the case with desktop systems. The risks include data loss and theft, use of time and equipment for unauthorized purposes, and theft of hardware and software.

Although the employer may have rules and provide training concerning desktop computing, the problem is one of compliance. The highly personalized nature of a desktop work station makes it very difficult to monitor computing activity in a non-intrusive way. While it is technically possible to monitor by connecting desktop equipment to networks, observing employees with closed-circuit television (CCTV) cameras, and providing closer overall personal supervision, these are not the accepted practices in a corporation that operates on trust.

Controls based on motivation would rely on the orientation, education, and training given to employees; the personal examples set for them; and, above all, an organizational culture which holds that when given a choice, people can be trusted to act in the best interests of the organization. The designers and implementers of the controls will come from the professional core. The CSO will be a key player in designing asset-protecting controls that on the one hand will be workable and effective, and on the other hand consistent with principles of trust and empowerment. The CSO will help gain acceptance of

the controls by exercising the skills of teaching and leading.

A Best Practices Approach

The CSO in an evolving organization can take the initiative in a best practices approach, i.e., practices that are done with excellence, both in and out of the corporation. Following are three hypothetical examples.

- Corporation A switched from in-house security officer services to services provided by an outside contractor. The CSO played a central role in negotiating the contract and monitoring contractor performance. Over a period of time, the corporate security department acquired considerable knowledge about contract administration. Many lessons were learned about how to hire honest, emotionally stable, and drug-free security officers; how to organize security officer operations so that services did not get in the way of the corporation's business processes; and how to train, develop, and generally treat security officers so that in return the corporation obtained quality performance accompanied by low turnover. These best practices had value to other units in the corporation that were making the switch to contractor services.
- Corporation B did pioneer work in establishing a drug- and alcohol-free workplace for its employees in the safety-sensitive environment of petroleum exploration and production. Through trial and error, corporate security learned how to educate employees against alcohol and drugs; trained supervisors to spot the indicators of impairment; and used chemical testing as a tool for steering employees away from abuse and for bringing afflicted employees into contact with treatment professionals. Corporate security shared this competency with the corporation's most important partners–the drilling contractors. A best practices approach transferred the positive elements of the substance abuse program to the contractors; and it was in the corporation's best interests to do so because, after all, the contractors performed jobs having high criticality in terms of physical loss, personal safety, and damage to the ecology.
- Corporation C observed that the corporate security department of a competitor regularly worked with the internal audit department to conduct investigative audits of vendors. The audit methodology of the competitor contained some innovative ideas for discerning patterns of collusion. Corporation C adopted and modified the methodology as a best practice.

These examples are in the nature of finding positives and putting them to work to the corporation's advantage. A best practices approach adds value and blends very well with control functions performed by a corporate security department.

Being a Contributor to Assets

It is important to remind ourselves that questions always arise about the value of providing protective services to assets that are static or in a state of decline. When the cost of protection increases or remains steady and at the same time the value of the asset falls off or remains unchanged, there is a natural tendency to want to reduce or eliminate the protection. This is an obvious fact, but it deserves mention because in the evolving organization corporate security needs to shift its focus to the enhancement of assets. The objective should be to move from simply being the watchdog of assets to being a contributor to assets. A best practices approach could be one facet of a larger effort to find and add value to the company's bottom line.

Finally, it seems appropriate to observe that the winds of change in the last half of the previous century have produced problems for nations, companies, and people. Inevitably, the enterprise we call corporate security has been affected and has risen to meet the challenges. Even greater challenges lie ahead as business organizations continue to restructure, innovate, and take on new cultures. There is no reason to suppose that the first half of this century will bring any lessening of change, and if corporate security is to evolve in harmony with the organization, it must change the ways of protecting assets.

John J. Fay

Sources

Frank, J., Shamir, B., and Briggs, W. 1991. *Security-Related Behavior of PC Users in Organizations, Information and Management.* Amsterdam: Elsevier Science Publishers.

Green, G. and Fischer, R. 2004. *Introduction to Security, 7th Edition.* Boston: Butterworth-Heinemann.

Handy, C. 1989. *The Age of Unreason.* Boston: Harvard Business School.

COUNSELING

An inherent function of supervision is to assist employees in solving personal problems that detract from their effectiveness in the workplace. Counseling can occur in almost any situation that brings the individual employee and the supervisor together for the purpose of helping the employee overcome problems.

Guidance should serve all employees and not be seen as a negative activity related only to employees with problems. Counseling given to good employees can make them even better employees. But when guidance is focused exclusively on workers who perform below the established standards, other employees may be reluctant to willingly participate in counseling for fear of being stigmatized.

A principal purpose of counseling is to help individuals learn to deal with personal problems. To be effective at counseling, the supervisor must be able to communicate on an interpersonal basis and exercise patience and good judgment. A facet of good judgment is to recognize that for an individual to deal with a personal problem there must first be a willingness to act decisively, and that one of the cardinal sins of counseling is to make decisions for the individual. An overly directive approach is apt to encourage dependence rather than self-reliance.

The opportunities for a supervisor to counsel are frequent and varied. Certainly one of the earliest opportunities is when an employee first arrives on the job. The new employee needs to become oriented geographically, meet co-workers, and learn the formal and unwritten rules of the organization. The supervisor is a main source of information, particularly with regard to showing the employee where and how he or she fits into the pattern of work activities, explaining job standards, and answering questions. A good orientation will often prevent small initial problems of adjustment from escalating to larger problems at a later time.

More than any other individual in the organization, the direct supervisor is positioned to evaluate the productivity, attitude, and potential of subordinates. Knowing something about the subordinate both as a worker and a person is necessary if the supervisor is to assist the subordinate in meeting the organization's expectations and at the same time satisfy personal goals.

Counseling Methods

Two general methods of counseling are widely recognized: the directive and non-directive methods. A third method uses the two methods together and is called the co-analysis method.

Directive Counseling. This approach is supervisor-centered. The supervisor takes the initiative in the dialogue, with the supervisor choosing the subject. The directive approach is appropriate when the individual needs to understand requirements and to identify personal deficiencies. This approach can succeed only when the individual sincerely wants to face and correct deficiencies. Although the supervisor may be very skilled in this approach, the critical element for success lies entirely within the employee.

Non-Directive Counseling. The subordinate is the central actor in non-directive counseling. He/she is encouraged to talk, to clarify personal thinking, and to discover a solution to problems through objective examination and honest articulation. The supervisor's role is to encourage the individual to take the initiative in discovering solutions, and moving positively and constructively to implement them. This approach can be helpful in removing emotional blocks and creating motives for improvement.

Co-Analysis. This approach falls somewhere between the extremes of the directive and non-directive methods. It is intended to join the supervisor and the subordinate in a mutual effort intended to work out a problem-solving regimen. Co-analysis can only succeed when the employee accepts the supervisor as a partner and sincerely wants to change. Success will also be a function of

how well the supervisor can bring the employee to a clearer understanding of the problems and to obtain agreement of the solution-oriented actions.

Conducting a Counseling Session

A counseling session cannot be effective without preparation. All pertinent information concerning the employee should be gathered and studied by the supervisor. Details that may be significant to the counseling process should be committed to memory so that the flow of the session will not be interrupted by referring to written materials. The presence of files or records and the taking of notes during the session can detract from a productive outcome.

The place of counseling should be relatively free from distractions and out of general view. An employee being counseled does not want to feel conspicuous, and the absence of privacy will inhibit the employee's willingness to open up. Seating, lighting, room temperature, and the physical setting should be comfortable for both the employee and the supervisor. Because the supervisor will need the employee's undivided attention, the employee's chair should face toward the supervisor and away from background distractions such as a window or open door.

The starting point will be critical. In the first few minutes the supervisor will set the tone of the discussions and attempt to open a two-way dialogue. This is often called establishing rapport, a subtle and important activity that can be difficult. The idea is to help the employee open up by getting a conversation going, usually about a topic of personal interest such as hobbies, achievements, or current events.

Encouraging the employee to talk and participate actively may cause the employee to feel constructively involved by describing the problem and playing a part in solving it. In the early part of the meeting, the supervisor should look for information that will define the dimensions of the problem. By asking questions that require more than yes or no answers, the supervisor can gain insights to the employee's motivations, attitudes, and dislikes. The responses may clarify the problem for the supervisor and provide clues to obtaining the employee's cooperation in taking corrective actions.

A counseling session should end on a positive note. The employee should walk away with a sense that something constructive has occurred. Even more importantly, the employee should leave with a commitment to take actions that were agreed upon in the meeting and the understanding that the supervisor will be expecting to see the evidence of them. Even if the employee is only helped to perceive the actual nature of the problem, this in itself is progress.

The supervisor will not always play a part in the problem-solving process. A supervisor's competency in recommending solutions will not usually extend to problems rooted in drug and alcohol abuse, marital and family stress, financial difficulties, and mental disorders. The role of the supervisor in these situations is to refer the employee to a specialized resource, such as an employee assistance program.

When an employee is referred to another resource, the supervisor should follow up to be sure the problem is being addressed. Specialized assistance should be regarded as a helping hand, not as a substitute for supervision. Responsibility to correct the employee's unacceptable performance remains in the venue of the supervisor even when third-party specialists provide the diagnosis and treatment.

A record should be made of every counseling session. The record should document the major discussion points, actions and deadlines agreed upon, and commitments of both the employee and supervisor. In some cases, the supervisor may want to give the employee a copy of the record for use as a reference in meeting the commitments.

John J. Fay

DEMING

Long after his death, Dr. W. Edwards Deming continues to be regarded by many as the leading quality guru in the United States. He argued that quality is measured in terms of the pursuit, yet quality is not definable. You can measure improvements in quality and you will know quality when you experience it.

Credited as one of the central figures in bringing Japan to a position of world leadership in competitive pricing and quality, Deming provided both a philosophy and a system for using statistical methods to achieve higher quality and productivity in manufacturing and management. Organizational theorists characterize his approach as being in the camp of teaching people

how to fish rather than feeding them. He believed quality is 85 percent the responsibility of management and 15 percent the responsibility of employees. Deming developed his fourteen points as a "charter for management" because he saw senior management's commitment as essential to the process. It is only within the past few years that his philosophy and methods have begun to gain widespread recognition for their impact on quality and productivity in U.S. companies.

Given his growing influence, it would be helpful to briefly review the highlights of his charter and examine how they can/need to be applied in the security profession.

Develop a Strategy for Constant Improvement

Deming suggested that organizations want a "quick fix," and in pursuing this they lose sight of the longer term and fail in the near term because quality is not something that can be achieved in incremental, individual efforts. Quality is a continuous, unfolding process. He offers this advice: determine what business the company is in and adapt to changing customer needs.

As a security decision maker, have you developed a process for Continuous Quality Improvement (CQI)? Are job descriptions and performance objectives centered more on encouraging CQI as a way of doing business, for example, by keeping track of the number of doors found opened and unlocked, or the hours of investigative time spent, or the number of escorts provided?

Adopt a New Paradigm

We need to approach quality with a persistence that establishes the ultimate goal as an error-free operation. The goal is to achieve quality over time through a process of continuous improvement.

Replace Mass Inspection with Employee Troubleshooting

By their very nature, inspections have a negative connotation. The process involves an overseer acting independent of the process. Inspections need to be replaced by employees assuming ownership for their service and/or production. As a part of assuming ownership, there is a need to develop a means of empowering employees to troubleshoot the process when errors are discovered. It's easy to put off known deficiencies, placing accountability away from oneself and saying simply, "Well it's not my job."

We know that security can't be everywhere, all the time. Unfortunately, for many years security professionals have preached that prevention begins with awareness. This is only half true. Prevention will not work until employees—including managers—assume responsibility for their awareness and translate this awareness into action (ownership).

End the Practice of Awarding Contracts on Price Alone

Instead of awarding work to the provider with the lowest bid, which is often tantamount to accepting minimal quality at best, companies need to develop long-term relationships with suppliers. Deming's view was that as long as organizations see vendors as vendors, they will remain vendors. When they see them as partners, they will become partners. Creating this new perspective requires nurturing mutual respect, trust, and responsibility, and offering rewards.

Promote Leadership and Institute Training

Managers need to understand that the title, manager, means that they are responsible for managing processes and things, not people. Managers lead people. This is a very critical, but oftentimes misunderstood difference. Leading involves supporting, delegating, and empowering people to achieve their fullest potential. Leadership involves coaching and mentoring as much as demonstrating by example and pushing people in positive ways to accomplish more. As many management theorists note, the organization is in the business it's in, but managers are in the organization business—and that means the business of developing people. A manager's final product is creating an environment in which people can make their best contributions, and consequently the organization can be productive and successful.

Leadership also involves eliminating fear. Deming noted that companies that make it "unsafe" for employees to ask questions and learn to do things right are facing tremendous economic losses on the way to their own demise. Employees who are afraid are not free to create. An environment of fear is directly rooted in traditional performance evaluations where compensation is tied to "those who toe the line" as opposed to those who dare to challenge assumptions and seek to make meaningful contributions.

Deming, along with many others, insisted that most performance problems can be traced to a lack of orientation and training programs. Management needs to set expectations for employees and demonstrate how workers can be successful in their jobs. This is especially true for people working in asset protection. Despite the emphasis that third-party suppliers put on their ability to train, educating employees is still one of their weakest links. The same can often be said for resident security programs.

In the security field, training is limited to primarily on-the-job learning. Initial officer training rarely exceeds twelve hours, and advanced officer training is done in a variety of ways, but invariably in the way determined to be the least costly. In short, the quality of training is largely determined by price, regardless of which side one considers. But real training is neither easy nor quick. Interactive communicating, group planning, and problem solving are the first stages. Deming believed that effective training is driven from the top down. When training begins at the top, managers and supervisors are aligned behind the same concepts and share a common language. Next, those in work groups or project teams on the pilot quality effort are trained in the new methods, teamwork, and statistical techniques. Eventually a training program is implemented for each area of work.

Eliminate Hype and Quotas

Deming rejected hype such as slogans, contests, targets, and other forms of internal competition. He thought that such efforts have little meaning and impact unless they originate from within the workforce. I'm not convinced that he is right here. Nonetheless, Deming contended that internal competition works against the goal of removing internal barriers. He believed that organizations need to redirect the competitive spirit to their real competitors in the outside business world.

Deming also believed that quotas should be eliminated. This move can be particularly difficult for many businesspeople since we have all been conditioned since the advent of the Industrial Revolution to believe that businesses run on numbers. Profit and losses, production units, services provided—all share a common denominator: they are driven by numbers. Yet achieving the numbers alone does not necessarily equate with achieving quality, market share, or innovation. Workers who are held to quotas are held to yesterday's standards; they are not moving the company into the future. Worse, quotas merely guarantee that workers will do whatever it takes to make the mark. An excellent example of a counterproductive system is today's version of the old Detext guard watch tours. Although the Detext watch tours system is hailed as the definitive means to track security officers, an experienced officer can quickly figure out ways to effectively "beat the system."

Remove Barriers and Promote Continuous Quality Improvement

It is up to management to encourage the process of interactive listening. This means really listening to what employees have to say about what gets in the way of their performing well. To eliminate barriers entails making available the resources necessary to accomplish the task(s) at hand—by developing innovative operating practices, assuring proper levels of staffing, and providing the necessary technology. Deming insisted that a special top management team must develop a plan of action to carry out the quality mission. The organization is a holistic system, including all of its influencing factors—internal and external customers, suppliers, and competitors—and it needs constant perfecting.

The remaining seven points of Deming's charter are known as the Seven Deadly Sins.

1. Failing to develop a long-term purpose. American businesses are driven by quarterly and/or annual results. Success is measured based on how well you perform this quarter or this year as compared to the previous quarter or year. The lack of a longer view makes

employees and managers feel insecure in their jobs, and this problem then feeds directly into the second deadly disease.

2. Focusing on near-term profits. American businesses define their success based on quarterly earnings. Public companies are driven by expected returns from the investment community. This preoccupation with profit for the sake of profit erodes concern for and attention to the longer view. Quite often resources that are designed to feed the future are sapped for the sake of making the near-term profit.
3. Conducting annual performance reviews. Annual performance reviews rarely measure true annual performance. Instead they reflect the last "you done me wrong" or "attaboy." Employees soon discover that performance reviews involve more punishment than encouragement. Deming believed that the impact of these measurements on the morale and productivity of both managers and workers is the opposite of what is intended because performance reviews promote fear, inequities, internal competition, anger, and discouragement.
4. Not discouraging management exodus. Deming pointed out that the migration of high-level managers from one company to another is a tradition. Whether those who leave are dedicated executives who have become disenfranchised or opportunists, the fault is the company's for not developing managers with the "big picture" in mind. Over the past several years, corporations have unwittingly turned on themselves by collaborating in the wholesale elimination of middle and senior layers of management. In their pursuit of lower operating expenses and higher dividends for stockholders, they have lost both their own continuity and the talent once hired to create their future.
5. Missing the hidden value. A company's success is linked just as much to intangible values as to empirical, or "known," data. Unfortunately, many companies miss the former altogether in their pursuit of the latter. As Deming explained, some of the most important factors are "unknowable," including the multiplier effect of a happy or unhappy customer, the absence of motivated managers and workers who are willing to go the extra mile that makes all the difference, and the hours saved down the line by front-end planning and proper communication.
6. Failing to emphasize health care prevention. Even though many companies are turning to health care prevention programs, the vast majority of American businesses have yet to make the transition. The evidence clearly demonstrates that significant savings can be achieved in premiums when prevention becomes the front line. These programs include wellness programs, antismoking programs, paid workouts and/or health club memberships, and annual medical checkups.
7. Substituting Continuous Quality Improvement for warranties. It has become easy for companies to offer warranties. Yet the real value of their product and/or service is not based on "customer satisfaction guarantees." While such guarantees provide an assurance that the company is concerned about the quality of its product, the real value to the company is in establishing error-free systems altogether. Companies that commit to quality and error-free work realize savings during a warranty period because they decrease the number of nonanticipated services. In other words, the warranty is the consumers' safety net; it is not the company's substitution for CQI.

On the surface, it would appear that these seven deadly sins have applications that are easily applied to security providers. Even though each has a specific lesson for the third-party supplier, the underlying principles apply to resident security programs as well. Security decision makers need to be focused on the longer-term strategy for providing asset protection, and this has special relevance to their systems purchases. All too often, the procurement process is driven by answering the need here and now. As the company grows or alters its course, today's "new" security system quickly becomes obsolete.

Similarly, focus on short-term profits can be just as deadly to security programs, and organizations as well. In today's litigious society, premises liability has become big business for plaintiff attorneys. Companies that defer taking the proper precautions until better economic times are in swing are placing themselves at greater risk. There are many ways to creatively finance capital expenditures or to budget operating expenses. One of the more commonly overlooked approaches, for example, involves splitting the cost over a longer budget period, for example, by extending the budget cycle from twelve months to eighteen months.

Deming's belief that annual performance reviews work against the employer-employee relationship is worthy of particular note with regards to the security operation. He did not advocate that performance not be reviewed; rather, he found the approach troubling. In his judgment, peer reviews, group assessments, quality circles, demonstrable contributions, and so forth worked better.

One of the more difficult challenges facing corporate America, and in particular the security profession, is the issue of management mobility. It remains true that a company's success is linked to its ability to come up with fresh ideas and new perspectives on a regular basis. It is also equally true that a company's success is linked to its ability to maintain a balance of continuity. Longevity is not bad.

Security programs are built on earned trust and proven reliability. Whether the people are proprietary, outsourced, or a combination of the two, the success that is achieved is directly related to demonstrated capability. Such know-how is difficult to measure, but it is very much real.

Deming's last two deadly sins speak to a reliance on traditional approaches and their inherent traps. There was a time when the costs of health care benefits were an insignificant part of the compensation formula. With runaway costs, however, this is no longer the case. As opposed to shopping for lower premiums among competing carriers, companies should be changing their strategy altogether. By seeking an alternative health care approach, companies can attack at the root the cost associated with escalating expenses. The result is lower cost all around. The question to be asked is whether or not the same type of paradigm can be applied elsewhere.

In a like vein, warranties have become a standard business practice. There was a time when guarantees by their nature forced employees to think error-free. The corporation understood well the cost associated with having to redo or replace a defective product. Over time, warranties have become the employee's safety net. After all, managers will reason, the company can afford a few mistakes. Besides, how many people really go through the effort to take us up on our warranty? Such misguided and what I would term "lazy" thinking misses the very point of offering a guarantee.

Conclusion

In concluding this discussion of Deming's contribution, it is appropriate to review several obstacles he identified. These obstacles plague organizations because they are grounded in management mind-sets that work against their best interests. Yet because of America's obsession with short-term fixes, executives and business unit heads frequently find themselves heading down a path that leads straight to such obstacles, and not in the direction of success, as they had hoped. Security managers are no exception in meeting obstacles:

- The quick fix. You cannot put a quality process in place overnight.
- Reliance on technology as the great problem solver. Technology is an administrative tool. Nothing more. Real quality arrives when tools are used by skilled specialists.
- Following the leader. Organizations that wait for "the other guy" to chart a new course and then follow the other's lead will always be behind.
- Accountability for quality assurance is limited. Too often, QA programs are meaningful to QA professionals but not to the entire workforce.

Deming and his ideas have had profound effects on how managers think and act. Unlike many other management concepts, the Deming approach has a proven track record. His ideas have been a catalyst for extensive research and have been an inspiration for many of today's business leaders.

Dennis Dalton

Sources

Dalton, D. 1995. *Security Management: Business Strategies for Success*. Boston: Butterworth-Heinemann.

Gulick, L. and Urwick, L. eds. 1937. *Papers on the Science of Administration*. New York: Institute of Public Administration.

Morehouse, D. 1992. *Total Quality Management: A Supervisor's Handbook*. Shawnee Mission: National Press Publications.

DISABILITY DISCRIMINATION

Title I of the Americans with Disabilities Act of 1990 prohibits private employers, state and local governments, employment agencies, and labor unions from discriminating against qualified individuals with disabilities in job application procedures, hiring, firing, advancement, compensation, job training, and other terms, conditions, and privileges of employment. The ADA covers employers with 15 or more employees, including state and local governments. It also applies to employment agencies and to labor organizations. The ADA's nondiscrimination standards also apply to federal sector employees under section 501 of the Rehabilitation Act, as amended, and its implementing rules.

An individual with a disability is a person who:

- Has a physical or mental impairment that substantially limits one or more major life activities.
- Has a record of such an impairment.
- Is regarded as having such an impairment.

A qualified employee or applicant with a disability is an individual who, with or without reasonable accommodation, can perform the essential functions of the job in question. Reasonable accommodation may include, but is not limited to:

- Making existing facilities used by employees readily accessible to and usable by persons with disabilities.
- Job restructuring, modifying work schedules, reassignment to a vacant position.
- Acquiring or modifying equipment or devices, adjusting or modifying examinations, training materials, or policies, and providing qualified readers or interpreters.

An employer is required to make a reasonable accommodation to the known disability of a qualified applicant or employee if it would not impose an "undue hardship" on the operation of the employer's business. Undue hardship is defined as an action requiring significant difficulty or expense when considered in light of factors such as an employer's size, financial resources, and the nature and structure of its operation.

An employer is not required to lower quality or production standards to make an accommodation; nor is an employer obligated to provide personal use items such as glasses or hearing aids.

Title I of the ADA also covers:

- Medical Examinations and Inquiries. Employers may not ask job applicants about the existence, nature, or severity of a disability. Applicants may be asked about their ability to perform specific job functions. A job offer may be conditioned on the results of a medical examination, but only if the examination is required for all entering employees in similar jobs. Medical examinations of employees must be job related and consistent with the employer's business needs.
- Drug and Alcohol Abuse. Employees and applicants currently engaging in the illegal use of drugs are not covered by the ADA when an employer acts on the basis of such use. Tests for illegal drugs are not subject to the ADA's restrictions on medical examinations. Employers may hold illegal drug users and alcoholics to the same performance standards as other employees.

It is also unlawful to retaliate against an individual for opposing employment practices that discriminate based on disability or for filing a discrimination charge, testifying, or participating in any way in an investigation, proceeding, or litigation under the ADA.

Source The U.S. Equal Employment Opportunity Commission 2006. <http://www.eeoc.gov/types/ada.html>

DISCIPLINE

As a rule, the word discipline evokes an emotional reaction, both to the giver and the receiver. No one enjoys being disciplined and most supervisors would rather do anything but administer it, but the fact remains that discipline is an important part of supervision.

On the brighter side, discipline need not be totally negative. A positive approach will emphasize discipline accompanied by guidance, sanctions that are balanced with fairness, and a system of rules that apply to all employees uniformly and consistently.

The word discipline is derived from the Latin word *discipulus*, which means learning. The word *disciple* is from the same root. Early Christian disciples were considered the learners or students of Christ. The word conveys an important concept in supervision, i.e., that discipline is a mechanism for correcting and molding employees in the interests of achieving organizational goals. Punishment, the negative aspect of discipline, is tangential to the larger purpose of fostering desirable behavior.

Discipline is an act of the organization, not of a supervisor personally. The process is a legitimate means to an end and condemns the employee's unacceptable behavior without condemning the employee. The process essentially says, "You're okay, but what you did is not okay."

It is also important that discipline be swift. Coming to grips with a problem immediately is better than putting it off until later. Uncorrected problem behavior tends to worsen and takes on new dimensions over time. Instead of one problem, the dilatory supervisor may discover that he has one very large problem plus a number of new ones. Discipline that is applied without undue delay has a preventive influence if only for the simple reason that the offending employee is not given time to repeat the unacceptable conduct.

A note of caution is appropriate here: the supervisor should not rush into disciplinary action. Acting swiftly is important, but is not as important as obtaining all of the facts of the situation and weighing the facts carefully to arrive at a considered and deliberate judgment.

Discipline Can Be Difficult

Discipline is a responsibility that rests squarely on the supervisor's shoulders. It cannot be passed upward to the boss or laterally to a human resources specialist. A supervisor can find lots of reasons for not giving discipline: the employee is a friend, a good person, or will get upset; the workload is too heavy right now; wait until performance appraisal time to bring it up; and, it's not a popular thing to do. These are, of course, rationalizations for avoiding a difficult responsibility.

The fact is that most employees want to work in a well-ordered environment and they recognize that discipline is an essential element of good order. While no one wants to be the object of discipline, there is an acceptance of discipline as an expected consequence of violating a rule. Employees may wish for leniency in those situations where it is deserved but not leniency across the board. They worry that overly tolerant supervision will allow a few employees to engage in violations that adversely affect everyone.

While leniency may be somewhat negotiable between a supervisor and the supervised, there can be no compromise with respect to fairness and consistency. Even a hint of unfair or discriminatory discipline can be poisonous to the process and destructive to the supervisor's reputation.

Disciplinary Principles

Principle 1: Assume Nothing. Ensure that everyone knows the rules. Put the rules in writing; make them a regular item of discussion in formal and informal sessions; disseminate and display them prominently. An employee who does not know the rules cannot be expected to follow them, and a supervisor should not discipline an employee when there is doubt that the employee was unaware of the rule.

Principle 2: Discipline in Privacy. Receiving discipline is never a pleasant experience and can be particularly unpleasant when it is received in the presence of co-workers or others who have no legitimate role in the process. Embarrassment, anger, and resentment are the natural emotions that follow criticism given publicly. Discipline is a private matter to be

handled behind closed doors or in a setting that ensures absolute privacy.

Principle 3: Be Objective. Rely on facts, not opinions and speculations. Consider all the facts and examine them with an open mind. Look for and eliminate any biases, for or against the offender. Make sure there is in fact a violation and determine the relative severity of the violation. Was the offender's act aggravated or mitigated in any way?

Principle 4: Educate the Violator. Administer discipline that is constructive. The purpose is to bring about a positive change in the violator's conduct or performance. Discipline should be a learning experience in which the violator gains new insights that contribute to personal improvement.

Principle 5: Be Consistent. Inconsistent enforcement of policy and rules should be totally unacceptable. For example, if the policy of the department is to terminate officers who sleep on the job, then all officers so caught must be terminated. To fire one and not another will breed contempt for the rules and those who set the rules.

Principle 6: Do Not Humiliate. The intended outcome is to correct, not hurt. When humiliation is made a part of the process, the offender will come away angry, resentful, and perhaps ready to fail again. Both the offender and the organization will suffer as a consequence.

Principle 7: Document Infractions. Make a record of violations. This is not to say that a negative dossier be maintained on each employee, but it does mean that instances of unacceptable performance have to be recorded. The record of an employee's failures is valuable as substantiation for severe discipline, such as termination, or as a diagnostic aid to counseling professionals.

Principle 8: Discipline Promptly. With the passage of time, an uncorrected violation fades into vagueness. The violator forgets details, discards any guilt he may have felt at the time of the violation, and rationalizes the violation as something of little importance. When opened for discussion, an uncorrected violation is likely to lead to disagreement about what "really happened" and any disciplinary action at that point can appear to be unreasonable.

Giving Clear Instructions

It is sad but true that discipline is sometimes meted out when the supervisor is partially at fault. When this occurs, it is usually not in connection with a rules violation, but with a failure of the employee to complete a task or to carry out the task in some particular way. The fault of the supervisor is in having given poor instructions.

The supervisor's instructions may not have been enunciated distinctly or presented in a logical sequence. The instructions may have been too complicated for the employee to follow, or they could have come across to the employee as intimidating or belittling. Even when an assignment is understood, it may not be completed because emotions get in the way. Asking is always better than demanding.

Following are tips on how to assign work:

- Know the assignment yourself.
- Do not assign work above the employee's ability.
- Explain the purpose of the assignment.
- Request or suggest—do not demand.
- Give brief, exact directions.
- Demonstrate if possible.
- Do not assume the employee understands perfectly.
- Do not watch every move; let the employee feel responsible.
- Let the employee know you are available to give assistance.

Most employees want to do a good job. If care is taken in giving assignments, there will be fewer failures and fewer resulting disciplinary problems.

Self-Discipline

No manager or supervisor can ever hope to discipline others effectively if he cannot discipline himself. Self-discipline is a foundation for working with other people, helping them overcome their failures, and for setting a workplace climate where good order is the norm.

Loss of temper may make a supervisor feel better for a while, but it will not improve personal performance or the performance of the supervised. Although some subordinates may quickly respond in the face of an angry outburst, the overall effect creates confusion, resentment, and loss of confidence in the supervisor as a leader.

Arguing with subordinates is a waste of everyone's time. Explaining and discussing are very necessary to good supervision because they operate to dispel misunderstanding, but when the dialogue gets argumentative, the process of communicating breaks down rapidly.

Recognizing subordinates for good work is a tried and true technique for creating harmonious working relationships. Those who use it well find that it works best when applied sparingly. Extending a great deal of recognition generally or directing it at one or a few persons reduces the effect. But certainly the greatest error in using recognition is to give the appearance of favoritism.

Consciously or subconsciously, subordinates tend to emulate their superiors. If the supervisor displays a lack of self-discipline, so will the supervised. Self-discipline in this sense goes beyond just maintaining personal composure. It deals with all manner of traits, for example, integrity, loyalty, and demeanor.

Constructive discipline is positive. It is focused on correcting unacceptable acts rather than on the personalities of the actors, and it is a process that relies more on education than on punishment. The supervisor administers discipline promptly but not hastily, objectively but leniently when appropriate, and always with fairness and consistency. Clear communications enhance the process, privacy and confidentiality cloak it, and good records provide a history.

Charles A. Sennewald

EQUAL PAY AND COMPENSATION DISCRIMINATION

The right of employees to be free from discrimination in their compensation is protected under several federal laws, including the following enforced by the U.S. Equal Employment Opportunity Commission (EEOC): the Equal Pay Act of 1963, Title VII of the Civil Rights Act of 1964, the Age Discrimination in Employment Act of 1967, and Title I of the Americans with Disabilities Act of 1990.

The Equal Pay Act requires that men and women be given equal pay for equal work in the same establishment. The jobs need not be identical, but they must be substantially equal. It is job content, not job titles, that determines whether jobs are substantially equal. Specifically, the EPA provides:

Employers may not pay unequal wages to men and women who perform jobs that require substantially equal skill, effort, and responsibility, and that are performed under similar working conditions within the same establishment. Each of these factors is summarized below:

- Skill—Measured by factors such as the experience, ability, education, and training required to perform the job. The key issue is what skills are required for the job, not what skills the individual employees may have. For example, two bookkeeping jobs could be considered equal under the EPA even if one of the job holders has a master's degree in physics, since that degree would not be required for the job.
- Effort—The amount of physical or mental exertion needed to perform the job. For example, suppose that men and women work side by side on a line assembling machine parts. The person at the end of the line must also lift the assembled product as he or she completes the work and place it on a board. That job requires more effort than the other assembly line jobs if the extra effort of lifting the assembled product off the line is substantial and is a regular part of the job. As a result, it would not be a violation to pay that person more, regardless of whether the job is held by a man or a woman.
- Responsibility—The degree of accountability required in performing the job. For example, a salesperson who is delegated the duty of determining whether to accept customers' personal checks has more responsibility than other salespeople. On the other hand, a minor difference in responsibility, such as turning out the lights at the end of the day, would not justify a pay differential.

- Working Conditions—This encompasses two factors: (1) physical surroundings like temperature, fumes, and ventilation; and (2) hazards.
- Establishment—The prohibition against compensation discrimination under the EPA applies only to jobs within an establishment. An establishment is a distinct physical place of business rather than an entire business or enterprise consisting of several places of business. However, in some circumstances, physically separate places of business should be treated as one establishment. For example, if a central administrative unit hires employees, sets their compensation, and assigns them to work locations, the separate work sites can be considered part of one establishment.

Pay differentials are permitted when they are based on seniority, merit, quantity or quality of production, or a factor other than sex. These are known as "affirmative defenses" and it is the employer's burden to prove that they apply.

In correcting a pay differential, no employee's pay may be reduced. Instead, the pay of the lower paid employee(s) must be increased.

Title VII, ADEA, and ADA

Title VII, the ADEA, and the ADA prohibit compensation discrimination on the basis of race, color, religion, sex, national origin, age, or disability. Unlike the EPA, there is no requirement under Title VII, the ADEA, or the ADA that the claimant's job be substantially equal to that of a higher paid person outside the claimant's protected class, nor do these statutes require the claimant to work in the same establishment as a comparator.

Compensation discrimination under Title VII, the ADEA, or the ADA can occur in a variety of forms. For example:

- An employer pays an employee with a disability less than similarly situated employees without disabilities and the employer's explanation (if any) does not satisfactorily account for the differential.
- A discriminatory compensation system has been discontinued but still has lingering discriminatory effects on present salaries. For example, if an employer has a compensation policy or practice that pays Hispanics lower salaries than other employees, the employer must not only adopt a new non-discriminatory compensation policy, he/she also must affirmatively eradicate salary disparities that began prior to the adoption of the new policy and make the victims whole.
- An employer sets the compensation for jobs predominately held by, for example, women or African-Americans below that suggested by the employer's job evaluation study, while the pay for jobs predominately held by men or whites is consistent with the level suggested by the job evaluation study.
- An employer maintains a neutral compensation policy or practice that has an adverse impact on employees in a protected class and cannot be justified as job-related and consistent with business necessity. For example, if an employer provides extra compensation to employees who are the "head of household," i.e., married with dependents and the primary financial contributor to the household, the practice may have an unlawful disparate impact on women.

It is also unlawful to retaliate against an individual for opposing employment practices that discriminate based on compensation or for filing a discrimination charge, testifying, or participating in any way in an investigation, proceeding, or litigation under Title VII, ADEA, ADA, or the Equal Pay Act.

Source The U.S. Equal Employment Opportunity Commission. 2006. <http://www.eeoc.gov/types/epa.html>

GRAMM-LEACH-BLILEY ACT

Information that many would consider private—including bank balances and account numbers—is regularly bought and sold by banks, credit card companies, and other financial institutions. The Gramm-Leach-Bliley Act (GLBA), which is also known as the Financial Services Modernization Act of 1999, provides limited privacy protections against the sale of private

financial information. Additionally, the GLBA codifies protections against pretexting, the practice of obtaining personal information through false pretenses.

The GLBA primarily sought to "modernize" financial services—that is, end regulations that prevented the merger of banks, stock brokerage companies, and insurance companies. The removal of these regulations, however, raised significant risks that these new financial institutions would have access to an incredible amount of personal information, with no restrictions upon its use. Prior to GLBA, an insurance company that maintained health records was distinct from the bank that mortgaged houses and stockbrokers that traded stocks. Once these companies merged, however, they would have the ability to consolidate, analyze, and sell the personal details of their customers' lives. Because of these risks, the GLBA included three simple requirements to protect the personal data of individuals:

- Banks, brokerage companies, and insurance companies must securely store personal financial information.
- The above companies must give consumers the option to opt-out of some sharing of personal financial information.
- Consumers must be advised of policies on sharing of personal financial information.

Privacy Protections

The GLBA's privacy protections only regulate financial institutions—businesses that are engaged in banking, insuring, stocks and bonds, financial advice, and investing.

First, these financial institutions, whether they wish to disclose personal information or not, must develop precautions to ensure the security and confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security or integrity of such records, and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Second, financial institutions are required to provide a notice of their information sharing policies when a person first becomes a customer, and annually thereafter. That notice must inform the consumer of the financial institutions' policies on:

- Disclosing nonpublic personal information (NPI) to affiliates and nonaffiliated third parties.
- Disclosing NPI after the customer relationship is terminated, and protecting NPI.

"Nonpublic personal information" means all information on applications to obtain financial services (credit card or loan applications), account histories (bank or credit card), and the fact that an individual is or was a customer. This interpretation of NPI makes names, addresses, telephone numbers, Social Security Numbers, and other data subject to the GLBA's data sharing restrictions.

Third, the GLBA gives consumers the right to opt-out from a limited amount of NPI sharing. Specifically, a consumer can direct the financial institution to not share information with unaffiliated companies.

Consumers have no right under the GLBA to stop sharing of NPI among affiliates. An affiliate is any company that controls, is controlled by, or is under common control with another company. The individual consumer has absolutely no control over this kind of "corporate family" trading of personal information.

There are several exemptions under the GLBA that can permit information sharing over the consumer's objection. For instance, if a financial institution wishes to engage the services of a separate company, it can transfer personal information to that company by arguing that the information is necessary to the services that the company will perform. A financial institution can transfer information to a marketing or sales company to sell new products (different stocks) or jointly offered products (co-sponsored credit cards). Once this unaffiliated third party has a consumer's personal information, it can be shared with the corporate family. However, the corporate family cannot likewise transfer the information to further companies through this exemption.

In addition, financial institutions can disclose information to credit reporting agencies, financial regulatory agencies, as part of the sale of a business, to comply with any other laws or regulations, or as necessary for a transaction requested by the consumer.

Fourth, financial institutions are prohibited from disclosing, other than to a consumer reporting agency, access codes or account numbers to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail. Thus, even if a consumer fails to "opt-out" of a financial institution's transfers, credit card numbers, PINs, or other access codes cannot be sold, as they had been in some previous cases.

Fifth, certain types of "pretexting" are prohibited by the GLBA. Pretexting is the practice of collecting personal information under false pretenses. Pretexters pose as authority figures (law enforcement agents, social workers, potential employers, etc.) and manufacture seductive stories (that the victim is about to receive a sweepstakes award or insurance payment) in order to elicit personal information about the victim. The GLBA prohibits the use of false, fictitious, or fraudulent statements or documents to get customer information from a financial institution or directly from a customer of a financial institution; the use of forged, counterfeit, lost, or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution; and asking another person to get someone else's customer information using false, fictitious, or fraudulent documents or forged, counterfeit, lost, or stolen documents.

However, investigators still can call friends, relatives, or entities not covered by the GLBA under false pretenses in order to gain information on the victim.

Source Electronic Privacy Information Center. 2005. <http://www.epic.org/privacy/glba/default.html>

IN PURSUIT OF QUALITY

Much of what is written today about quality is not very complex. Among the many themes discussed, you'll discover some old concepts hidden behind some new names, yet they're easy to miss because the current terminology sounds very technical. For example, what today is called "reengineering" is, for the most part, simply reorganizing. When asked why reengineering is necessary, organizational specialists will point out several advantages. They will begin by explaining the merits of "enhanced levels of productivity." We will read about how analyzing "cycle times"—a process initially developed for manufacturers to measure the cost associated with bringing a new product to the market—reduces costs while increasing quality. We'll also hear about structuring the workplace to achieve "added value for a greater return on investment."

These ideas and this new language may sound refreshing, but in many cases businesses are revisiting concepts and challenges that have faced managers, owners, and investors for decades.

In 1928 John Lee, controller of the Central Telegraph Office for England, addressed a group of work directors, managers, foremen, and forewomen at Oxford and detailed the pros and cons of functionalism. We can find relevance with his concepts in today's organizational gurus about the need to structure along functional lines as opposed to geographic boundaries. Many of today's Fortune 200 companies are restructuring themselves to consolidate business units based on the inner relationship of their functional utility and not demographic regions.

Simply put, today's emphasis on quality improvement is but the next step in the evolution of maximizing efficiency without diminishing effectiveness. Since early on, management theorists and practitioners have explored a wide variety of new approaches. Regardless of history or who is saying what, clearly today's emphasis is on achieving quality. In the context of customer satisfaction, quality can be pursued in a number of different ways. New concepts are being integrated with centuries-old approaches. Much of what is being advocated is an attempt to quantify quality. The mission is to establish criteria that can be measured empirically. And, in pursuing such criteria, we are somehow led to understand that we are engaging in quality efforts. Wrong! Quality is not something that can be pursued. It is an end result. Quality arrives when efficiency and effectiveness are maximized. Business executives can develop and pursue pricing strategies. They can achieve profitability and reduce production time and costs. They can do these things and more and still not achieve quality. Quality is a consequence. It has its own essence and comes only when certain elements occur in a proper alignment.

Understanding the nature of quality is critical to achieving quality. Many companies have become extremely frustrated in their attempts to pursue quality because they follow the mechanics, many of which will be discussed below. They work hard at achieving measurable, mechanical results. And when they are all done, they question whether or not their efforts were worthwhile since they fail to see quality. Others mistakenly believe that when they have completed a prescribed task list, they have achieved quality. They are convinced that completing the course means they now possess quality—whatever that means. After all, aren't they assured quality promised if they accomplish each task? Unfortunately, the answer is no.

Quality is a state of being. We know quality when we see a fine piece of furniture handcrafted by a master carpenter. We see it in art and in the design of such things as automobiles and buildings. We also see it in service performance. One of the central principles of quality is caring. People who are quality driven will accomplish improvement in carrying out tasks because they care—they want to do a good job. They take pride in their work and like the credit given to them, but they don't necessarily seek it. After all, they know that quality will be recognized naturally, and due credit will come.

I have said that quality arrives. What exactly does this mean? Perhaps an example will help. You go to a concert or a sports event. At some point in the process of watching you find that "you are into it." You are no longer just the disengaged spectator. The performer or athlete has engaged you. It's more than just cheering or applauding; you feel the experience. You're excited. You're uplifted. You identify with what is unfolding in front of you. The athletes on the field or the performers onstage have captured you because of their professional skill. Another way of putting this is to say that because they have efficiently and effectively maximized their skills, they have brought you, the customer, truer satisfaction. You know that it is quality, but you cannot measure the quality you feel. It's there. It's very real. Quality is a phenomenon that emerges. It is the blending of the science and the art and transcends the mere mechanics of a process.

Dennis Dalton

Sources

Dalton, D. 1995. *Security Management: Business Strategies for Success*. Boston: Butterworth-Heinemann.

Gulick, L. and Urwick, L. eds. 1937. *Papers on the Science of Administration*. New York: Institute of Public Administration.

Morehouse, D. 1992. *Total Quality Management: A Supervisor's Handbook*. Shawnee Mission: National Press Publications.

INTERNSHIPS: THE SECURITY MANAGER'S APPRENTICE

Internship programs provide college students with opportunities to learn on the job while receiving degree credits. Internship programs have succeeded so well that many schools require students to complete one or more as a degree requirement, and on some campuses the number of prospective interns exceeds the number of available internships. Students are often caught in a Catch-22 situation created by a degree requirement (or a personal desire) that is unmatched by opportunities to gain relevant work experience with local companies. The problem seems to be rooted in a preoccupation of business leaders with the pursuit of business goals and a failure of college administrators to effectively promote internship programs.

As a result, students in Security Management degree programs are often denied the chance to develop insights and skills that can only come from working in a security management setting. This is a damaging result both for the development of the individual and professionalization of the security field.

Employers needing to fill entry-level positions often seek candidates who have a blend of formal education, training, and related experience. A Security Management degree fills the educational requirement. The elements of training and experience, however, are often absent in the personal portfolios of candidates. The reason is that many students were too busy pursuing their degrees to be more than superficially involved in the security profession. The internship program provides learning based on meaningful work experience.

A minimum number of hours are required from the intern for the semester. In a few cases

they are paid (usually minimum wage); in most cases they are not paid. The intern is graded on participation, with the sponsor providing feedback to the school. A short-term paper describing the work is usually required and this can be reviewed by the sponsor as well.

Work and observation begins at the start of the semester and continues throughout the term. The school provides a set of expectations covering such topics as conduct, dress, and expectations of the school, supplemented by similar instructions from the sponsor. It serves a business well when internships can span two semesters. Scheduling assignments are made easier and continuity improves the quality of the work product.

A waiver can be developed addressing any inherent liability issues, if that is a matter of concern. The laws vary from state to state, and the waiver should be developed jointly with the school and the company's legal representative.

Interns should neither be used merely to supplement clerical staffing nor for mundane assignments. Obviously, there will be some duties that involve clerical effort. Interns should not be used to stand post, unless it applies specifically to their internship. They should be exposed to as many elements of the program as is permitted, including attendance at staff meetings, for example.

Interns required to comply with the National Industrial Security Program (NISP) can be processed for personnel security clearances. Since the clearance process can take several months, the interns can be exposed during the first semester to those elements of the NISP that do not require a clearance; during the second semester, after receiving clearances, they can be assigned more sensitive tasks.

Advantages and Disadvantages

The potential advantages to a business of an internship program include:

1. An intern can be a valuable contributor. This presupposes that the business has interviewed the candidate and found him/her acceptable; has placed the intern under a good supervisor; and assigned to the intern a combination of tasks that when properly performed, will result in a valuable work product or service.
2. The intern's competency and suitability for future hire as a full-time employee can be evaluated during the internship period.
3. Projects put on hold for lack of personnel can be completed through internship contributions. Projects can include conducting studies, writing procedures, and creating security awareness materials.
4. An intern program casts favorable light on the sponsoring company, both as a responsible corporate citizen in the surrounding community and as a supporter of security professionalization.

The potential disadvantages include:

1. Time devoted to the internship program may draw the sponsoring company from business objectives of greater import.
2. The sponsor may not be oriented toward training to the degree necessary to ensure good work performance by the intern and to ensure that the intern learns from the work experience.
3. Liability issues could be presented.

Joining an Internship Program

A company that agrees to participate in an internship program will need to meet the administrative requirements of the local college or university and at the same time set up its own mechanisms for selecting interns, in-processing them, assigning supervisors, reviewing their performance and learning, and returning them to the academic setting in an improved condition. Following is an outline of action steps in setting up and operating the program within the sponsoring company.

1. Interview candidates. Ensure that the company's criteria for employment can be met by the candidate. Fully discuss the company's expectations and requirements with respect to work hours, use of company equipment, care of company assets, dress, conduct, etc.

2. Obtain an understanding from the school and the intern concerning the length of the internship, the beginning and ending dates, and any days that may require the intern to be absent. Ascertain the school's requirements with respect to reports of the intern's work performance, progress, achievements, and so forth.
3. Complete all necessary paperwork, e.g., employment application, and payroll and tax forms, if applicable.
4. Subject the intern to the same pre-employment and post-employment screening processes that apply to regular employees.
5. Provide an orientation to the company and to the functions of the company's security program. Caution is needed concerning disclosure of sensitive information. Issue pertinent manuals, handbooks, procedures, guides, etc.
6. Thoroughly review safety rules, the wearing of personal protective equipment, reporting of injuries, evacuation procedures, and the like.
7. Consider an arrangement that will permit the intern to rotate within the security department to maximize his or her exposure to many functions.
8. Choose and brief a supervisor who can be counted on to obtain value for the company and the intern.
9. Take the intern on a tour of the facility to establish familiarity with parking areas, rest rooms, break areas, cafeteria, etc.
10. Introduce the intern to co-workers and other employees with whom the intern will be expected to interact.

Lonnie R. Buckels and
Robert B. Iannone

JOB TASK ANALYSIS

Reduced to its simplest level, job task analysis is a method for describing work in terms of tasks. The method is broad and includes a variety of techniques. Technique is influenced by the nature of the job and the purpose of the analysis. For example, the technique used to analyze investigative work for the purpose of determining job classifications is likely to be different from analyzing security officer work for the purpose of determining training needs.

The Task

The common factor in all techniques is the preparation of task statements. Preparation of good task statements requires having a clear understanding of the characteristics of a task. A task:

- Is visible and measurable.
- Has a clear beginning and end.
- Is of relatively short duration.
- Is always directed toward a specific purpose.
- Results in a meaningful product, service, or outcome.
- Is performed independently of other tasks.

A task is often confused with related terms, such as duty and job. A duty is a cluster of closely related tasks, and a job is a cluster of closely related duties. To illustrate, the job of security console operator is comprised of several duties, which might include evaluating alarm signals, dispatching security officers, and maintaining an activity log. Within the duty of dispatching, the console operator performs certain tasks, such as operating a radio, communicating by telephone, and prioritizing responses.

We can distinguish between job, duty, and task by applying the task definition. To operate a console cannot be a task because it has no definite beginning and end, it is not relatively short in duration, and by common understanding is a broad function. Dispatching security officers cannot be a task either because the action of dispatching involves a series of steps, such as evaluating the need to respond, setting a priority among needed responses, and deciding which officers to send. In this process, the console operator may use different pieces of equipment such as a base station radio and telephone.

Breaking a job down into its parts has the effect of finding where and how the tasks are performed. Conceptualizing how a job is carried out, determining the equipment needed for performance, and identifying the points where the job interfaces with other jobs has value. Information of this nature can be useful input to a full range of management decisions. Finding the tasks and critically examining them can help management get a fix on the tools

and equipment needed to be purchased, where they should be placed, how much space will be required, what skills and knowledge will need to be possessed by the job incumbent, and what level of compensation will be needed to attract and retain an effective performer.

The Task Inventory

Tasks are identified by persons close to the job such as the incumbents or those who directly supervise the incumbents. The means for collecting the information can be by survey, questionnaire, interview, direct observation, and by studying job descriptions, job procedures, training manuals, and the like.

Each task is expressed in a written statement that has three elements, which appear in this order:

1. An action verb that describes what is done
2. An identification of what is being acted upon
3. A clarifying phrase, if needed

The task statement is declarative and understood to contain "I" or "he" or "she." In the task statement "Prepare property removal passes," the action verb is prepare and the thing being acted upon is the pass. If property removal passes are issued only to employees, a clarifying phrase could be added so that the task statement reads, "Prepare property removal passes for employees."

A task statement tells what is done, not how or why it is done. Statements are short, to the point, and leave little room for interpretation. The action verb is unambiguous. It is better to state "test the fire alarm detectors" than to leave room for doubt by stating "Arrange to test..." or "Coordinate the testing of...."

Rating the Tasks

Rating a task means to apply to it one or more questions that are important to the purpose of the analysis effort. Following are some questions and their implications:

Q: Is the task so critical that an error in performance will result in serious consequences?
A: Prospective incumbents should (1) possess a combination of skills, knowledge, and attitude commensurate to learning the task; (2) master the task in practice situations before going on the job; (3) receive intensive initial training and frequent refresher training; and (4) be compensated at a level sufficient to attract and retain.

Q: Is performance of the task hazardous to the incumbent or others?
A: The job will most probably be subject to some form of regulatory review; safety considerations must predominate; special insurance may be appropriate to reduce risk; and task mastery will be essential.

Q: Is performance of the task in this job essential to the performance of any tasks performed in other jobs?

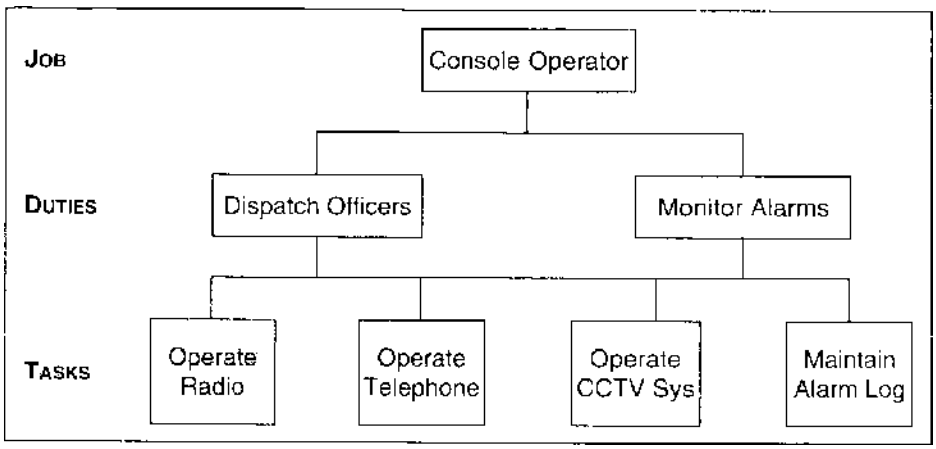


Figure 1. This chart illustrates that tasks make up a duty and that duties make up a job.

A: The incumbent will need to be informed of the relationship of the task to the work of others, and vice versa and a back-up compensating arrangement may need to be put in place.

When the question needs to be answered with more than a "yes" or a "no," the answer format can use scales, for example:

How critical is the task?

1. Not critical at all
2. Somewhat critical
3. Moderately critical
4. Critical
5. Very critical

How difficult is the task?

1. Easy
2. Easy-to-moderate
3. Moderately difficult
4. Difficult
5. Very difficult

How soon will the task be performed after the incumbent goes on the job?

1. In the first month
2. In the second month
3. In 3 to 6 months
4. In 6 to 12 months
5. After 12 months

After the persons close to the job have responded to the questions, the data are analyzed. A computer-assisted analytical procedure might be developed just for the study, or a software package might be purchased.

Task analysis can be done in a variety of ways, but all have one thing in common, i.e., they analyze jobs in terms of the ways in which work is actually performed. The approach is always objective, sometimes quantitative, and likely in many cases to lead to work improvement, which in the absence of analysis would not be possible.

John J. Fay

Sources

Fay, J. 1988. *Approaches to Criminal Justice Training, 2nd Edition*. Athens: University of Georgia.

McCormick, E. 1979. *Job Analysis: Methods and Applications*. New York: American Management Association.

MANAGEMENT: HISTORICAL ROOTS

Efforts to organize the work of people have surely existed since people started living in tribes, but few descriptions of managed work were recorded prior to about 200 years ago. Before then, work activities were fairly simple and involved relatively small groups. Typically, the workplace was tiny by contemporary standards and the workforce consisted of a single craftsman and a handful of apprentices. The craftsman was the equivalent of today's line supervisor and directly observed the work in progress. The tasks carried out by the apprentices involved relatively low levels of technology and hence were not complicated to manage.

The Industrial Revolution

In the late 18th century, the Industrial Revolution sweeping across Europe spread quickly to the United States. In his classic book, *The Wealth of Nations*, Adam Smith stole a glance into America's future when he recognized the great increases in work output offered by the use of machines.

America provided fertile ground for cultivating a system of mechanized factories. Funds needed to form manufacturing companies were willingly provided by a monied class in search of profit. The lack of tariff barriers between the states, coupled with an expanding network of roadways and waterways, facilitated large-scale movements of mass-produced goods.

Nature's generous endowment assured a large and dependable supply of raw materials. The advent of the steel plow opened the West to agricultural production, and the factories that produced farm equipment and other work-enhancing machines provided jobs that attracted large numbers of people to urban industrial centers.

The growth of the factory system led to mass employment, which in turn provided incomes that made mass consumption possible. Consumer demand for mass-produced goods enabled mass production to prosper. At

the same time, improvements being made in agricultural techniques freed a large part of the work force from food production. With abundant farm land and industrial raw materials, the young American republic developed a balance of agriculture and industry.

The Industrial Revolution was essentially a shift of the production process from small workshops to large factories. Many more people were employed, each working on only one part of the manufactured article and having little contact with those who were making the other parts. Specialization of labor introduced new requirements for managing production. Coordination of separate work efforts was crucial and at the same time more difficult to achieve.

The beginning of the Industrial Revolution was marked by the absence of recorded references to management practices. While managers likely discussed common problems among themselves and thereby improved their skills, little or no exchanges of ideas in writing were circulated and passed on to succeeding managers. In the latter part of the Industrial Revolution, descriptions of management practices began to appear mainly in the professional journals of management societies. It was during this time that the faint outlines of a management movement first appeared. The movement unfolded in three phases.

The Scientific Management Era

Frederick W. Taylor observed that workers were pretty much free to carry out their job assignments at their own paces by their own methods. He used the scientific method of logical inquiry to experiment with work methods in search of better ways to perform jobs.

Although not all of the ideas that came to be known as scientific management originated with Taylor, he brought them into a comprehensible whole, put them into operation, and verified that they worked. Taylor published his findings in *Principles of Scientific Management*. He stressed that his concepts provided a method for labor and management to work together. Taylor's pioneering efforts, however, were widely misunderstood at the time.

Taylor is often referred to as the Father of Scientific Management, but he was not the only expert in this area. Among others, Frank and Lillian Gilbreth developed the principles of motion study, through which jobs were broken into component movements and studied so that wasted motions and fatigue could be reduced. Henry L. Gantt invented the "Gantt Chart" for the scheduling of work and the checking of progress against plans.

Similar management research was taking place in Europe as well. For example, Henri Fayol, chief executive of a large French mining and metallurgical firm, studied management from the top down, with emphasis on overall administration. He published widely on management practices applicable to industrial and governmental organizations.

The Human Relations Era

The pioneers of scientific management, although clearly oriented to efficiency in production, recognized the human element in management. Elton Mayo's study of workers' social needs emphasized the need to take workers' attitudes into account and to recognize them as important contributors to production.

The emphasis by Mayo and others did not downplay the prevailing interest in efficiency. It simply added a new dimension to the field of management, i.e., that management's legitimate interest in getting the work done has to be tempered with an interest in the people who do the work. Technical systems for performing work through social interactions of workers quickly evolved, and the term *sociotechnical systems* came into use to describe the merger.

The Management Science Era

Management science had its beginnings during World War II. Mathematical analyses of data led to decisions that improved the effectiveness of the war effort. In the late 1940s these analytical methods began to be applied to problems of government and industry. Management science often involves the use of models, such as equations and formulas, to describe and provide an understanding of a problem and to identify the optimum solution.

Management science brought a change in the approach to solving work problems.

Computers and other scientific tools capable of dealing with large and complex problems are routinely used for business purposes. The modern manager is expected to have strong quantitative skills.

The Age of Technology

In the early craft shop environment, tasks were performed with humans controlling the process and providing the energy to perform the work. In the transition to mass production, people controlled the operation of machines directly but the energy was provided by another source. The next improvement was automatic control in which the machine could sense its manipulations, compare them to preset requirements, and adjust accordingly. Today's automated systems provide instructions to machines, the machines comply, and provide feedback.

Without question one of the greatest triumphs of technology was the electronic computer, and business was profoundly changed as a result. Many of the early applications were to mechanize routine clerical operations, such as payroll and accounting, and as software advanced so did the use of computers in performing more difficult work tasks.

Computer-controlled equipment can make decisions based on signals generated at the points of production. For example, automatic material-handling equipment can move objects to locations depending on the signals they receive; robots can perform operations with the items being produced; and machines equipped with racks of tools and automatic tool changers can carry out commands, all without human intervention.

While technology can be used to improve efficiency and productivity, much can be gained from new management practices. The concept of just-in-time (JIT) production, which originated in Japan, is an example. JIT is founded on the simple notion that costs can be avoided by employing a minimum of inventories to make products. Companies operating in this way coordinate their operations so that one work center produces only what is required by subsequent work centers; production is timed to occur at the moment when the necessary components arrive. Successful implementation of JIT requires reliable sources of supplies and effective preventive maintenance to avoid breakdowns on the line.

Service Sector Growth

As changes have taken place in the management field, the types of operations being managed have changed as well. Operations have spread across wider geographical areas; they have come to use more and increasingly varied technologies; they have become increasingly diversified; and the aggregate mix of operations has changed, with service operations assuming increasing importance. In this century, great changes have occurred in the American workplace. The number of persons needed to produce food has decreased while the service sector has increased. The increase in service jobs was almost three times as great as the decline in other industries—enough to absorb displaced farm workers and provide many of the additional jobs required by a growing work force.

The direction of growth has been fueled by advances in technology. The shift is clearly in the direction of service operations. Among these is the increasing demand for security-related services.

Much has been said and written about the dramatic growth and the vast future potential of the security services industry. If the past 200 years can serve as an indicator of challenges to management, lively times lie ahead. Managers in the field of security can look forward to even greater changes and greater opportunities for reward.

John J. Fay

Sources

Dilworth, J. 1986. *Production and Operations Management: Manufacturing and Nonmanufacturing*. New York: Random House.

Emmons, H., et al. 1987. *Quantitative Modeling for Decision Support*. Cleveland: Case Western Reserve University.

Heyel, C. 1982. *Encyclopedia of Management, 3rd Edition*. New York: Van Nostrand Reinhold.

Levine, S. 1984. *Dow-Jones Business and Investment Almanac*. Homewood: Dow-Jones Irwin.

MOTIVATION

The success of a Chief Security Officer (CSO) in leading subordinates rests on an ability to motivate them. The CSO needs interpersonal skills that will take him far beyond being likable and popular. Leadership is not a matter of earning admiration but of inspiring people to work together constructively. The CSO's principal task is to create a climate for work in which employee efforts are organized and directed toward the goals of the organization. To effectively discharge that task, the CSO must understand the human needs, differences, and emotions of those being supervised.

The willingness of people to apply themselves to productive work activities is linked to how much personal value they find in the work itself. The CSO's challenge is to discover what satisfactions a worker finds in a job and to harness them to the objectives of the Security Group.

Maslow's Theory of Motivation

A commonly accepted theory of motivation was advanced by A. H. Maslow. It describes people as having needs in five categories: physiological, safety, love, self-esteem, and self-actualization. According to Maslow, human needs operate in an ascending hierarchy that begins with a natural striving to satisfy the physiological needs and ends with self-actualization. In this hierarchy, which can be abstracted as a pyramid, a higher need does not provide motivation until all lower, more basic needs have been satisfied. When a need is satisfied, it ceases to be a motivator.

The physiological needs are a human's basic requirements for nourishment, water, air, and rest. A person's focus will be entirely on these needs for as long as they continue to be unmet. Once met, the individual's focus shifts upward to the next level.

At the next level is a requirement to be free from harm. The safety and security of the individual dominates. Like the underlying physiological needs, this level is concerned with survival and self-preservation.

At the third level, the individual strives for love and belonging. Affection and human relationships are the focal points.

Self-esteem comes next. These needs relate to what a person thinks of himself. They include achievement, competence, independence, status, and recognition. Self-esteem needs are similar to love needs because both are social in orientation.

The highest order of needs is self-actualization. At this level the individual expresses himself through the exercise of personal capabilities. Satisfaction is derived through self-fulfillment. It is the development of one's own potentiality and the manifestation of creative urge.

The major principles of Maslow's theory can be summed up by observing that:

- A human is a continuously wanting animal. When he is fulfilled in one need, he develops desires in another.
- When a person's needs have been satisfied, they cease to motivate. A person must be confronted with a need before he is moved to initiate, change, or sustain his behavior.
- Identical needs may be satisfied in different ways. A person who needs money will be motivated to acquire it. The method of acquisition, however, could be to earn the money or steal it.
- A given style of behavior may satisfy more than one need. A person who works hard to earn money may want the money to buy food (physiological), pay the mortgage (safety), or gain prestige (self-esteem).

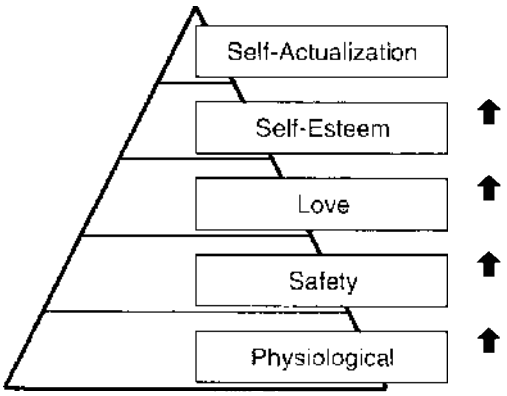


Figure 2. An individual's needs can be seen as moving upward through a series of stages.

Maslow in the Security Environment

A person's natural striving to establish human relationships and to experience self-esteem are present as much in the workplace as in any other setting. A security employee, whether working at the line level or in management, has social needs that include friendship with co-workers and acceptance within the work group. The extent and intensity of individual efforts will vary, however. An individual who satisfies social needs outside of the workplace may exhibit less striving than someone whose entire social experiences are dependent on co-workers.

Attempts to satisfy the higher needs of self-esteem are often expressed by security employees in the form of seeking recognition as a standout performer or as a valued contributor to the attainment of group goals. Most of us never stop looking for assurance that we are held in high regard by our peers, and even when we obtain that assurance today, we will seek it tomorrow and every day thereafter.

Basic to an understanding of human needs is the recognition that people respond to other people and situations as they are perceived, not as they actually are. If an employee sees work as a path to the attainment of a personal goal, he is likely to be motivated at work. A second employee may not have a goal or a goal that requires much effort and as a result will not see work as a means to realizing personal ends. A third employee may have a goal so lofty that he will view the job as an impediment.

It is not enough anymore to simply assign work. The CSO has to establish conditions, within reason, in which employees can fulfill their belonging, self-esteem, and ego needs. In some respects the CSO can be likened to a buffer that accommodates the demands of the organization and the personal needs of the employees. Using a variety of motivational techniques, the CSO can create an arrangement that allows employees to meet personal aspirations while at the same time meeting the organization's work requirements.

The CSO must appreciate that different employees will have different needs and that their needs will affect their motivations. The CSO has to recognize and assess the differences when they are manifested and to administer supervision accordingly. A critical ability in the CSO's personal inventory will be a combination of knowledge and skill that addresses the ego needs of subordinates. It is an ability resting on an understanding of motivation and a deft touch in working with people.

John J. Fay

NATIONAL ORIGIN DISCRIMINATION

Whether an employee or job applicant's ancestry is Mexican, Ukrainian, Filipino, Arab, American Indian, or any other nationality, he or she is entitled to the same employment opportunities as anyone else. EEOC enforces the federal prohibition against national origin discrimination in employment under Title VII of the Civil Rights Act of 1964, which covers employers with 15 or more employees.

> "With American society growing increasingly diverse, protection against national origin discrimination is vital to the right of workers to compete for jobs on a level playing field," said EEOC Chair Cari M. Dominguez, announcing the issuance of recent guidance on national origin discrimination. "Immigrants have long been an asset to the American workforce. This is more true than ever in today's increasingly global economy. Recent world events, including the events of September 11, 2001, only add to the need for employers to be vigilant in ensuring a workplace free from discrimination."

About National Origin Discrimination

National origin discrimination means treating someone less favorably because he or she comes from a particular place, because of his or her ethnicity or accent, or because it is believed that he or she has a particular ethnic background. National origin discrimination also means treating someone less favorably at work because of marriage or other association with someone of a particular nationality. Examples of violations covered under Title VII include:

- Employment Decisions. Title VII prohibits any employment decision, including recruitment, hiring, and firing or layoffs, based on national origin.

- Harassment. Title VII prohibits offensive conduct, such as ethnic slurs, that creates a hostile work environment based on national origin. Employers are required to take appropriate steps to prevent and correct unlawful harassment. Likewise, employees are responsible for reporting harassment at an early stage to prevent its escalation.

Language

Prohibited are:

- Accent discrimination. An employer may not base a decision on an employee's foreign accent unless the accent materially interferes with job performance.
- English fluency. A fluency requirement is only permissible if required for the effective performance of the position for which it is imposed.
- English-only rules. English-only rules must be adopted for nondiscriminatory reasons. An English-only rule may be used if it is needed to promote the safe or efficient operation of the employer's business.

Coverage of Foreign Nationals

Title VII and the other antidiscrimination laws prohibit discrimination against individuals employed in the United States, regardless of citizenship. However, relief may be limited if an individual does not have work authorization.

Source The U.S. Equal Employment Opportunity Commission. 2006. <http://www.eeoc.gov/origin/index.html>

ORGANIZATION: FORMAL AND INFORMAL ORGANIZATIONS

The Formal Organization

The organizational structure of a department within a company will reflect a logical division of tasks and clear lines of authority and responsibility, both within the department specifically and within the organization generally.

An organizational chart is two-dimensional. On the horizontal plane the chart indicates the division of work, and on the vertical plane it defines levels of authority or rank. Although all charts will reflect these two dimensions, organizational charts will differ in widely varying degrees. This is true because organizational structures are the products of the human intellect reacting to the pressures of efficiency, economy, politics, and other variables.

The reality of organizational structure is the inevitable conflict between rational and irrational issues. It might, for example, be rational, based on considerations of productivity and cost, to place a particular function in Department A. Irrational issues, such as internal politics and opportunities for personal advantage, might dictate placing the function in Department B. Conflicts and compromise are not alien to organizational charts.

A tendency in structuring an organization is to build functions around people rather than determine the functions and then fill in the boxes with qualified individuals. This tendency can be overwhelming to the security manager who is told that he has no choice except to use existing humanpower to carry out work functions, even when the functions have changed in response to crime threats. Because the existing humanpower is unequal to the real tasks, the security manager assigns functions on the basis of ability rather than genuine work needs. When this occurs, it is testimony to the questionable belief that it is easier to tinker with the organization's structure than to change the abilities of people.

The ideal structure is developed by identifying the functions that are necessary to the attainment of organizational goals, arranging the functions into logical work units, and staffing the work units with qualified people.

An organizational chart depicts what is called the formal organization, i.e., an arrangement of people designed and formally approved by management to operate in furtherance of organizational goals. An equally important arrangement of people is called the informal organization.

The Informal Organization

The informal organization also sets goals, has a hierarchy of functions and of people, and communicates among its members. Its goals and functions, however, will often conflict with

those of the formal organization, and leadership will rest on qualities other than the assignment of authority from management.

Some organizational theorists will refer to the informal organization as the "real" organization. A more accurate description might be to call it the engine that makes the formal organization work. Although the engine has been designed by management to work in particular ways, it is cantankerous and chooses to chug along in other ways that are at least tolerable and in some instances superior to expectations.

Examples of activities by the informal organization in a security organization include subordinates taking problems around the supervisor to employees they believe are better qualified even though lacking in authority, obtaining supplies and equipment through channels not officially approved, and operating "grapevine" communication networks.

Informal organizations, and there may be many within a single formal organization, exist whether management likes it or not. Some are quite obvious and even demand recognition, albeit unofficial, and others are subtle and may not even be known to or understood by management. Enlightened managements have recognized and even encouraged informal organizations. A security manager would make a serious mistake to ignore them because their opposition to security could defeat even the best practices.

Charles A. Sennewald

PERFORMANCE APPRAISAL

Performance appraisal is the ongoing process of setting objectives and assessing individual and collective behavior and achievements during a finite period of time. It is primarily about counseling and feedback on ways to improve performance at an individual and team level, and the quality of work relationships. Performance improvement results from people being clear about priorities and objectives, what skills need to be enhanced, and which types of behavior can help to this end. This comes from open, positive, and constructive discussion between supervisors, individuals, and teams, and agreement on how to focus on doing the job better.

In the appraisal process, a security manager evaluates, coaches, counsels, and develops subordinates on a continuing basis throughout the reporting period, usually 1 year. In the conduct of these activities, the manager's performance is subject to appraisal, as well.

Setting Objectives

Near the close or at the very beginning of the reporting period, the manager and his direct subordinates, individually or as a team, meet for the purpose of setting performance objectives. Objective setting ensures that the manager and the people to be rated are in agreement as to what should be achieved.

The objectives are specific, measurable, relevant, and time-related. Although firm when formulated, they can be amended and supplemented throughout the reporting period. Objectives will vary according to the type of work involved, but will normally relate to business results and expected standards of performance. Objectives can also relate to personal development. For example, the security manager may encourage a subordinate to attain the Certified Protection Professional (CPP) designation. While attainment of an objective along these lines is not directly related to a specific work output, few can dispute the job relatedness of skills and knowledge acquired in pursuit of CPP status.

To the uninitiated, objective setting may appear to be more trouble than it is worth. Objectives can be difficult to formulate and sometimes impossible to agree on. They cause problems when the manager and subordinates cannot come to terms because the objectives are irrelevant, unchallenging, or overly demanding. The manager might reject a subordinate's suggested objectives on the grounds they lack sufficient work value, are not in line with business goals, or are simply too easy. The subordinate may resist the manager's objectives (especially when they are passed down from above like Moses' tablets) because they appear inflexible or carry the risk of failure.

Posing certain questions may be helpful to manager and subordinate alike in formulating an objective:

- Does the objective make good sense? Is it important to the subordinate, the manager, the department, and the company?
- Does it mesh with departmental or organizational goals?

- Does the objective fall within the manager's area of responsibility and authority?
- Does it carry risks operationally? Financially? Politically?
- Will top management support it?
- Will the subordinate (and others who may contribute) have the knowledge, skill, and resources to complete the objective?
- Can achievement of the objective be verified in some measurable way?

For most jobs, six to eight objectives will be sufficient, and it is possible that some or all of them will change or evolve as work progresses. Objectives will sometimes be contingent upon factors beyond the manager's ability to control, such as higher-level approval of a planned project, availability of funds or equipment, and a dependence upon the work of others outside the manager's supervision.

In determining objectives, it is useful to focus on the action steps required for achievement of expectations. A single objective can incorporate several action steps. If the objective is to "develop and administer a training module for entry level security officers," the action steps could include writing a lesson plan, preparing or acquiring audiovisuals, constructing a test to measure learning, setting a training schedule, arranging for the place of training and needed training equipment, preparing certificates of completion, and making a record of attendance and scores. Time frames or deadline dates can be established for each action step, they can be programmed to occur in a particular sequence, and they can be assigned to several individuals in a team effort.

Objectives can be of two types: base and stretch. A base objective involves tasks that are integral to the job and sometimes routine in nature. Writing a report of investigation is an integral part of a security investigator's job and is fairly routine, at least to the investigator. A productivity gain might be possible by performing this task in a different manner. The manager and his investigator may agree on an objective calling for the investigator to revise the report writing method. A stretch objective goes beyond the norms of job expectations. It typically addresses a major problem, challenge, or opportunity. Achievement of the objective, if it can be done, will bring a substantial reward to the organization. It may seek to raise quality, increase productivity, reduce costs, create new markets, etc.

Once the objectives are set, they need to be put into writing, and any later changes to them should also be written down and acknowledged by the manager and subordinates with signatures or initials.

Reviewing Performance

On a continuing basis and at pre-established intervals, the manager and subordinate meet to review progress. The subordinate is invited to comment on performance with respect to the agreed objectives, highlighting areas of success, improvement, and difficulties encountered. The manager coaches and counsels as needed. A review meeting is also a time for revising, canceling, or creating objectives in light of experience.

The meeting is often documented, sometimes with the use of a form. The subordinate may be invited to comment, such as offering suggestions about how performance on particular objectives could be improved. The documentation can serve as a discussion point at the next review meeting. The usual practice is to not make any formal rating of the subordinate until the final review meeting of the reporting period.

The Performance Appraisal Cycle

Evaluation of performance is a process that continues uninterrupted. While significant events relating to performance may occur at points over time and are certainly worthy of consideration, they are not the sole criteria for making an overall judgment.

The process described here operates cyclically, that is, it transitions to a starting point from the ending point of a previous period, passes through one or more phases marked by pre-set time intervals, and moves to the starting point of the next cycle.

The Starting Point. Manager and subordinate agree on objectives for the upcoming cycle, agree on the measures that will be used to evaluate performance, and agree to meet on or about particular dates for the purpose of reviewing

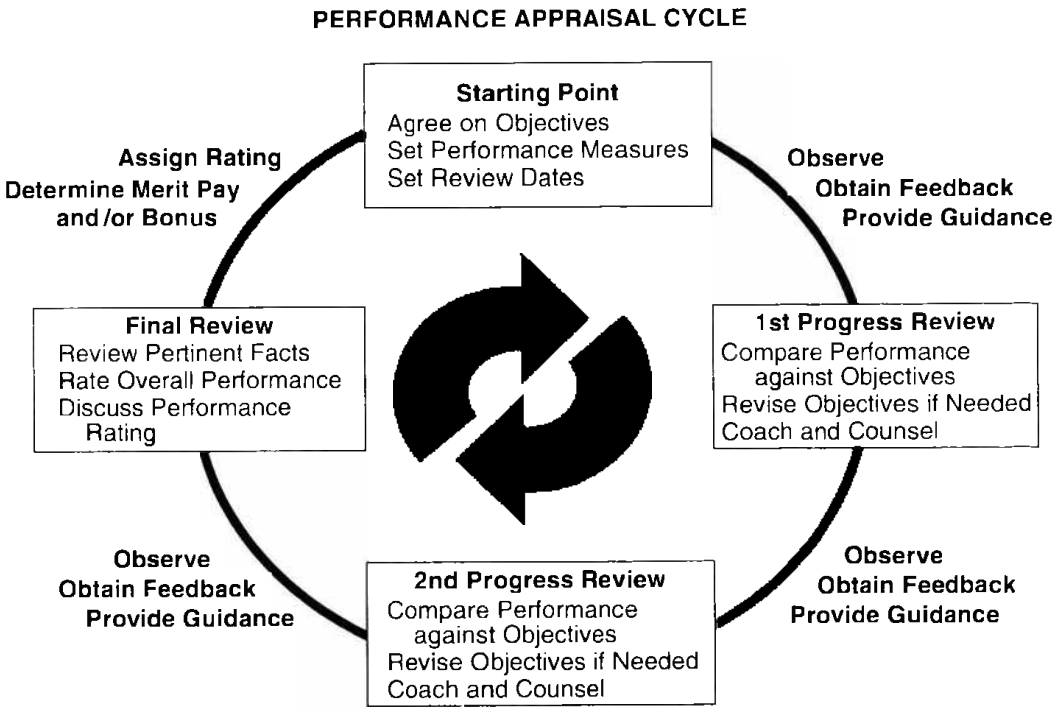


Figure 3. Performance appraisal is a continuous process with stopping points for communication between the appraiser and the person being appraised.

progress. Between progress reviews, the manager observes the subordinate's performance, obtains feedback from the subordinate, and provides appropriate guidance or assistance.

Progress Reviews. On specified dates, usually at the end of the first, second, and third quarters of the reporting period, manager and subordinate meet to compare performance against the objectives. The objectives are revised, if needed, and the subordinate is coached and counseled, if needed. During the final progress review, the subordinate's overall performance is considered, forming a foundation for a written rating.

The Ending Point. The end of one cycle and the start of the next tend to blur. Between the final progress review and the end of the cycle, the manager selects a performance rating; writes the performance report and obtains the subordinate's comments and signature on the report; determines the subordinate's merit pay increase or bonus, if any; and begins to develop with the subordinate a new set of objectives for the upcoming cycle.

Merit Rating

A chief purpose of performance appraisal is to administer salary in a manner that takes into account the separate contributions of individual employees. Through a systematic rating procedure, usually called merit rating, a manager is able to make equitable decisions regarding salary awards based on appraisal records. Despite constant complaints about the imperfections of procedures that link performance to pay, such procedures are usually objective and provide information that often cannot be obtained in any other way.

Merit ratings are designed to replace subjective, general impressions with judgments that are formed from empirically derived evidence. Generally, the evidence is quantitative in nature, capable of analysis, and collected over a period of time, such as 1 year. When soundly developed and systematically administered, merit ratings can stimulate the person being rated, particularly when the rating methodology provides opportunities for manager and subordinate to discuss ways and means for focusing performance on meaningful work outputs. This aspect of appraising is in the nature of making a "reality check."

A merit rating system requires the rater to make objective judgments and present supporting evidence. The rater is confronted with two questions: "What is the standing of the rated person, relative to others, in terms of receiving a financial reward for work contributions?" and "What proof is there to support that standing?"

Unfortunately, the appraisal process is sometimes used only as a tool for making merit, salary, and promotion determinations, as opposed to harnessing the process to the larger issue of improving productivity. In some organizations, supervisors have come to view the appraisal process as a necessary evil to be endured. They admit the process may have some value to the human resources staff but little value to the tasks of supervision or to the enhancement of work output. Appraising becomes nothing more than filling out forms.

Conducted casually, performance appraisal can be destructive. Without a clear focus and a commitment at all levels, the process can poison supervisor-subordinate relationships and seriously detract from optimum productivity. The rater and the rated person can be soured on the process and management's credibility damaged.

Evaluating human performance in the workplace is both essential and difficult. Evaluating is essential because it provides the data for making important decisions—decisions that affect the profitability of the organization and the aspirations of employees. Evaluating is difficult because it is continuous, complex, and fraught with hazards at every turn. The negative outcomes of an imperfectly administered program can be substantial, but so also are the positive outcomes.

John J. Fay

Sources

Performance Appraisal and Goal Setting. 1991. Management Paradigms, Plano, TX.

Guidance Notes on the Performance Appraisal Process. 1991. Guidance Notes, British Petroleum, London.

POSITION EVALUATION

Position evaluation is the determination of an appropriate grade level for a specific position or job. In this context, the evaluation process is focused on the nature of the job, not on the qualities of the job incumbent. Because grade level is the chief determinant of salary or wage and other job benefits, the process of position evaluation is both critical and sensitive.

Certain key pieces of information are necessary to make an accurate determination:

- The nature and function of the job
- How the job fits into the organization
- The extent of accountability built into the job, including the dimensions and quantity of accountability

Grade level determination is an attempt to systematize or make objective what would otherwise be a subjective endeavor. The employer, in trying to sort out and make sense of the comparative values of different work functions in the organization, recognizes that the best he can do is introduce some order into making what are essentially human judgments. Although many evaluation schemes use numbers and other seemingly objective criteria, the process is more art than science.

The Position Description

The basic work of evaluating positions is done by managers who assemble and analyze information about the positions to be rated. This activity often produces a document called a position (or job) description.

Although position description documents come in many sizes and varieties, the form will typically contain particular items.

Identifying Details. These include job title, department, major business unit, location, and so forth.

Nature of the Position. A description is made of the overall purpose and chief objectives of the position and the nature of activities, such as guard force management, investigations, or special projects. The description, presented in a narrative style, might begin with, "The incumbent is responsible for...," or words to that effect.

Organizational Relationships

In this section will be an identification of the person to whom the position reports, those reporting to the position, and those who hold

☐ Position Revision/Update
☐ New Position

POSITION DESCRIPTION

To Be Filled Out by HR Staff
Job Number _____
Approved By _____
Date Approved _____

Position Title: Manager of Security
Name of Person: John Q. Doe
Department: Administration
Location: Houston, Texas
Reports to: (Name) William J. Anderson (Title) Chief Executive Officer

NATURE OF POSITION

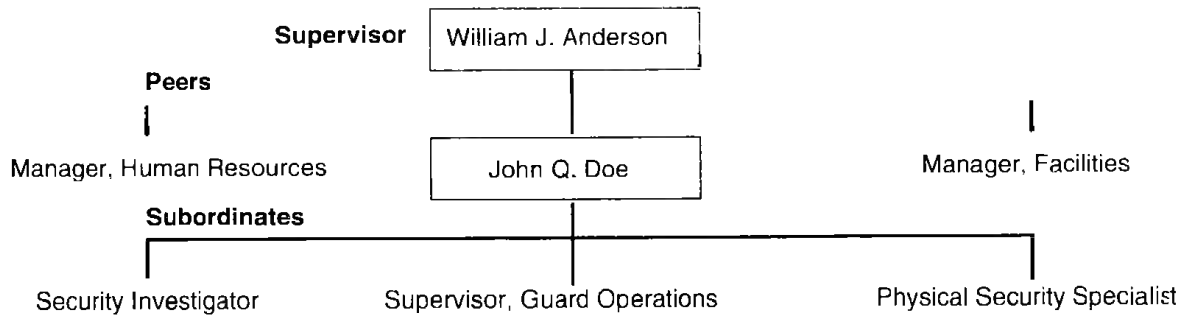
Responsible for planning, leading, organizing, and evaluating security operations at all Company locations. Identifies exposures to crime-related loss, damage, or compromise of assets, and recommends corrective actions. Carries out proactive prevention strategies, and counsels the chief executive officer and other senior managers concerning significant loss exposures and deviations from established controls. Directs investigations of criminal activity directed against the Company and unethical conduct on the part of Company employees. Maintains working relationships with peers in private sector organizations and criminal justice agencies.

This key position is responsible for providing a wide range of assets protection services which include protecting executives, implementing physical and procedural safeguards, overseeing security officer operations, and promoting security awareness among employees at all levels.

Decisions are frequently required in matters that involve complex legal and business issues. The incumbent must necessarily possess a blend of business knowledge, analytical skill, decisiveness, and practical field experience.

The major emphasis and challenge is for the incumbent to maintain an effective security program without incurring declines in efficiency and productivity.

ORGANIZATIONAL RELATIONSHIPS



POSITION DATA

Annual Budget $1.5 million **Number of Employees Supervised** 18

Education and Experience Required Baccalaureate, MBA highly desired. CPP highly desired.
Five years experience in an equivalent or lead-in position.

Figure 4. A position description form describes the job, not the person holding the job.

comparable positions. These are often displayed in the style of an organizational chart. The position titles are almost always identified and, in some organizations, the names of the incumbents are included.

In evaluating a position, it may be helpful to identify the equivalent jobs, i.e., the peers of the job holder. The salary grades of the equivalent jobs can be used as a baseline for determining the grade of the position being evaluated.

Position Data

The pertinent data for this section of the form would include the annual budget of the activity performed, the number of employees supervised, the nature and amount of funds that are affected by the incumbent, licensing, education, and experience requirements, and the extent and nature of contacts maintained by the incumbent. For example, it might be pertinent to reflect that the position of security manager requires Certified Protection Professional status, an advanced degree in business administration, and five years of responsible experience in security management or administration.

Principal Accountabilities

This section usually consists of a list of the major job tasks that the incumbent performs in accomplishing the overall purpose and chief objectives of the job. The task statements are often listed in the order of importance or frequency.

John J. Fay

Sources

Heyel, C. 1982. *Encyclopedia of Management, 3rd Edition.* New York: Van Nostrand Reinhold.

"Position Description Preparation Guide." 1992. *BP America.*

PREGNANCY DISCRIMINATION

The Pregnancy Discrimination Act is an amendment to Title VII of the Civil Rights Act of 1964. Discrimination on the basis of pregnancy, childbirth, or related medical conditions constitutes unlawful sex discrimination under Title VII, which covers employers with 15 or more employees, including state and local governments. Title VII also applies to employment agencies and to labor organizations, as well as to the federal government. Women who are pregnant or affected by related conditions must be treated in the same manner as other applicants or employees with similar abilities or limitations.

Title VII's pregnancy-related protections include:

- Hiring. An employer cannot refuse to hire a pregnant woman because of her pregnancy, because of a pregnancy-related condition or because of the prejudices of co-workers, clients, or customers.
- Pregnancy and Maternity Leave. An employer may not single out pregnancy-related conditions for special procedures to determine an employee's ability to work. However, if an employer requires its employees to submit a doctor's statement concerning their inability to work before granting leave or paying sick benefits, the employer may require employees affected by pregnancy-related conditions to submit such statements.

If an employee is temporarily unable to perform her job due to pregnancy, the employer must treat her the same as any other temporarily disabled employee. For example, if the employer allows temporarily disabled employees to modify tasks, perform alternative assignments, or take disability leave or leave without pay, the employer also must allow an employee who is temporarily disabled due to pregnancy to do the same.

Pregnant employees must be permitted to work as long as they are able to perform their jobs. If an employee has been absent from work as a result of a pregnancy-related condition and recovers, her employer may not require her to remain on leave until the baby's birth. An employer also may not have a rule that prohibits an employee from returning to work for a predetermined length of time after childbirth.

Employers must hold open a job for a pregnancy-related absence the same length of time jobs are held open for employees on sick or disability leave.

Health Insurance

Any health insurance provided by an employer must cover expenses for pregnancy-related conditions on the same basis as costs for other medical conditions. Health insurance for expenses arising from abortion is not required, except where the life of the mother is endangered.

Pregnancy-related expenses should be reimbursed exactly as those incurred for other medical conditions, whether payment is on a fixed basis or a percentage of reasonable-and-customary-charge basis.

The amounts payable by the insurance provider can be limited only to the same extent as amounts payable for other conditions. No additional, increased, or larger deductible can be imposed.

Employers must provide the same level of health benefits for spouses of male employees as they do for spouses of female employees.

Fringe Benefits

Pregnancy-related benefits cannot be limited to married employees. In an all-female workforce or job classification, benefits must be provided for pregnancy-related conditions if benefits are provided for other medical conditions.

If an employer provides any benefits to workers on leave, the employer must provide the same benefits for those on leave for pregnancy-related conditions.

Employees with pregnancy-related disabilities must be treated the same as other temporarily disabled employees for accrual and crediting of seniority, vacation calculation, pay increases, and temporary disability benefits.

It is also unlawful to retaliate against an individual for opposing employment practices that discriminate based on pregnancy or for filing a discrimination charge, testifying, or participating in any way in an investigation, proceeding, or litigation under Title VII.

Source The U.S. Equal Employment Opportunity Commission. 2006. <http://www.eeoc.gov/types/pregnancy.html>

QUALITY ASSURANCE

The pursuit of quality initiatives has taken hold in every business sector. Over the past few years many of the security giants have also developed their own programs. Others have professed to adhere to "high-quality standards" and aggressively position their marketing efforts around the theme of quality. These companies would fall into the category of "talking the talk." What makes it possible to come to this conclusion? A company is only talking the talk if it has no mechanism in place to promote quality continuously throughout the company. Regardless of how an organization frames its program, it needs to develop the following elements in order to have a true QA program:

- An articulated set of quality values
- An action plan for accomplishing each quality value
- A mechanism for soliciting customer expectations and needs
- A program that actively involves employees at each level in the decision-making and feedback process
- A program for training all employees, including managers and supervisors, in the principles of best practices and quality customer service tailored to meet the customer's needs and expectations
- A customer satisfaction program that measures satisfaction and includes a complaint resolution component
- A timely customer feedback mechanism
- A data analysis strategy that provides a springboard for continuous improvement

These eight components serve as the basic framework. If any one is missing, the program is incomplete. One of the clearest ways to test whether such a program is in place is simply to try to describe each of the components in clear language. If the descriptions are generally anecdotal, this strongly suggests that the program is either in the initial phase of development or does not include QA at all.

Asking security providers about their QA program is especially important because they may have developed a program that is limited in that it serves only those clients that require a QA program. This means that pursuit of QA is not really an integrated part of their corporate culture; instead the provider may view QA as

something that is client specific and therefore a commodity rather than a process for seeking continuous quality improvement. To determine whether a company is committed to QA or not, test its ability to demonstrate that values have been identified, action plans developed, feedback received, results measured, and that plans for revision or adjustment are in evidence.

Many high-tech companies implement very elaborate programs. Unfortunately, some fall victim to the advice of so-called QA specialists who subscribe to a philosophy that says, "If it can't be measured, graded, and forced into some formula, it can't be worth much." Tragically, their approach is fundamentally flawed when it comes to implementing the quality process. This may appear to be a somewhat harsh judgment. Unfortunately for those companies, it is. Their misguided pursuit of quality assurance has caught the attention of many critics, and rightfully so. These companies unknowingly have put themselves out of touch with what their customers want. This is because total quality management programs are more often run by technocrats.

It's also interesting to note that those who seem more likely to miss the mark are those who profess an allegiance to the Malcolm Baldrige process, a methodology used by the U.S. Department of Commerce to give recognition to companies that subscribe to rigorous criteria in implementing quality improvement. Named after a former commerce secretary, the Baldrige process has become synonymous with excellence in customer service—at least according to one school of thought. The problem for many companies is the misconception as to who is the true customer.

Rarely is security the customer. Security is the conduit for delivering a service to customers. For some reason security managers—whether they employ a resident staff or rely on external partners—believe that they are the end user. Their error is further exacerbated when they measure success in terms of turnover, response time, e-mail messages and pages received, and so forth. Although these factors are critical to achieving operational success, they reflect infrastructure issues and not true QA.

As the end users of security, internal customers want to know that their expectations and needs are being met. But are these expectations realistic? If one of the customer expectations is that each security officer will know the name of certain employees, then that becomes a QA measure. If officers don't know certain names, dinging them for not knowing is unfair and unrealistic.

This leads us to another aspect of a misguided QA program—namely, the way in which programs are measured. Some companies implement grading systems that have been taken right out of the classic high-school grading system; they evaluate security personnel using numeric scores that are converted to letter grades such as A plus through D minus.

Other companies use grading systems that do not allow for failure. This is not a point to take lightly. Such a perspective, taken to its logical end, would mean that if a security officer deliberately stood by and watched while a customer/client was brutally attacked and did nothing at all, the officer would not have failed to provide quality customer service. Failure is part of the continuous improvement process and should therefore be built into the QA program. Failing to recognize failure limits the value of the program and undercuts the seriousness of the effort.

Dennis Dalton

Source Dalton, D. 1995. *Security Management: Business Strategies for Success*. Boston: Butterworth-Heinemann.

RACE AND COLOR DISCRIMINATION

Title VII of the Civil Rights Act of 1964 protects individuals against employment discrimination on the bases of race and color, as well as national origin, sex, and religion. Title VII applies to employers with 15 or more employees, including state and local governments. It also applies to employment agencies and to labor organizations, as well as to the federal government.

Equal employment opportunity cannot be denied any person because of his/her racial group or perceived racial group, his/her race-linked characteristics (e.g., hair texture, color, facial features), or because of his/her marriage to or association with someone of a particular race or color. Title VII also prohibits employment decisions based on stereotypes and assumptions about abilities, traits, or the performance of individuals

of certain racial groups. Title VII's prohibitions apply regardless of whether the discrimination is directed at Whites, Blacks, Asians, Latinos, Arabs, Native Americans, Native Hawaiians and Pacific Islanders, multi-racial individuals, or persons of any other race, color, or ethnicity.

It is unlawful to discriminate against any individual in regard to recruiting, hiring and promotion, transfer, work assignments, performance measurements, the work environment, job training, discipline and discharge, wages and benefits, or any other term, condition, or privilege of employment. Title VII prohibits not only intentional discrimination, but also neutral job policies that disproportionately affect persons of a certain race or color and that are not related to the job and the needs of the business. Employers should adopt "best practices" to reduce the likelihood of discrimination and to address impediments to equal employment opportunity.

Recruiting, Hiring, and Advancement

Job requirements must be uniformly and consistently applied to persons of all races and colors. Even if a job requirement is applied consistently, if it is not important for job performance or business needs, the requirement may be found unlawful if it excludes persons of a certain racial group or color significantly more than others. Examples of potentially unlawful practices include: (1) soliciting applications only from sources in which all or most potential workers are of the same race or color; (2) requiring applicants to have a certain educational background that is not important for job performance or business needs; (3) testing applicants for knowledge, skills, or abilities that are not important for job performance or business needs.

Employers may legitimately need information about their employees' or applicants' race for affirmative action purposes and/or to track applicant flow. One way to obtain racial information and simultaneously guard against discriminatory selection is for employers to use separate forms or otherwise keep the information about an applicant's race separate from the application. In that way, the employer can capture the information it needs but ensure that it is not used in the selection decision.

Unless the information is for such a legitimate purpose, pre-employment questions about race can suggest that race will be used as a basis for making selection decisions. If the information is used in the selection decision and members of particular racial groups are excluded from employment, the inquiries can constitute evidence of discrimination.

Harassment/Hostile Work Environment

Title VII prohibits offensive conduct, such as racial or ethnic slurs, racial "jokes," derogatory comments, or other verbal or physical conduct based on an individual's race/color. The conduct has to be unwelcome and offensive, and has to be severe or pervasive. Employers are required to take appropriate steps to prevent and correct unlawful harassment. Likewise, employees are responsible for reporting harassment at an early stage to prevent its escalation.

Compensation and Other Employment Terms, Conditions, and Privileges

Title VII prohibits discrimination in compensation and other terms, conditions, and privileges of employment. Thus, race or color discrimination may not be the basis for differences in pay or benefits, work assignments, performance evaluations, training, discipline or discharge, or any other area of employment.

Segregation and Classification of Employees

Title VII is violated where employees who belong to a protected group are segregated by physically isolating them from other employees or from customer contact. In addition, employers may not assign employees according to race or color. For example, Title VII prohibits assigning primarily African-Americans to predominantly African-American establishments or geographic areas. It is also illegal to exclude members of one group from particular positions or to group or categorize employees or jobs so that certain jobs are generally held by members of a certain protected group. Coding applications/resumes to designate an applicant's race, by either an employer or

employment agency, constitutes evidence of discrimination where people of a certain race or color are excluded from employment or from certain positions.

Retaliation

Employees have a right to be free from retaliation for their opposition to discrimination or their participation in an EEOC proceeding by filing a charge, testifying, assisting, or otherwise participating in an agency proceeding.

Source The U.S. Equal Employment Opportunity Commission. 2006. <http://www.eeoc.gov/types/race.html>

RELIGIOUS DISCRIMINATION

Title VII of the Civil Rights Act of 1964 prohibits employers from discriminating against individuals because of their religion in hiring, firing, and other terms and conditions of employment. Title VII covers employers with 15 or more employees, including state and local governments. It also applies to employment agencies and to labor organizations, as well as to the federal government.

Employers may not treat employees or applicants more or less favorably because of their religious beliefs or practices—except to the extent a religious accommodation is warranted. For example, an employer may not refuse to hire individuals of a certain religion, may not impose stricter promotion requirements for persons of a certain religion, and may not impose more or different work requirements on an employee because of that employee's religious beliefs or practices.

Employees cannot be forced to participate—or not participate—in a religious activity as a condition of employment.

Employers must reasonably accommodate employees' sincerely held religious practices unless doing so would impose an undue hardship on the employer. A reasonable religious accommodation is any adjustment to the work environment that will allow the employee to practice his religion. An employer might accommodate an employee's religious beliefs or practices by allowing: flexible scheduling, voluntary substitutions or swaps, job reassignments and lateral transfers, modification of grooming requirements and other workplace practices, policies, and/or procedures.

An employer is not required to accommodate an employee's religious beliefs and practices if doing so would impose an undue hardship on the employer's legitimate business interests. An employer can show undue hardship if accommodating an employee's religious practices requires more than ordinary administrative costs, diminishes efficiency in other jobs, infringes on other employees' job rights or benefits, impairs workplace safety, causes co-workers to carry the accommodated employee's share of potentially hazardous or burdensome work, or if the proposed accommodation conflicts with another law or regulation.

Employers must permit employees to engage in religious expression, unless the religious expression would impose an undue hardship on the employer. Generally, an employer may not place more restrictions on religious expression than on other forms of expression that have a comparable effect on workplace efficiency.

Employers must take steps to prevent religious harassment of their employees. An employer can reduce the chance that employees will engage in unlawful religious harassment by implementing an anti-harassment policy and having an effective procedure for reporting, investigating, and correcting harassing conduct.

It is also unlawful to retaliate against an individual for opposing employment practices that discriminate based on religion or for filing a discrimination charge, testifying, or participating in any way in an investigation, proceeding, or litigation under Title VII.

Source The U.S. Equal Employment Opportunity Commission. 2006. <http://www.eeoc.gov/types/religion.html>

RETALIATION DISCRIMINATION

An employer may not fire, demote, harass, or otherwise "retaliate" against an individual for filing a charge of discrimination, participating in a discrimination proceeding, or otherwise opposing discrimination. The same laws that

prohibit discrimination based on race, color, sex, religion, national origin, age, and disability, as well as wage differences between men and women performing substantially equal work, also prohibit retaliation against individuals who oppose unlawful discrimination or participate in an employment discrimination proceeding.

In addition to the protections against retaliation that are included in all of the laws enforced by EEOC, the Americans with Disabilities Act (ADA) also protects individuals from coercion, intimidation, threat, harassment, or interference in their exercise of their own rights or their encouragement of someone else's exercise of rights granted by the ADA.

There are three main terms that are used to describe retaliation. Retaliation occurs when an employer, employment agency, or labor organization takes an **adverse action** against a **covered individual** because he or she engaged in a **protected activity**. These three terms are described below.

Adverse Action

An adverse action is an action taken to try to keep someone from opposing a discriminatory practice, or from participating in an employment discrimination proceeding. Examples of adverse actions include:

- Employment actions such as termination, refusal to hire, and denial of promotion.
- Other actions affecting employment such as threats, unjustified negative evaluations, unjustified negative references, or increased surveillance.
- Any other action such as an assault or unfounded civil or criminal charges that are likely to deter reasonable people from pursuing their rights.

Adverse actions do not include petty slights and annoyances, such as stray negative comments in an otherwise positive or neutral evaluation, "snubbing" a colleague, or negative comments that are justified by an employee's poor work performance or history.

Even if the prior protected activity alleged wrongdoing by a different employer, retaliatory adverse actions are unlawful. For example, it is unlawful for a worker's current employer to retaliate against him for pursuing an EEO charge against a former employer.

Of course, employees are not excused from continuing to perform their jobs or follow their company's legitimate workplace rules just because they have filed a complaint with the EEOC or opposed discrimination.

Covered Individuals

Covered individuals are people who have opposed unlawful practices, participated in proceedings, or requested accommodations related to employment discrimination based on race, color, sex, religion, national origin, age, or disability. Individuals who have a close association with someone who has engaged in such protected activity also are covered individuals. For example, it is illegal to terminate an employee because his spouse participated in employment discrimination litigation.

Individuals who have brought attention to violations of law other than employment discrimination are NOT covered individuals for purposes of anti-discrimination retaliation laws. For example, "whistleblowers" who raise ethical, financial, or other concerns unrelated to employment discrimination are not protected by the EEOC enforced laws.

Protected Activity

Protected activity includes:

- Opposition to a practice believed to be unlawful discrimination.
- Opposition to informing an employer that you believe that he/she is engaging in prohibited discrimination. Opposition is protected from retaliation as long as it is based on a reasonable, good-faith belief that the complained of practice violates anti-discrimination law; and the manner of the opposition is reasonable.

Examples of protected opposition include:

- Complaining to anyone about alleged discrimination against oneself or others.

- Threatening to file a charge of discrimination.
- Picketing in opposition to discrimination.
- Refusing to obey an order reasonably believed to be discriminatory.

Examples of activities that are NOT protected opposition include:

- Actions that interfere with job performance so as to render the employee ineffective.
- Unlawful activities such as acts or threats of violence.
- Participation in an employment discrimination proceeding. Participation means taking part in an employment discrimination proceeding. Participation is protected activity even if the proceeding involved claims that ultimately were found to be invalid. Examples of participation include:
  - Filing a charge of employment discrimination.
  - Cooperating with an internal investigation of alleged discriminatory practices.
  - Serving as a witness in an EEO investigation or litigation.

A protected activity can also include requesting a reasonable accommodation based on religion or disability.

Source The U.S. Equal Employment Opportunity Commission. 2006. <http://www.eeoc.gov/types/retaliation.html>

SECURITY SERVICES

Security services do not produce tangible outputs, although tangible products, such as access control hardware, are often provided or operated as an element of service. Security services are always customer-centered. The customer often has some contact with the service provider, although the customer does not have to be present when the service is actually being delivered. Each type of security service operation has its unique characteristics. When viewed in sufficient detail, a security service operation can be seen as changing through time.

Three characteristics of security service operations are known:

- Productivity generally is difficult to measure because the products of service operations are somewhat intangible. Intangible products are difficult to evaluate because they cannot be held, weighed, or measured.
- Quality standards are difficult to establish and to evaluate. No one knows for certain the amount of loss that was avoided because a security officer was present as a psychological deterrent or because the officer acted in a particular way to discourage or prevent a criminal act.
- Persons who provide security services generally have contact with the customers. The marketing and customer relations aspects of the service often overlap the operations function. For example, the relationship between the security services account representative and the client contact is often considered to be a very important component of the total services.

Managers of Security Services

Some companies have executives with titles such as vice president of operations, director of investigations, and account manager. In a good-size security services company, many persons serve in managerial positions, representing disciplines in planning, financing, marketing, and so forth. A company's management team, from the top executive right down to the supervisors of line workers, is at the center of directing and controlling services.

In working through others, managers exercise skills in two dimensions: technical competence and behavioral competence.

Technical Competence

Since managers make decisions about the tasks that other people are to perform, they need a basic understanding of the processes and technologies that drive the company's internal systems, and they need adequate knowledge of the work they manage. Technical competence is usually obtained through training and experience.

Behavioral Competence

Since managers work through others, their work necessarily involves a great deal of interpersonal contact. A good manager will have the ability to work with other people. Managers, and those being managed, often work in groups. Groups exist because people find they can achieve more, both in output and in social satisfaction, by working together.

Managers are responsible for seeing that their companies are successful. A successful security services company will meet at least three basic requirements. The services will be:

- Suited to the company's capabilities and the market's demand.
- Delivered with consistent quality at a level that appeals to customers and serves their needs.
- Provided at a cost that allows an adequate profit and a reasonable sales price.

The operations function plays a major role in accomplishing all of these requirements. Managers at the senior level must ensure that company objectives are consistent with operational capabilities and that the appropriate strengths are developed within operations to be consistent with broad, companywide strategy. In many companies the operations function consumes the greatest portion of company resources, thereby strongly impacting cost and price. Since the operations function produces services, it is largely responsible for quality.

Quality and productivity are two factors frequently mentioned as challenges facing security service companies. Achievement of high quality relates very closely to productivity. Providing a service that has to be repeated because of inadequate performance is both a quality and productivity issue. Consistently providing poor quality services leads to certain death in the services industry.

The idea of productivity is broader than just achieving high output per worker hour. It means balancing all factors of operations so that the greatest output is achieved for a given total input of all resources.

Even when security service companies offer the same menu of services, each company will be a uniquely different entity. Many factors account for the differences but the factor that clearly stands out is called management.

A security services company spends a great percentage of income and employee effort carrying out activities that stem from decisions made by managers. As these activities progress and evolve, they determine the current worth and the potential destiny of the company. A company's achievements can be enormous when all of its separate parts work in harmony and pull together to meet carefully established goals.

John J. Fay

Sources

Dilworth, J. 1986. *Production and Operations Management: Manufacturing and Nonmanufacturing*. New York: Random House.

Heyel, C. 1982. *Encyclopedia of Management, 3rd Edition*. New York: Van Nostrand Reinhold.

SEX-BASED DISCRIMINATION

Title VII of the Civil Rights Act of 1964 protects individuals against employment discrimination on the basis of sex as well as race, color, national origin, and religion. Title VII applies to employers with 15 or more employees, including state and local governments. It also applies to employment agencies and to labor organizations, as well as to the federal government.

It is unlawful to discriminate against any employee or applicant for employment because of his/her sex in regard to hiring, termination, promotion, compensation, job training, or any other term, condition, or privilege of employment. Title VII also prohibits employment decisions based on stereotypes and assumptions about abilities, traits, or the performance of individuals on the basis of sex. Title VII prohibits both intentional discrimination and neutral job policies that disproportionately exclude individuals on the basis of sex and that are not job related.

Sexual Harassment

This includes practices ranging from direct requests for sexual favors to workplace conditions that create a hostile environment for persons of either gender, including same sex harassment.

Pregnancy Based Discrimination

Title VII was amended by the Pregnancy Discrimination Act, which prohibits discrimination on the basis of pregnancy, childbirth, and related medical conditions.

The Equal Pay Act of 1963 requires that men and women be given equal pay for equal work in the same establishment. The jobs need not be identical, but they must be substantially equal. Title VII also prohibits compensation discrimination on the basis of sex. Unlike the Equal Pay Act, however, Title VII does not require that the claimant's job be substantially equal to that of a higher paid person of the opposite sex or require the claimant to work in the same establishment.

It is also unlawful to retaliate against an individual for opposing employment practices that discriminate based on sex or for filing a discrimination charge, testifying, or participating in any way in an investigation, proceeding, or litigation under Title VII.

Source The U.S. Equal Employment Opportunity Commission. 2006. <http://www.eeoc.gov/types/sex.html>

SEXUAL HARASSMENT

Sexual harassment is a form of sex discrimination that violates Title VII of the Civil Rights Act of 1964. Title VII applies to employers with 15 or more employees, including state and local governments. It also applies to employment agencies and to labor organizations, as well as to the federal government.

Unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature constitute sexual harassment when this conduct explicitly or implicitly affects an individual's employment, unreasonably interferes with an individual's work performance, or creates an intimidating, hostile, or offensive work environment.

Sexual harassment can occur in a variety of circumstances, including but not limited to the following:

- The victim as well as the harasser may be a woman or a man. The victim does not have to be of the opposite sex.
- The harasser can be the victim's supervisor, an agent of the employer, a supervisor in another area, a co-worker, or a non-employee.
- The victim does not have to be the person harassed but could be anyone affected by the offensive conduct. Unlawful sexual harassment may occur without economic injury to or discharge of the victim.
- The harasser's conduct must be unwelcome.

It is helpful for the victim to inform the harasser directly that the conduct is unwelcome and must stop. The victim should use any employer complaint mechanism or grievance system available.

When investigating allegations of sexual harassment, EEOC looks at the whole record: the circumstances, such as the nature of the sexual advances, and the context in which the alleged incidents occurred. A determination on the allegations is made from the facts on a case-by-case basis.

Prevention is the best tool to eliminate sexual harassment in the workplace. Employers are encouraged to take steps necessary to prevent sexual harassment from occurring. They should clearly communicate to employees that sexual harassment will not be tolerated. They can do so by providing sexual harassment training to their employees and by establishing an effective complaint or grievance process and taking immediate and appropriate action when an employee complains.

It is also unlawful to retaliate against an individual for opposing employment practices that discriminate based on sex or for filing a discrimination charge, testifying, or participating in any way in an investigation, proceeding, or litigation under Title VII.

Source The U.S. Equal Employment Opportunity Commission 2006. http://www.eeoc.gov/types/sexual_harassment.html

STRATEGY

Three observations about security management are in order. First, the chief security officer (CSO) operates in a rapidly changing business world. The fast-paced and highly competitive nature

of business is forcing companies to continually find new ways to be productive at lower cost. The new ways of doing business bring new security risks.

Second, every important decision made by the CSO depends upon technical knowledge. Important security decisions are never risk-free, and technical knowledge is often a critical factor in arriving at the best possible decision.

Third, international terrorism is on the scene in a very serious way. It can take many forms, is shrouded in secrecy, and threatens critical assets essential to the operation and viability of national infrastructures.

Strategic Planning

In most of the previous century, planning carried out by senior management was called long-range planning. In today's high-tech environment, it is deserving of a fancier name: strategic planning. Large companies everywhere plan strategically, and smaller companies in increasing numbers are following suit. Indeed, it can be said that in the fast-paced and intensely competitive marketplace of the new millennium any corporation worth its salt cannot afford to operate without strategic planning. According to Christopher Hoenig, a leadership guru, an organization has no choice except to engage in strategic planning. The real issues are how much planning to do, how to do it well, and when to do it.

Strategic planning underscores a point sometimes forgotten, i.e., that a business organization has two types of management. That which is done at the top is called strategic management. Everything else is operational management. Planning done at the top is strategic in nature, and planning below the top is tactical in nature. The CSO is always a developer of operating (tactical) plans, but is only sometimes involved in the development of strategic plans.

The proposition that a CSO should have a basic understanding of strategic planning rests on a number of simple observations. One is that strategic planning is a consistent element in companies that are successful. Another is that strategic planning is clearly a part of managing. Every leader is expected to understand the nature of planning and to be comfortable in its design and execution. Yet it's a fact that some leaders have such a fuzzy understanding of planning or feel threatened by it. The gains to be made to a leader personally and to his/her subordinates can be lost when the leader is excluded from strategic planning. A leader who shies away is apt to be viewed as a non-player, particularly when the planning involves the leader's sphere of operations.

Hoenig in his excellent article, "The Master Planner" (CIO, May 1, 2001) identifies what he calls Strategic Planning Elements.

- *Measurable Goals.* Specific tasks that lead to measurable goals and assign personal accountability
- *Incentives.* Rewards that make people want to carry out the plan
- *Realistic Estimates.* Ambitious outcomes grounded in reality
- *Incremental Efforts.* A division of work that organizes a big plan into achievable chunks
- *Landmarks.* Results-oriented milestones that signify progress according to plan
- *Flexibility.* A forward view that allows alternative paths and modified expectations
- *Focus.* A keen eye on the course and a steady hand at the wheel
- *Value Perspective.* A view that looks at the cost of plan execution as an investment

Policy and Planning

The relationship between policy development and strategic planning can be described as totally intimate. You can't have one without the other, and although the functions are distinguishable, they are at the same time inseparable.

A policy establishes the arena in which the actions of the business are to occur. It provides a vision for the business and, as such, serves as a guide for action. Planning, on the other hand, is the architecture of the arena; it is specific and detailed. But the main point here is that a policy broadly defines the universe of action, whereas planning is concerned with what happens inside.

Policies abound in the corporate environment. They cover staffing, growth, planning, managerial authority, conflicts of interest, marketing, production, finance, facilities, and many more. There are

also the qualitative differences in policies. Some are simply more important than others, giving credence to the term "high-level policy."

The badge of honor in the corporate environment is often the extent to which a leader is involved in policy development. The higher the policy and the more the leader shares in the decision is a determinant of status in the formal, corporate organization.

It helps to think of policies as many trees in an orchard. The gardener is the CEO. The roots of the security tree spread deep into the organization. Each root is a separate element such as security officer operations, physical security, and investigations. All roots collectively draw nutrients from the soil in the form of funding for labor and equipment. The gardener is ever watchful for blooms that produce the fruit. If the security tree does not bear fruit, the gardener will investigate and, where appropriate, change the composition of the soil, prune the unproductive limbs, or remove the tree entirely.

The CSO and Strategic Planning

Strategic plans send ripples throughout the whole of the organization. Negative ripples impacting the CSO can be lessened to the extent that the CSO participated in developing the plan. The degree of involvement by a CSO tends to be determined by three factors. First is where the CSO sits on the organizational chart. If at the lower end of the pecking order, he/she won't have much input. Second is the shape of the organization. If it is a flat organization with only few levels separating the chairman from the frontline workers, the chance for a lower-level manager to contribute is increased. Third is the personality of the CSO. If perceived as being inept or uncaring about strategic planning, he/she won't be invited to participate, no matter where located on the organizational chart and no matter the shape of the organization. If perceived as having something meaningful to contribute and willing to contribute, the CSO may be invited into the upper, upper realm.

Core and Support Activities

Nearly every business of size is organized along lines that permit simultaneous management of two main activities: the core activities at the heart of the enterprise and the support activities that contribute to the core. The core work, being essential to the business and having value that demands protection, is usually assigned to proven and trusted employees. The support work, while important to some degree, usually does not produce a significant or sustainable advantage to the business. The support staff tends to be varied, running the gamut from unskilled to highly skilled.

In a fast-evolving market where new technologies are emerging, the knowledge and skills of individuals are very limited. The technologies themselves may be proprietary and not available on the open market. If organizations can attract the knowledge and skills base of technologies, they have an advantage.

An often under-appreciated skill is the anticipation of the effect that a particular management strategy will have on the provision of security services. In the development of a company strategy, the CSO can be a key contributor by proposing measures to close security-related exposures that may arise when the strategy is implemented.

While potential exposures are not easy to detect and even more difficult to prevent or mitigate, the CSO can at least rely on the common sense observation that security risks rise when adjustments are made to the manner of work performance. A shift in strategy can move through the organization like a slow moving earthquake. Formal and informal controls on people performance that have been set in place by tested practice can be broken. Tiny fissures on the surface signal large disturbances below, foretelling eruptions that carry high risk. Loss events are waiting to happen, and it is the CSO's function to anticipate and prevent them.

Technical Knowledge

Although it is unreasonable to expect the CSO to possess a comprehensive range of technical knowledge, it is quite reasonable to expect him/her to know where to find it and to have it available on demand. Technical knowledge can be viewed as a dimension of business that operates in three human competencies: access, quality, and teamwork.

Access implies that the CSO knows where to find the right information, service, or product

at the best price. It often means building sound relationships with actual and potential vendors and networking with peers. The transfer of "best practices" among security practitioners in different companies and industries is an example of accessing technical knowledge.

Quality is the optimal balance between cost and technical excellence. It includes quality control and quality assurance. Quality control is the responsibility of the supplier; quality assurance derives naturally from confidence in the relationship. In a mature connection between client and vendor, cost and quality will occur together, to the advantage of both parties.

Teamwork is the bringing together of people who each contribute from complementary specialties. It is a competency which also gives to the players the right information, service, or product. A team or teams may be the security group or the security group in tandem with various product suppliers and consultants. Team composition will vary according to the mission, with each member contributing a different set of skills and abilities. Teamwork calls for sustained leadership and goal orientation.

Strategy and Risk

The ability to predict and quantify a full menu of risks is the CSO's highest mark of excellence.

To predict risk, which is restricted by the limitations of human understanding and available technology, is to identify the nature of threats confronting the organization and assess the probability of their occurrence.

To quantify risk is to measure potential consequences through the application of science and experience. To control risk is to logically and flexibly manage resources in ways that offset threats.

The genuinely competent CSO will obtain through continuous self-development an ability to deal with evolving threats, know where to find the technical assistance sufficient to counter them, and be positioned to acquire that assistance when it is needed.

The reader may detect the outlines of a security strategy taking shape. Integral to it are six mutually-reinforcing imperatives:

- Improve on quality and cost.
- Forge close links to customers.
- Establish close relationships with suppliers.
- Make effective use of technology.
- Operate with minimum layers of management.
- Continuously improve the security staff.

Improve on Quality and Cost. The measuring stick of security performance is high quality at reasonable cost. The facets of quality are excellence, reliability, and speedy delivery of services. The successful security operations are those that strive to be the "best in class" in all the main performance activities. A characteristic of the leading performers is an emphasis on competitive benchmarking, i.e., comparing personal and unit performance with the industry's leaders, and setting goals to measure progress.

Forge Close Links to Customers. Successful CSOs make concerted efforts to develop close ties with their customers. A customer is the user of security services. Who are the users? They are all of the persons within the organization that employs the CSO, a fact that too many CSOs lose sight of.

Forging a link is less like making friends through public relations and more like getting into "the mind" of the customer. It can happen that the CSO will know what should be in the customer's mind even before the customer becomes aware of it. Having that mental connect allows the CSO to respond rapidly and appropriately to the users of security services.

Strategy in any business context is meaningless without reference to customers. The dominant aim of strategy is to deliver superior value to customers. A persistent and unavoidable challenge of the CSO in the battle to enhance and sustain superior value is to stay one or more steps ahead of security groups that support competitors. Simply emulating what others do cannot lead to superior performance.

Establish Close Relationships with Suppliers. Too often, cooperation with suppliers is achieved through the coercive power of the buyer. The alternative described here, however, is the creation of partner relationships in which price is not always the single most important factor. Coordination with external vendors is crucial to a CSO in acquiring technical assistance in

whatever form that assistance might take, e.g., electronic countermeasures, forensic examinations, surveillance, undercover operations, etc.

If a key element of strategy is to position the in-house security staff to be a leader in using technical advances in support of the mission, it follows that the CSO will be active in developing partnerships with the suppliers of technology. The idea is to select a small number of capable suppliers and work with them. A partnership arrangement has little room for second-guessing and beating suppliers down to the last penny.

When a vendor provides contracted guard services, the CSO should forge a positive working relationship with the guard company's account manager. An understanding between them can help both parties find a balance between assuring high guard performance and recognizing the guard firm's right to supervise its own employees. If guard performance is inadequate, the CSO has a duty to offer constructive direction and the account manager has an obligation to listen and respond within reasonable limits. None of this is possible without a solid working relationship.

Make Effective Use of Technology. A security strategy linked to technology will demand of the CSO knowledge of work-enhancing technologies available in the marketplace and a skill in using them wisely. Being wise about technology involves recognizing that newer is not always better, and even when a technology is in fact superior, the final payoff has to exceed the costs of applying it. In short, technology must earn its way.

In looking for a technological solution, the CSO should not try to reinvent the wheel but at the same time not have a closed mind to a it. Common mistakes are to reject a technology that is not totally applicable but is workable in important respects, and to expect more than a technology can deliver. Very important also is to get the solution right the first time because retrofitting can be costly.

Another consideration is the working relationship between the security employees and the equipment or routines that make up the technology. This is not so much a matter of ergonomics but of the symbiotic linkage of man and machine. In companies where technology is routinely applied, the security employees are better able to adjust when a new or more complicated technology is acquired for their use.

Operate with Minimum Layers of Management. Organizational structure, i.e., the horizontal distribution of departments and the vertical arrangement of managerial layers, varies considerably from company to company. Today's trends favor greater functional integration and fewer layers of management, both of which promote speedy delivery of services and a strong responsiveness to customer needs. These are virtues to be cherished by any prudent CSO.

Execution of the security strategy in a flat, lean organization will in most cases rely upon a small, yet well-rounded staff of the highest quality, working in partnership with suppliers who bring to the arrangement a broad array of technical competencies. The competencies that stand out are in the job domains of computer security specialists, anti-surveillance technicians, auditors, architects, access control specialists, and others. The security profession, although very broad and mature, is surprisingly innovative when it comes to harnessing special talent.

Continuously Improve the Security Staff. The first five strategy elements require departures from the conventional way of dealing with employees. The changes call for developing a new mindset, a new commitment, and strong leadership. Progress will seldom be comfortable as old ideas are cast off and refashioned.

The improvement of security staff depends on the infusion of large doses of meaningful, useful knowledge. The modes of teaching can include counseling, formal classroom instruction, and on-the-job coaching. The constant in the process is unending development of employees, not merely development to get the strategy up and going, but development throughout the employees' working lifetimes.

The outcome of staff development will be technical competency, quality output, teamwork, and a flexibility that permits the acceptance of daunting challenges.

No Absolutes in Strategic Planning

Strategic planning has common elements in all competitive human endeavors, yet there is no such thing as a standard or universal system for

strategic planning. It's not possible to transfer the strategic planning mechanism of one company to another and expect it to work properly. Business organizations, even when in the same line of work, will be different in many key respects, including differences in the nature and the how of planning.

It is no accident that geniuses often occupy senior executive chairs; these are leaders whose intuition and intelligence bring them like cream to the top. Their success is seldom the result of developing a written plan and sticking to it without deviation. They tend to fly on the seat of their pants and make snap decisions intuitively, often relying on a past experience, a gut feeling, or a flash of brilliant insight. If an organization is managed by a genius, and there are many examples in the high-tech businesses of today, formal strategic planning will likely suffer, and that may be just as well. But if the CEO is not the intuitive type, strategic planning can be "set in stone." This is not altogether bad and very appropriate for mature organizations. Planning will be formalized, highly documented, based on research and input from many sources, and involve the participation of many people.

Strategy and Change

A change in strategy precipitates changes in policy which precipitates changes in plans which precipitate changes in work practices. The strategy change begins as a snowball that gets larger and larger as it rolls downhill, producing change all along the way.

The CSO must anticipate resistance to change in the security group. "But we've always done it this way" is a common cry heard when work practices change. The old ways of doing things may be so entrenched that even the best-laid preparation will falter. Engineering change even under the best of circumstances is hard work. It requires imagination, analytical ability, and fortitude.

To sum up, every company has a strategic management at the top and operational management below. Strategic plans are extensions of policy. Policy and plans are not always created with input from the CSO, but without exception, the CSO is impacted by them.

John J. Fay

Sources

Fahey, L. 1999. *Competitors.* New York: John Wiley and Sons.

Fay, J. 2006. *Contemporary Security Management.* Boston: Butterworth-Heinemann.

Hoenig, C. "The Master Planner" *CIO magazine,* May 1, 2000. 76 and 78.

Maurice, F. 1999. *Strategic Outsourcing: A Structured Approach to Outsourcing Decisions and Initiatives.* New York: American Management Association.

THRIVING FOR QUALITY

A security manager can demonstrate an ability to think beyond the limits of asset protection in several ways. One way is to propose to senior management ideas for recognizing employees and enriching their lives. Those ideas might be:

1. A charity day one day a year when employees volunteer to work for free (on one of their days off). The proceeds of their day's pay are dedicated to a charity of their choice.
2. Leverage on the distribution of payroll checks to employees by enclosing promotional items granting employees discounted prices on the company's products.
3. Negotiate discounted prices with local handymen, electricians, plumbers, and so forth, for company employees.
4. Likewise, depending on the size of the organization, senior managers, through their procurement process, could negotiate volume discounts with local merchants such as snow and water ski rental companies, bicycle companies, camping suppliers, and so forth.
5. Leverage your professional network. Whether you are a proprietary security manager or a contract provider, think of the added value that inures to you if you are able to arrange a reciprocal agreement with other security directors for your employees or clients to take advantage of the other company's services or products at a discounted rate. For example, you might know the security director of the local

museum. What a wonderful idea it would be if your employees or clients could take in a local museum show at a discounted rate by virtue of their association with you and your connections with the security director of the museum. Similar discounted rates might apply for high-tech companies, entertainment centers, and even supermarket chains.

6. Create a charity fine program. Getting employees to wear photo identification badges can be both difficult and frustrating. One way to encourage full participation is to assess a "charity's fine" for non-compliers. Anytime an employee is found not wearing his or her photo identification badge, the violating employee would be assessed a $1 fine, or more, the proceeds of which would be donated to a local charity at the end of the year.
7. Review the top twenty-five versus the bottom twenty-five. For a number of years now Wal-Mart stores have assembled the top twenty-five performing stores within a district along with the bottom twenty-five stores every Saturday. As a company they celebrate the performance of the top companies and work on ways in which they can improve the performance of the bottom twenty-five. For contract providers, there is a significant lesson in quality assurance and customer service to be learned here. Those units that are not meeting performance expectations are able to learn both successful techniques and obstacles associated with bottom-line profitability and performance.
8. Create forgiveness notes. Great organizations understand that the freedom to fail and try again applies to both operations and customer service. Success is built on failures. Some companies distribute to all of their employees GET OUT OF JAIL FREE cards. When an employee makes a mistake in his or her attempt to deliver outstanding service, he or she goes to a corporate executive, discusses what he or she has learned from the experience, turns in the GET OUT OF JAIL FREE card, and is forgiven. Think what could happen in your department if your employees realized that they had an opportunity to make an honest mistake without punishment.
9. Nordstrom's golden rule. The Nordstrom Department Store Company has developed one performance rule: Use your good judgment in all situations. Almost as an afterthought, they have attached a rider to this rule: "There will be no additional rules." In other words, employees are expected to always use good judgment, and as a result there is little reason to develop the typical three-inch binder of additional rules and regulations.
10. Got an idea? Give it away. One of the principles behind thriving is continuously striving to do something different. By encouraging your suppliers or employees to give away their best ideas, this forces them to push the envelope to try out new ideas. In other words, you cannot become complacent, since eventually you will become but one in a sea of penguins. By giving ideas away, you make room for bold thinking, thereby creating an opportunity to thrive in unsettling times.
11. Sometimes career development means moving on. As organizations trim down, more and more demands are being placed on the surviving staff. Companies need to be able to expand beyond the limits for which employees were originally hired. For some, the transition will be made regardless of whether it is easy or difficult. Unfortunately for others, the transition will never be made. Consequently, a thriving-oriented manager owes it to those struggling employees to suggest that their professional development may be better enhanced by moving on to another organization.
12. Create a professional library for others. One Atlanta based security services provider developed an extensive library, which they made available to their clients and local college students. It is an excellent way for the company

to demonstrate added value to its clients and a concern for the surrounding community.

13. Ask "Why not?" An executive for one of the country's largest radio station networks wanted to offer worldwide live broadcasting on the Internet. As he began to explore the possibilities, he was continuously confronted by specialists saying, "Well, we can't do it that way." Each time he received that answer, he responded by asking the question "Why not?" The specialists eventually began to relent and ask themselves the "Why not?" question. It didn't take long for the specialists to realize that the goal was achievable. Within a period of months, the radio station became the world's first to live-broadcast on the Internet. The lesson for security managers is that gains can be made by continuously challenging traditional approaches by asking the great "Why not?"
14. The brain problem syndrome. Thriving means having the ability to translate past mistakes into learning opportunities. I recently had an opportunity to work with a security director in the development of a new program for his company. As a contract provider, he had managed to bridge the perception of being an outside provider and was seen, for all practical purposes, as a member of his client's management team. In the process of implementing the operation of a closed-circuit television monitoring function, we discovered that a number of his officers were unfamiliar with the equipment. Initially I was surprised because the officers involved were veteran employees with an average tenure in excess of five years. When confronted with this situation, the security manager said that he would look into the matter and report back to me shortly. Later that afternoon he sought me out to report that the problem seemed to be rooted in what he termed a "brain problem syndrome." When I asked him to explain, he stated that he had made the assumption that tenured officers were experienced in the operation of CCTV systems, so he had not included them in the initial training program. This ability to acknowledge basic mistakes and quickly correct them when they were brought to his attention reinforced my perception that he was a thriving-oriented manager; a perception that was also shared by his clients.
15. Create on-line teams. With the explosion of electronic mail and the Internet, staff members located anywhere from a few feet to thousands of miles away can be electronically connected and communicate at rapid speed. The thriving-oriented manager fully understands the power associated with the ability to communicate with his entire staff, irrespective of physical distance. By putting an issue out on the Internet or company e-mail system and soliciting feedback from a variety of staff resources, the manager is able to take advantage of the multiplicity of resources available in the resident staff.
16. Creating reserve resources. As companies experience fluctuation in their labor pools, retaining experienced staff can sometimes be challenging. Consider the value of actively participating in helping employees seek temporary work assignments outside of the organization. The strategy is to position valued employees so that when circumstances change you'll have the opportunity to reintroduce them into the organization. By working out alliance relationships with companies that have high turnover rates, security companies can move their employees between employers to the advantage of everyone. The security department literally cross-trains employees with another profession, thus enabling both employers to take advantage of swings in their business cycles.

These sixteen examples illustrate how security managers, whether proprietary or external, can integrate themselves and their programs into

the overall business plan of the organization. They underscore the fact that success is tied directly to an ability to demonstrate an aptitude for thriving as opposed to struggling to survive in uncertain times.

Dennis Dalton

Source Dalton, D. 1995. *Security Management: Business Strategies for Success.* Boston: Butterworth-Heinemann.

UPWARD FEEDBACK

Upward feedback is a communication process between managers and their subordinates that can be mutually beneficial. Upward feedback has four objectives: (1) improve communication between the manager and his or her team, (2) improve teamwork, (3) identify management practices where change will result in managing people more effectively, and (4) create an action plan to which all members of the team commit.

Upward feedback is marked by open thinking, personal impact, empowerment, and networking. It can be a key tool in helping a manager understand his or her abilities to lead others.

Research into the responses of managers receiving feedback reveal a sequence of reactions called SARAH. The sequence begins with Shock, followed by Anger and Rejection, moves to Acceptance, and concludes with a request for Help.

A natural instinct is to react to what first appears to be personal criticism. When a manager is able to get past the initial surprise, annoyance, and rationalization, he or she is ready to accept the feedback as valid and then to accept help.

The Upward Feedback Process

The process usually begins by distributing a questionnaire to the persons who report to the manager. The questionnaire is anonymous and contains questions relating to management practices that are widely held to be supportive of effective teamwork. (The person filling out the questionnaire will be asked to rate each practice in certain dimensions; for example, the relative importance that the respondent places upon the practice and the degree to which the manager uses the practice.)

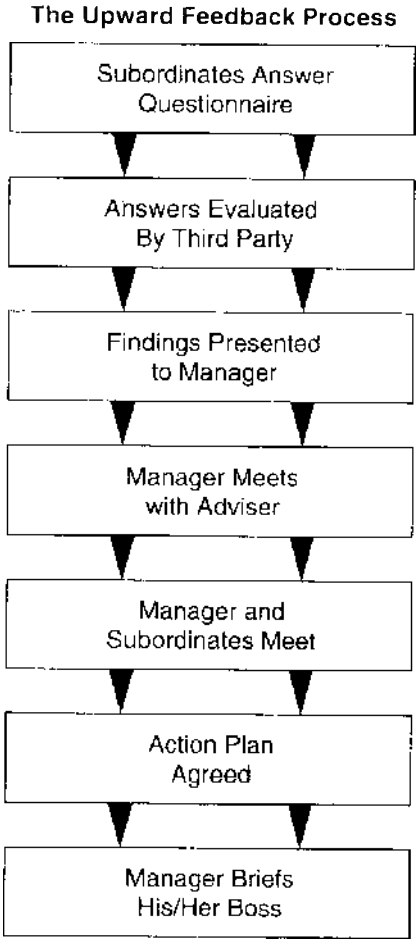


Figure 5. Upward Feedback is a process that involves three levels of employees.

The completed questionnaires are sent to a third party, such as an outside consultant or a specialist within the organization's human resources department. The questionnaires are scored, with significant variances noted. An example of a significant variance might be that the respondent considered conflict resolution within the team to be highly important but rated the manager very low in effectively resolving conflict. A report is generated in the scoring process and it may present findings in the form of numerical data, such as bar charts, and short narratives describing outstanding strengths and weaknesses.

The report provides a snapshot of team members' perceptions. The report is provided to the manager. A one-to-one meeting between the manager and an upward feedback adviser assists the manager in moving through the SARAH process. In this meeting, the manager sizes up the information, raises issues and questions with the adviser, identifies areas that need to be clarified,

and develops an agenda and a plan to meet with the team to review the findings of the report.

The next step is to hold a team meeting chaired by the manager, with the adviser present to facilitate the process. The adviser's role also includes easing the comfort level of the manager and the team, and serving as an objective third party. The role of the manager is to actively solicit observations and examples pertinent to the feedback report, listen carefully and probe for understanding, and look for improvement opportunities. The desired outcomes are that the manager will gain from the team members a clearer, truer understanding of the feedback and determine a foundation for action.

Immediately following the team meeting, the manager and the adviser confer privately. They review and obtain clarity on what was said. The adviser provides objective commentary and assists the manager in "reading between the lines." The manager is led to explore areas where change is appropriate and to make a personal commitment for improvement steps. In this regard, the manager develops a draft of a realistic action plan that incorporates personal and team objectives.

Finally, the manager sets up a meeting with his or her boss to identify ways to fully support achievement of the objectives in the action plan. Included on the agenda can be a discussion of the training, education, or other resources that may be needed to carry out the plan. The manager should circulate the agreed action plan to team members. This helps confirm that the feedback has been heard at a level higher than the manager and that commitments have been made to act on the key areas.

Following is a list of team building practices:

- Meeting frequently with employees to review their overall individual performance
- Working with people to determine realistic personal development plans
- Accurately representing the views, opinions, and feelings of staff up the line
- Anticipating future business opportunities and requirements, and planning ahead to meet them
- Maintaining the right balance of skills within the work team to meet the team's objectives
- Making problems and their cases clear so that they may be corrected
- Being effective at initiating and sustaining change
- Resolving conflicts
- Understanding and clarifying the best interests of the Company and the business unit
- Involving others in decisions where necessary
- Maintaining high standards for the team's work
- Relating the total reward system to the excellence of job performance
- Agreeing on challenging and achievable performance objectives with employees
- Sharing power in the interest of common goals
- Managing time effectively
- Providing equal development and advancement opportunities to all employees
- Creating a sense of enthusiasm about the work team's direction
- Encouraging employees to be innovative to improve the business
- Being innovative and creative in responding to changing business conditions
- Supporting and helping employees
- Making tough decisions
- Setting team and individual goals

John J. Fay

II: Emergency Management Practices

BOMB THREAT MANAGEMENT

The proposition is well accepted that the organization's chief security officer is invested with the main responsibility for managing bomb threats. Even when there has been no history of threats and no reason to believe the organization has become a target, the chief security officer must anticipate the possibility and have a program in place.

Prevention Activities

Being ready to respond to a bomb threat is one thing; taking preventive action is another. A balanced program for the management of bomb threats will include proactive steps, for example:

- Coordinate with intelligence collection units of law enforcement agencies to learn the operating locales of criminal and terrorist groups known to use bombs; stay current with new developments in bomb construction and the methods of operation of groups that use them; and determine if the organization is a potential target.
- Confer with security counterparts to learn the bomb incident experiences of other organizations. Set up information sharing agreements.
- Liaise with bomb disposal experts who can be helpful to the organization in conducting training programs for plan respondents, for employees generally, and for certain employees whose duties would bring them into contact with mail bombs. This last group would comprise mail room employees and executive secretaries.
- Control suspect packages entering the workplace. Considerations can include examining packages at an offsite location that poses minimum danger in the event of an explosion; using bomb detection equipment; and training the package examiners in the visual techniques for spotting the indicators of package bombs.
- Maintain a positive means of identifying and channeling people who enter and move within the workplace.
- Educate employees to look for and report strangers in the workplace, and educate employees and visitors alike to not leave personal items, such as briefcases and gym bags, unattended in public areas of the facility.
- Conduct periodic inspections of the workplace to identify areas where a bomb could be planted with minimum chance of detection and at the same time cause major property damage or personal injuries. The areas to think about are the facility's power plant, flammable storage rooms, telephone switching center, computer room, and executive offices.
- Educate employees, generally, and security and maintenance personnel, specifically, to be alert for suspicious persons and activities in areas that are accessible to the public, offer bomb concealment opportunities, and are sensitive in terms of damage and/or injury.
- Require security officers during each tour of duty to make random checks of public areas to look for unauthorized persons who may be hiding in or reconnoitering the facility.
- Ensure physical protection of key assets. Fire resistant safes and vaults can protect sensitive documents, cash, small valuables, magnetic media, and similar materials against bomb damage.
- Educate fire wardens and other emergency respondents to look for and report unusual activities that might signal the early stage of a bombing attempt.

An intelligent and determined adversary is likely to find a chink in even the best defensive armor. Without considering the elaborate schemes, some of the readily available means for introducing a bomb into a workplace are: on the person of an employee, by postal or commercial delivery service, and by motor vehicle into the facility's garage. Once inside, placement of a bomb is mainly a matter of the attacker's nerve

and knowledge of the premises. The attacker might choose to place the bomb in a rest room, janitor's closet, stairwell, receiving platform, lobby, or elevator.

Security management must regard, as a top priority, the degree of control exerted by the security force at access points. Control at the perimeter is the first and most important line of defense in a proactive strategy. Although most bomb threats prove to be hoaxes or are resolved by disarming the bomb before detonation, we cannot rule out the skilled attacker intent upon inflicting maximum harm without warning. The best preventive course in such a case is to deny access.

The Bomb Threat

A bomb threat is rarely made in person and sometimes is transmitted in writing. A bomb threat in writing should be handled carefully, touched by as few persons as possible, and the envelope or any other accompanying materials preserved as evidence. Observing these simple precautions can be extremely helpful to a post-incident investigation.

Nearly all bomb threats are made by telephone. Two reasons can be attributed to a bomb threat call:

The caller has certain knowledge that a bomb has been or will be placed. The caller wants to minimize personal injury or property damage by alerting persons at the target area. The caller is likely to be the bomber or an accomplice.

The caller wants to disrupt the normal activity and cause inconvenience. In most cases this type of call will not involve placement of anything, although in some few cases a simulated bomb will have been placed.

When prior preparation and practice have not been made, panic can result from a bomb threat call. Panic is an infectious fear capable of spreading quickly, and when present, the potential for injury is substantially increased. One of the ways that the potential for panic can be minimized is to train persons in how to receive a bomb threat call. Training would teach the recipient of a bomb threat call to:

- Keep the caller talking for as long as possible. Ask the caller to repeat the message. Take notes. Try to take down the exact words used by the caller.
- Ask the caller to specifically state where the bomb is located and when it is set to detonate.
- Ask what part of the facility should be evacuated first.
- Ask for a description of the bomb. What does it look like? How is it packaged? What is it made of and how does it work?
- Ask why the bomb was placed and what group is responsible. Ask the caller if he or she was the person who placed the bomb. Ask where the caller is now.
- Tell the caller that the facility is occupied and that a detonation could result in death and serious injury to many innocent people.
- Listen closely to the caller's voice. Is the caller male or female? Calm or excited? Accent? Speech impediment?
- Pay attention to background noises that may give a clue as to the caller's location. Traffic sounds, music, and voices heard in the background may be important.
- Keep the line open after the call has ended. It may be possible to trace the call.
- Notify the Security Department immediately after the caller hangs up. Be ready to be interviewed by a security representative and to pass over the notes made during the call.

A checklist form for receiving a bomb threat call can be very helpful. The form can be made a part of the training and distributed to employees for posting close to the telephone.

Formal training in how to receive a bomb threat call should be supplemented by informal refreshment through an ongoing program of security awareness and education. The objective is to condition the employees (most particularly telephone operators, receptionists, executive secretaries, and security officers) to properly receive and report a bomb threat call. The initial report triggers a cascade of notices.

Evaluating a Bomb Threat Call

The very first task of the chief security officer who has been informed of a bomb threat is to evaluate it. Interviewing the person who received the call

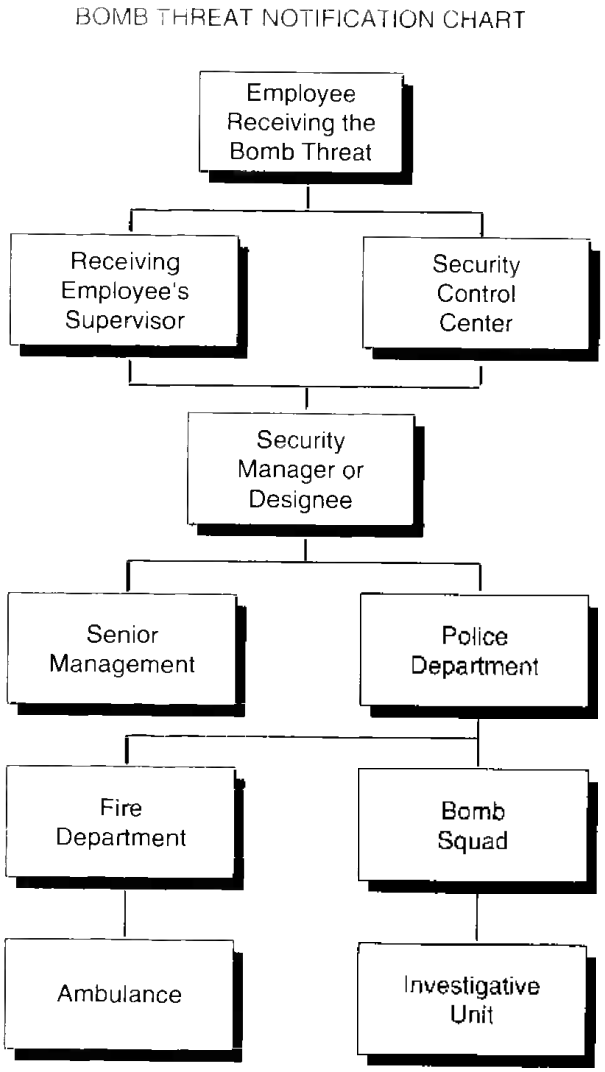


Figure 6. This chart depicts a method for initiating responses in a bomb threat situation.

and examining the notes taken during the call are preliminary to making any judgment. The evaluation takes into account the details and characteristics of the call itself, prior calls, and similar threats that have been made in the community or against counterpart organizations.

Evaluation is essentially a process of judging the credibility of the threat. Is the call a hoax or is it real? In this process, absolutes are not possible. The chief security officer is weighing probabilities and if an error is to be made, it has to be made on the side of caution. For example, in looking at the details of a call, the chief security officer may learn that the caller was a young female, probably a teenager; giggling sounds and music were heard in the background; and the caller's answer to the question as to motive was that "it seems like a good idea." In this case, the chief security officer may conclude that the call is probably a hoax.

In another case, the chief security officer may be looking at entirely different indicators, such as nervousness in the caller's voice, an expressed grievance against the organization, knowledge of the workplace or of persons who work there, and knowledge of bomb construction. The conclusion here is that the threat is probably or most probably real. When the indicators are not clear cut, the chief security officer has to act as if the threat were real.

The senior managements of many organizations will insist, as a matter of policy, that bomb threat evaluation be a shared process in which the chief security officer presents his findings to one or more senior executives before decisions are made to search or evacuate.

Search and Evacuation Options

Some organizations will require, even when searching and evacuating are deemed unnecessary, that all employees be informed of the receipt of a bomb threat and those that wish to leave may do so without penalty. The concern appears to be with the liability that may arise if a bomb explodes after the management received a warning that it chose not to disclose.

Three possible options proceed from a judgment of the threat: (1) to search without evacuating; (2) to evacuate partially or fully, and then search; and (3) to fully evacuate and not search.

Searching without Evacuating. This option is appropriate when the bomb threat call is judged to be a hoax or probable hoax. Immediate and total evacuation would at first glance seem to be the only possible response to a bomb threat. Upon close analysis, however, we can note at least two factors that operate against automatic evacuation. First, there is the matter of safety. Even the most orderly evacuation can produce injuries from tripping and falling. There is also the risk of moving large numbers of people along designated exit routes where a bomb might be planted or assembling them in an area where even a small explosive device would cause many casualties.

Evacuation is also disruptive to work. While the protection of life certainly outweighs

any economic loss, repeated threats and evacuations would soon escalate productivity losses to an unacceptable level.

Evacuating Partially or Fully and Then Searching. This option is appropriate when the call is assigned a greater degree of credibility. For example, if the caller indicates that the bomb is in a particular area, employees from that area and surrounding confines would be evacuated. Similarly, full evacuation would be appropriate if the caller is credible and indicates multiple bomb locations or refuses to name any specific location.

Fully Evacuating and Not Searching. This option is rarely taken because it is only appropriate when the call is given a high degree of credibility and when not enough time is available to conduct a search. In selecting this option, management is essentially saying it is better to get out and wait until the bomb goes off, if it goes off at all, or wait until more than sufficient time elapses to permit a conclusion that the threat was false.

These three options represent preliminary courses of action that can be changed as circumstances change. The option to search without evacuation might be upgraded if a second bomb call increased the credibility of the threat, or if during the search a suspect bomb was discovered. The size and location of a suspect bomb will influence the extent of evacuation. For example, a suspect bomb about the size of a cigarette pack that is found in a non-safety sensitive area might not require a total evacuation.

As a general rule, at least 300 feet of lateral area around a suspect bomb should be cleared of all non-essential response personnel. The vertical areas above and below a suspect bomb should also be cleared. If a suspect bomb is found on a floor of a multi-story building, the floor involved plus the floors immediately above and below should be cleared.

Does total evacuation mean that every person must leave? The answer is always yes when there is reason to believe a discovered bomb is capable of inflicting damage or injury. In the absence of that belief the answer could be no. Some persons, such as security officers and maintenance employees, may remain to perform essential life-protecting and shutdown duties when the risk to them appears to be low.

Searching Considerations

Bomb searching is in most cases conducted by persons familiar with the workplace and almost never by police officers. Public safety policy often discourages the participation of police department personnel in bomb searches on private property, unless probable cause exists to believe that a bomb is in fact present. Probable cause can be established by the details of the bomb threat call or by the discovery of a suspect bomb. With a belief established, the police are more likely to want to be actively involved in making or directing the search. Although employees at the workplace will have a greater familiarity with the possible places of bomb concealment, officers trained in bomb disposal will know how to avoid booby traps and mistakes that can lead to detonation.

Three key points need to be emphasized: (1) that the search be thorough; (2) that the search be careful; and (3) that when a suspect bomb is found, it be approached only with great caution.

Putting the key points into practice means that: (1) for a search to be thorough it is best to do it with people familiar with the physical environment, i.e., security officers, maintenance workers, and other employees who know the nooks and crannies; (2) that for a search to be careful it should be done by people who are trained, i.e., that the organization give training to its bomb searching personnel; and (3) that the dangerous nature of bomb disposal requires people with highly specialized qualifications, i.e., that a suspect bomb be approached and handled only by duly authorized and certified bomb disposal technicians.

A search team's thoroughness will be affected by the size and configuration of the workplace to be searched. It might be fair to say that making a thorough search is not easy in any working environment. Even small environments uncomplicated by multiple workstations, equipment, and labor-intensive activities will present problems. Large and complex environments, such as manufacturing plants and high-rise office buildings, are searchable on a genuinely thorough basis only with substantial expenditure of effort and time. A 20-story office building, for example, might require 48 hours of uninterrupted looking with a 20-person team

before it can be said that every conceivable hiding place has been examined.

It will seldom be possible in a large and complex environment to conduct a comprehensive search because time will not allow looking into false ceilings, examining every file cabinet, and removing panels from equipment. Neither will it be acceptable to disrupt or shut down work operations for two full working days while a search is in progress. A practical solution might be to prioritize, as part of the planning process, those places that should be thoroughly searched within the time available for searching. Note that the principle of searching with thoroughness remains uncompromised but that selectivity is introduced with respect to what should be searched.

Probability and criticality stand out in prioritizing the search effort. How probable is it that a bomber would be able to penetrate the organization's security defenses, and if the probability is high, how probable is it that a bomb or bombs would be placed in some areas as opposed to others? An evaluation of probability might lead to a search priority that concentrates on areas that are outside the umbrella of high security control, such as lobbies, garages, and other areas easily accessible to the public.

An evaluation of criticality might establish a priority for searching in areas where greatest damage can be done to the organization's most valuable assets. Criticality, however, needs to be balanced by probability. For example, it may not be sensible to set a high priority on searching the computer center when the probability is low that a bomb could be brought into the computer center without detection.

A technique associated with the prioritization of searching is the use of a card system. Each area or object to be searched is represented by a card that describes its location and other details, such as a particular telephone number to be called when the search has been completed. The cards are coded or numbered according to priority and are kept by the chief security officer or other person responsible for directing search team activities. At the search team briefing that precedes the starting of a search, the cards are handed out to team members. At the end of the search, checkmarks or signatures on the cards can provide a quick reference for ensuring that no areas were overlooked.

Search Methods

As mentioned earlier, the time requirements and the disruption of a comprehensive search make that method impractical in most cases. Two other general search methods present themselves for consideration: the non-evacuation method and the post-evacuation method.

The Non-Evacuation Method. The decision to not evacuate would be based on a judgment that the bomb threat call is a hoax and that persons in the workplace are not in danger. But because a bomb threat call is never judged to be absolutely false, a search should be made even when evacuation is not deemed appropriate.

The non-evacuation method is performed in a "walk-through" manner, but not in a cursory manner. A searcher is typically working alone, and is making searches of one or more specific areas that are likely to be occupied by employees who may or may not have been informed of the bomb threat. The searcher is typically a security officer, maintenance worker, or other person known to the employees.

The searcher moves in a steady, unhurried pace looking for objects that seem to not belong. Employees can be a source of information in determining if an object is really suspicious or simply not in its proper place. In areas where there are few or no employees present, the searcher can give closer attention to containers, closets, and areas that are out of direct sight.

The Post-Evacuation Method. When employees are absent, such as following an evacuation or during non-working hours, the searcher can move into workstations, offices, and conference rooms to examine shelves, waste baskets, storage bins, and the like. Even though each searcher can move faster when employees are not in the way, the time gained is expended in looking with more intensity. Also, if the post-evacuation search is conducted after hours, the search team will not be at full force because maintenance employees and other day workers who would normally assist in the search are likely to be off duty.

Discovery of a Suspicious Object

One of the fundamentals is to not touch a suspicious object. A searcher, however, will need to

do a certain amount of touching in the routine course of looking into, behind, and under the many items that can conceal a bomb. But at the instant a suspicious object is seen, all touching should stop. The searcher then needs to alert persons nearby to leave the area.

The next step is to notify the chief security officer or other person coordinating the search. The responsive actions that can follow include:

- Questioning employees who may be able to account for the presence of the suspicious object.
- Ordering a partial or full evacuation.
- Notifying the bomb disposal team.
- Notifying the fire department.
- Readying first aid supplies and calling for standby medical personnel and equipment.
- Asking the police to assume command of the situation.

The bomb disposal team leader or the fire officer in charge may ask for further information, such as the location of the suspect device relative to stored fuels, chemicals, flammables, power plant, and fire exits. Requests may be made to identify other possible hiding places, to open doors or windows for the purpose of dissipating blast effects, and to establish traffic control around the facility to permit free movement of emergency vehicles.

Command and Control

The chief security officer will find it advisable to pre-designate a location where the response coordinators can assemble at the outset of a bomb threat. The pre-designated location should be easily accessible to bomb incident response personnel, contain the applicable bomb threat response procedures, and have adequate communications, such as a radio network and telephones that can quickly connect to key persons inside and outside of the organization.

John J. Fay

BUSINESS CONTINUITY PLANNING

Business continuity planning is defined in many different ways, each reflecting its author's particular slant on contingency planning. Many of these definitions attempt to combine the definitions of continuity planning and of a continuity plan. There is an important distinction between the two.

Business continuity planning is a process that identifies the critical functions of an organization and that develops strategies to minimize the effects of an outage or loss of service provided by these functions. The most common strategies involve some type of third-party data center or alternate, off-site processing and alternate workspace to restore operations to a minimally acceptable level. In today's business environment, it is no longer acceptable to return to, or to achieve a minimum level of, service after a disaster.

These companies wish to, or need to, maintain operations at the current level or to take advantage of the disaster by the existence of the plan to gain market share over the competition. Disaster recovery planning is really synonymous with business continuity planning, but the term is a product of the data center. It represents the idea that recovery planning is important only to telecommunications and data centers. Business continuity planning implies recovery planning for all the critical functions or business units of an organization. Today, these terms are increasingly drifting apart. Disaster recovery refers to the reestablishment or continuity of information technology and data systems; business continuity refers to the recovery or continuity of business unit operations (systems versus people).

A business continuity plan is a comprehensive statement of consistent action taken before, during, and after a disaster or outage. The plan is designed for a worst-case scenario but should be flexible enough to address the more common, localized emergencies, such as power outages, server crashes, and fires. Although the actions listed in the plan contain sufficient detail to implement strategies designed to recover critical functions, they are more guides than inflexible dictates. Because it is not practical to plan for every type of contingency, and because each disaster has its own set of conditions, the ability to modify the plan must be incorporated.

Although a recovery plan is important, it is the planning process that returns the greatest value. This distinction is often missed by both planners and end users of continuity plans. The identification of critical functions, the thought and analysis behind the development of the strategies designed to recover the functions, and

the knowledge of why one particular strategy was selected over another are not always apparent from simply reading the plan. This is valuable knowledge when last-minute decisions are required to adapt the plan to a particular situation. The planning process is also a training exercise. The participants must think through contingencies, so that the actions required to recover from them will be already familiar. Reading the plan for the first or second time just after the disaster will provide for a less than effective recovery. This is assuming, of course, that the plan is not buried under a hundred tons of rubble.

Why Plan?

Responsibility for continuity planning often resides with the risk manager, the chief financial officer (CFO), or the data center manager. Security managers are, however, increasingly taking the role of plan developers. Their experience with the protection of assets, involvement in the identification and the mitigation of risk, and emergency response duties makes them logical choices for this role. The ability to work effectively with all levels of management is a required trait for security managers, a trait that all successful continuity planners must possess.

Some types of businesses, such as financial institutions and industries regulated by toxics laws, are required to maintain continuity plans. Businesses are increasingly regulated by laws and standards, many differing widely in their approach and requirements. Some are intended to be industry specific and others broad based. Some use differing terminology, or try to package the same methodologies in different looking boxes.

Without continuity planning, the organization may lose its competitive advantage, valuable employees, and future research. Organizations cannot insure against lost customers or a diminished public (customer) image. History consistently shows that between 35 and 50 percent of businesses never recover after major disasters.

The Planning Process

The basic steps involved in business continuity planning are simple, although their implementation can be complex and time consuming. The critical functions of the organization are identified and ranked according to their value to the organization or to their interdependencies with other critical components. Cost-effective strategies for recovering the critical functions to an acceptable level are evaluated. Once the recovery strategies are chosen, a plan is developed to implement the strategies. The plan is tested (the proper term is exercised or simulated), and provision for maintenance of the plan is established.

Before these steps commence, it is important to identify physical or procedural hazards that could cause an outage or delay the recovery process. When dealing with multiple sites, the planner should visit each location and conduct an inspection for these hazards. This inspection should identify single points of failure in critical systems, and it should produce a set of recommendations to mitigate the results of the hazards identified in the business impact or risk analysis. This is often included as part of the business impact analysis (BIA).

Next, the organization must prepare to respond to the disaster or to the emergency when it happens. The goals of emergency response are to protect the health and safety of employees, guests, and the community and to minimize damage to the organization by stabilizing the situation as quickly as possible. Response planning is not continuity planning, but the two plans can be integrated.

Once the disaster or emergency is stabilized, recovery and restoration will begin. The terms recovery, resumption, and restoration refer to separate phases of the organization's return to pre-disaster service levels (although some planners use them interchangeably).

Resumption embraces the initial, short-term strategies and steps to get back into production as quickly as possible. Moving to a hot site (a separate building or office area with duplicate, or equivalent, equipment already installed, waiting for emergency use) and transferring production to a satellite facility are examples. Recovery and restoration refer to the long-term strategies and steps the company will follow to reestablish its normal goals, service, or production levels. The replacement of a production line, installation and testing of replacement equipment, and the construction of new facilities are examples.

Project Management

Business continuity planning projects, if not properly managed, will lose momentum, languish, and die, or assume such a negative tone that the participants become hesitant to complete the project. Information and the strategic mission of an organization can rapidly change, so that once the project is started, any significant delay will cause the end product—a business continuity plan—to be outdated before it is completed.

Project management is a major skill, and it is required of anyone who undertakes responsibility for business continuity planning. It is a partnership between members of management, outside services and vendors, employees, and sometimes regulatory agencies. The ability to schedule and manage resources, time, and people will help bring the project to a successful conclusion.

Components of business continuity planning are briefly described as follows.

Identify the Planning Coordinator. A person within the organization is designated as the planning manager, coordinator, leader, or other appropriate title. This person is responsible for the management of the project (that is, the completion of the plan) and possibly for coordinating or leading the recovery effort subsequent to a disaster. The coordinator may also have major responsibilities for plan activation. Ideally, this person should be a management-level employee who has good people and project management skills and a good understanding of the organization, and is detail oriented.

Obtain Management Support and Resources. No planning effort or project will be successful without the support of upper management. This support must be communicated to all levels of management. Most agree that the development of a business continuity plan is a noble project, but all too often other priorities take precedence if participants are not held accountable to time lines and milestones. Its timely completion should be included in the goals and objectives for all expected participants.

Define the Scope and Planning Methodology. It can be a daunting, if not impossible, task to produce plans for a large, worldwide corporate structure unless the job is accomplished in small pieces. Narrow the scope of the project to a single division, site, or building, something small enough to allow a positive outcome. A successful project will add momentum for the completion of subsequent projects throughout the remainder of the organization.

Conduct Risk Identification and Mitigation Inspections. The more hazards and risks you can identify and mitigate beforehand the more you will minimize the effects of the disaster, allowing for a faster recovery.

Inspect the buildings, grounds, and community for any hazard that may injure employees, damage equipment or facilities, or cut off the supply of materials, resources, or services. When searching for these hazards, the techniques learned from scenario planning are useful. Think through the causes and effects of likely scenarios and offer recommendations to mitigate their effects.

Conduct a Business Impact Analysis. When relevant risks and hazards have been identified, submit a report to the steering committee, senior management, or the sponsor of the project outlining recommendations to mitigate the hazards. This report can be combined with the results of the BIA, especially if the analysis has been completed informally, as is too often the case.

Identify Critical Functions. The identification of critical functions is a major result of the BIA. Many planners believe it is a waste of time, effort, and resources to include in the plan functions that are not critical to the organization. Equipment and space at a hot site or other alternative location are expensive and limited; therefore, priority is given to the most important functions and employees. Remember that recovery operations are time sensitive. In many cases, there must be a logical sequence (order) of recovery actions, especially on the information technology side. Others argue that if a function is not critical, it should not be a part of the organization in the first place. I believe that every function should have a plan, but not necessarily a seat at the alternate site. Generally speaking, a critical function can be a process, service, equipment, or duty that would have one of the following impacts on the company if the function were lost or if access to it were denied:

- Affect the financial position of the company
- Have a regulatory impact
- Reduce or destroy public or customer image or confidence or sales

Develop Recovery Strategies. The number and nature of recovery strategies are determined by the nature of the business. Following are brief descriptions of some strategy choices.

- Hot, Cold, and Warm Sites. A hot site is an alternative recovery location prepared ahead of time, in this case with computers, servers, or a mainframe, and related equipment such as hardware and telecommunications. Hot-site vendors exist to provide this service on a first-come, first-served basis. The hot sites typically include a limited number of workstations and both data and voice communications infrastructure, enabling the organization to relocate employees temporarily. A cold site consists of an empty facility or leased space where computer hardware, telecommunications, and furniture would be delivered to construct a temporary processing capability. At a cold site, nothing is prewired or ready for immediate operation. Obviously, this is a less expensive strategy, but because of the time required for setup, it may not be a practical solution. Something in between a hot and cold site is a warm site.
- Relocation. Another common strategy is to simply relocate from one part of a damaged building or site to another. Executive suites, hotel rooms, client and vendor offices, empty warehouses, or mobile home trailers are other options to consider to relocate some or all of your business functions. The use of circus-type tents is generally not a good strategy.
- Work at Home. Many employees, given the proper resources ahead of time, can work effectively at home. This may free office or work space for those who can't.
- Telecommunications. Many of the strategies used to recover data systems are also used for telecommunications. These include emergency service and replacement agreements, divergent routing, radio systems (radio frequency and microwave), mobile switches, third-party call centers, and hot sites.
- Third-Party Manufacturing. Identify sole-source suppliers and take action to find alternatives far ahead of such problems. If the operation uses "just in time" manufacturing, arrange to warehouse a sufficient quantity of material to allow for delay caused by a disaster or contingent interruption. Some distributors will warehouse materials at your location, retaining ownership until the material is removed and used.
- Data Systems. Data recovery strategies include hot sites, spare or underutilized servers, the use of non-critical servers, duplicate data centers, replacement agreements, and transferring operations to other locations. Ahead of time, identify the critical applications and prioritize the order in which they are restored. If applications or operating systems are dependent on others, restore them first. Servers that are on the same network (or can be easily connected) and that have excess capacity can be pressed into service to rescue a server that has failed. Some organizations keep spare, preconfigured servers in storage for immediate replacement if a primary fails. Unfortunately, this is a very costly strategy.
- Revert to Manual Methods. More and more functions rely on automated systems to perform their work. When the automated systems fail, businesses can revert to the manual methods used before the system was automated.
- Workforce Management. Working extra shifts with the existing workforce or with temporary personnel is a simple strategy to recover from a short-term outage, especially when employees are cross-trained to perform a variety of functions.
- Reciprocal Agreements. Excess capacity at other sites, similar industries, or even competitors can be used to remain in production until damaged facilities are repaired or replaced. The protection of proprietary information, disruption of the host's operations, and fluctuations in the amount of excess capacity can make this a difficult strategy.
- Equipment Rental. If equipment is damaged or destroyed, many plans call for

their temporary replacement with rentals. List this equipment and its sources in the plan. Whenever possible, have the rental company pre-configure the equipment to your specifications. Remember that other firms may be after the same equipment, so have alternate or out-of-town sources available. Arrange for priority agreements when possible.

- Rescheduling Production. A priority task for many companies after a disaster is to determine the expected length of the outage and compare this to remaining capacity, current production schedules, critical deadlines, and pending product releases. Decide whether production schedules should be changed to concentrate on the most critical products or to eliminate others.
- Reallocation of Resources. Similar to rescheduling production, firms should reexamine the assumptions, strategies, and critical time frames and compare them to the extent of the disaster. As necessary, reallocate resources among teams, functions, or sites.
- Service-Level or Quick-Ship Agreements. Enter into agreements with manufacturers, suppliers, and repair companies to deliver replacement items and provide services within 24 hours.

Recovery Teams. Form individual recovery and continuity teams arranged along departmental lines or drawn from several departments with similar functions (and therefore with similar recovery strategies). Large departments or teams may contain sub-teams that focus on particular issues.

Train Recovery Teams. All employees are trained in some aspect of the plan, even if it is to simply make them aware of its existence. The planning process should accomplish most of the orientation and training required to implement the plan. Those with an active role in the recovery should understand all aspects of their duties and all components of the plan.

Exercise the Plan. No plan is complete until every element has been subjected to some type of testing, exercise, or simulation. Simulating the plan will validate the effectiveness of strategies, ensure the accuracy of information, and increase the preparedness of the individuals who will execute the plan. It will pinpoint areas that need attention or improvement and reveal gaps in instructions, misplaced or absent assumptions, or the need for better strategies and tasks.

Maintain the Plan. These plans must be "living documents." Employee and vendor contact numbers change often and must be kept current in the plan. This information must be reviewed quarterly. The plans must be reviewed annually to determine whether they still match the overall strategic direction of the organization, and be changed accordingly.

Review

Business continuity planning is a process that identifies a company's critical functions, develops cost-effective strategies to recover those functions if they are lost or if access to them is denied, and lists the instructions and resources necessary to implement the strategies. Systems, applications, products, and processes are prioritized and recovered in a logical manner that will allow the firm to remain in business and to retain or gain market share over competitors that don't have a continuity capability.

Eugene L. Tucker

Source Broder, J. and Tucker E. 2006. *Risk Analysis and the Security Survey, 3rd Edition.* Boston: Butterworth-Heinemann.

DATA-DRIVEN INCIDENT MANAGEMENT

Businesses and organizations today face enormous consequences from crime, especially "white-collar crime." Fraudulent and other illegal acts by company executives have in recent years caused billions of dollars in lost shareholder value. These high profile cases have caused legislated and internal controls that place greater responsibility on the boards of directors of publicly traded corporations to know what is going on and to take all reasonable steps to protect shareholder value. Many companies and organizations that are not affected by legislation, such as the Sarbanes Oxley Act, voluntarily comply with the requirements simply because they make sense.

Good corporate governance is the watchword of today. At the core of good corporate governance is appropriate response to incidents that include injuries to employees and visitors and criminal acts that negatively impact a corporation's reputation and shareholder value. It does not matter if the perpetrators are internal or external. Successful security directors understand the role professional security management plays in good corporate governance.

It should be obvious that the massive amounts of relevant data that cross security managers' desks must be turned into corporate intelligence. The only way this can be achieved is by using the power of computerized database management to track incidents, determine their root causes and their disposition. The answers to who, what, when, where, and how enable trend and relationship management which, in turn, facilitates corrective action and justifies any countermeasures. Additionally, any automated system must allow for performance measurement; as Peter Drucker stated, "If you can't measure it, you can't manage it." Most importantly, introducing measurement allows for accountability.

If an organization requires additional motivation to become serious about reputation management, all they have to consider is the vast sums of money that may be awarded by juries in cases where companies are found negligent. Good records are of paramount importance when defending against negligence, especially records that show the company to be a good corporate citizen. A demonstrable commitment to collecting and constructively acting on the information is at the heart of mitigating liability when the prosecution argues that the defending organization could have foreseen and prevented violent and other damaging events.

The types of incidents that a company or organization must document and respond to include:

- Business crime. Misappropriation of funds, corporate espionage, theft of PCs and other equipment, hijacking of high-tech products. These acts harm thousands of corporations every year.
- Violent crime. Senseless shootings on school campuses and violent attacks on fellow employees in offices and plants. These incidents cause extreme disruption, personal loss, and huge lawsuits.
- Hotels and hospitals. Aggravated assaults, rape, and murder, cause terrible human suffering as well as extensive litigation, costly settlements, and jury awards.
- Retail establishments. Chronic shoplifting, money laundering, violent robberies, and accidents of every type and level of severity.
- Financial institutions. Fraud, embezzlement, theft, robbery, and money laundering.
- All institutions. International terrorism, such as bombing buildings. Domestic terrorism includes arson and bombings at abortion clinics and vivisection research laboratories, damaging and destroying equipment that harm the ecology, planting booby troops in forests undergoing harvesting, sending chemical, biological, and explosive materials through the mail, and tampering with products.
- Computer and Internet crime. Cybercrime and cyberterrorism are increasing in number and frequency. They can and do cause enormous economic losses both to individuals (as in cases of identity theft) and businesses (as in cases of online fraud and theft of trade secrets).

Finding Information

Today's business world is a data-centric world. Decisions based on carefully analyzed data are not only more likely to be correct and bring results, they are also more readily accepted and trusted. The term "knowledge-based decisions" has gained currency as a term that describes decisions based on knowledge and insights that come from information gleaned from raw data.

Corporate security professionals need to know about and relate to these trends and capabilities, in particular, they need to think about and be sensitive to how this reality impacts their departments' operations and even their careers.

The daunting challenge for security professionals is to develop measures that protect a world of data that is growing exponentially and becoming increasingly complex. In our wired and networked world, turning on and off electronic devices, e-mailing correspondence, and faxing documents leave electronic trails and send sensitive information to what are called "data dumps."

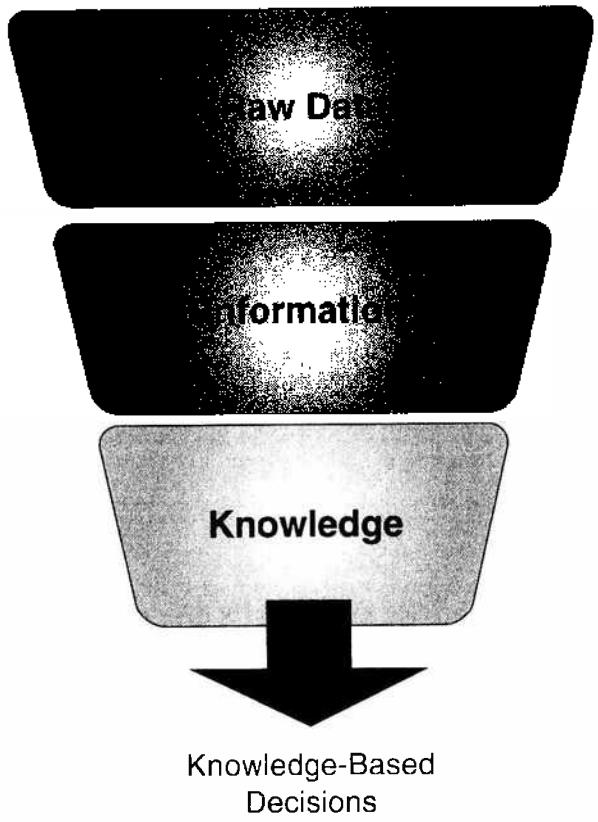


Figure 7. Information gleaned from raw data establishes a body of knowledge which becomes a foundation for intelligent decision-making.

The World of Incident Management

Incident management represents the single best opportunity for security departments to:

- Achieve "break through" status in terms of positive upper management visibility and peer respect.
- Not only justify budgets, but to also demonstrate tangible and intangible value and ROI to "stakeholders" within and outside the organization.
- Leverage the power of information to defend the organization against accusations of inadequate security and to foresee danger.

However, much progress must still be made in mindset change and the practical integration of incident management technology into daily security operations.

Challenges. For the sake of fairness, it must be pointed out that, while the incident data-information-knowledge equation is a powerful driver of best-class business performance, it is not without its challenges. Incident management practices do not happen without conscious and conscientious commitment and discipline.

For security departments, and indeed other functional departments, there are challenges to be recognized and overcome before true incident management can be realized. Meeting the challenges involve:

- Outlining or "mapping" the collection, organization and useful purpose of incident data that streams into a security department from multiple sources on a 24X7 basis.
- Understanding and ensuring the quality of incident data and the processes of data collection.

In a typical security department—and indeed in most other functional business departments—data is generated and delivered in multiple media and formats (including hand-written and word-processed documents, spreadsheets, videos, and audio or electronic transaction logs) from systems scattered throughout a site and across multiple sites. Incident reports generated

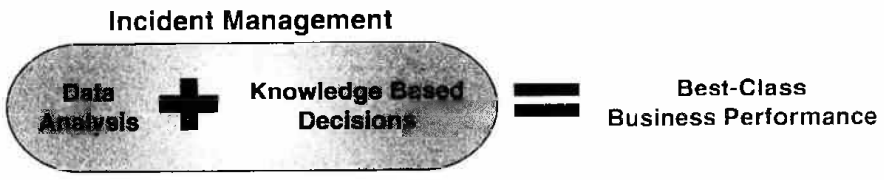


Figure 8. Superior performance in the management of incidents is the result of decisions based on meaningful knowledge.

by a monitoring station operator are often substantially different from those filed by a security supervisor or patrol officer. The formatting and completeness of security officer incident reports can vary according to the officers' skill and enthusiasm for reporting incidents.

To be really meaningful, incident data must be resident in a relational database so that it can be sorted and analyzed intelligently in order to identify patterns and trends that can point both to root causes and to the emergence of serious issues and problems. It is obvious that repeated incidents of petty cash theft in a particular department should lead to the introduction of procedural and physical measures to reduce or eliminate the thefts. On the other hand, incidents of repeated attempts by a disgruntled ex-employee to make contact with a former manager could presage a much more serious threat.

Another major challenge related to how security data is put to use is that functional "silos" within security departments can create data-collecting and data-sharing. Security can be porous and decision making erratic without established procedures for sharing data received from different systems.

A New Age of Security Management

There is a strong, if somewhat slow, trend in security management to strengthen and make more consistent the management of security information. This trend is driven, in no small measure, by the much broader corporate interest in data analysis and knowledge-based decision making. There is also relentless pressure to improve the speed and quality of decision-making, reduce costs, improve productivity, and demonstrate a commitment to best practices.

Data-Driven Security Myths. While it may be relatively easy to appreciate the macro-level, idealistic virtues of incident management automation, the change such technology causes can be unsettling. It is also true that a new, high-tech approach to such old problems as crime is not a panacea. Nonetheless, change in the security industry is deep and broad. The trend can, and must, be understood and used for good advantage—and doing so requires an understanding of the myths, realities, and emerging benefits that change offers.

Disclosure and Foreseeability. At professional conferences and in customer meetings, the question is sometimes asked, "Could actually knowing what we currently do not know end up hurting us?" The short answer is that, as with most issues in life, it is better to know than not know. For example, the courts have held in some cases that there is a duty to know. Also, potentially damaging information in a matter being litigated can be uncovered through the process of legal discovery despite attempts to hide or ignore the information.

An ancillary, but significant, benefit to having a data-driven, automated incident management program is that a company has more control of its destiny in a lawsuit that alleges failure to establish reasonable security measures to prevent foreseeable injury or damage to others. Company counsel stands a better chance of shaping, and even limiting, a court-ordered demand for information related to an allegation of negligence.

Compliance, Risk Management and Insurance. It is sometimes pointed out that one of the curiosities of the security industry is that it is virtually unregulated and follows no independent standards. The finance and accounting professions follow a myriad of government and professional standards, practices, and reporting requirements. Most human resource policies and procedures are likewise shaped by legislative mandates and regulations. In the realm of safety, there have long been OSHA guidelines, industry standards, and fire codes that influence the ways in which security is operated and managed.

An increasingly important driver of change in the security industry will be heightened levels of government regulation and the emergence of recognized professional standards for security that will inevitably trigger compliance and disclosure requirements. Even the foremost world security association, ASIS International, has acknowledged the requirement for standards by establishing a program for articulating standards for basic security processes.

Clearly, the ability of security managers to prepare such disclosures will require the adoption of data-driven security practices. Incident management and reporting will be at the heart of both regulatory compliance and, more importantly, the ability of organizations and corporations to improve their security and reduce losses.

We would also point to the obvious relevance and expanding interaction among security departments, corporate risk management departments, and insurance companies. The risk management profession has, over many decades, built a substantial body of knowledge that has been drawn primarily from the mathematical, statistical, and actuarial sciences. It is now possible to quantify all kinds of corporate business risk. This allows companies to "finance" as much risk as they can afford; for example, entering into risky yet seemingly profitable business ventures and covering potential losses by purchasing insurance policies.

In an environment of serious, and potentially costly, risk caused by high-stakes crime and terrorist attacks, documented security practices and incident management reports can be a powerful, proactive risk management tool. Because a professional security program can prevent, or at least minimize, many types of losses, companies can make their security programs a positive element in negotiations with insurers.

Conversely, insurers have begun to require that certain coverage—including kidnap and ransom and premises liability converge—requires companies to engage the services of security consultants and to install reasonable safeguards.

Return on Investment (ROI)

Incident management is the keystone in the architecture of a data-driven security program. Without this capability, security management will remain mired in the conventional model of intuitive and reactionary decisions that lead to erratic practices. Security managers will continue to struggle to deliver management reports that reflect an understanding of the company's business. A date-driven security program can aid budget development and justify security expenditures.

Today's incident management practices make possible a "closed loop" of security program design, budgeting, implementation, measurement, and improvement. Rather than relying on intuitive and anecdotal assessments of security program effectiveness, security executives can generate crisp management reports that capture specific reductions or increases in all incident categories.

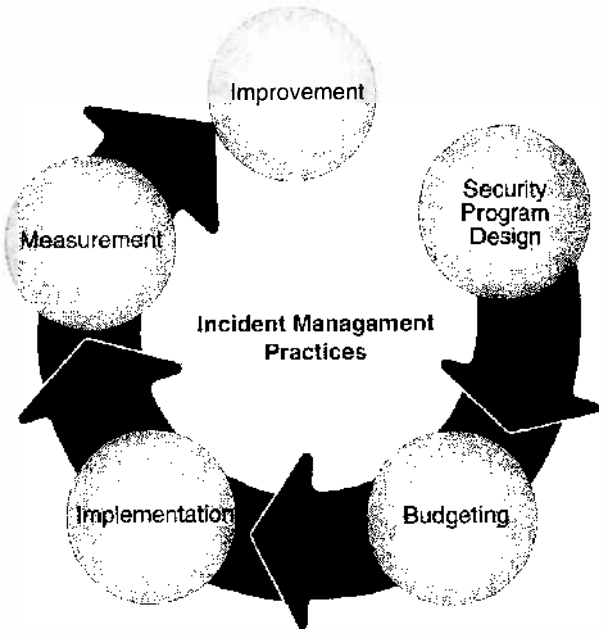


Figure 9. Incident management practices move in a five-step cycle.

Incident management systems also can project adverse incidents and their costs. Using factual data:

- Security resources can be more effectively deployed, thereby maximizing ROI.
- The relative effectiveness of individual security safeguards and a mix of safeguards can be tracked and measured, allowing for cost-effective improvements over a given period of time at various locations.
- Return on a company's investment in its security program can be discussed in more precise business, financial, and risk management terms.
- Security program effectiveness and budgeting can be discussed using the same logical, organizational, and analytical techniques used by other corporate departments.

Conclusion

This article makes the argument that incident management is a critical element of protecting businesses and other organizations against crime, violence, and the losses they cause. In a

real way, security management is similar to the management of any other business function. Data-based (or knowledge-based) decisions can be a security professional's credibility within the organization. The challenge is to adopt a data-driven mindset, acquire the necessary software tools to manage the data, and galvanize security department employees to accept and operate using the principles, practices, and disciplines of incident management.

Denis O'Sullivan

DISASTER TYPES

On March 1, 2003, the Federal Emergency Management Agency (FEMA) became part of the U.S. Department of Homeland Security (DHS). FEMA's continuing mission within the new department is to lead the effort to prepare the nation for all hazards and effectively manage federal response and recovery efforts following any national incident. FEMA also initiates proactive mitigation activities, trains first responders, and manages the National Flood Insurance Program.

National Response Plan

The National Response Plan establishes a comprehensive all-hazards approach to enhance the ability of the United States to manage domestic incidents. The plan incorporates best practices and procedures from incident management disciplines—homeland security, emergency management, law enforcement, firefighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector—and integrates them into a unified structure. It forms the basis of how the federal government coordinates with state, local, and tribal governments and the private sector during incidents. It establishes protocols to help:

- Save lives and protect the health and safety of the public, responders, and recovery workers
- Ensure security of the homeland
- Prevent an imminent incident, including acts of terrorism, from occurring
- Protect and restore critical infrastructure and key resources
- Conduct law enforcement investigations to resolve the incident, apprehend the perpetrators, and collect and preserve evidence for prosecution and/or attribution
- Protect property and mitigate damages and impacts to individuals, communities, and the environment and
- Facilitate recovery of individuals, families, businesses, governments, and the environment

FEMA has more than 2,600 full-time employees. They work at FEMA headquarters in Washington D.C., at regional and area offices across the country, the Mount Weather Emergency Operations Center, and the National Emergency Training Center in Emmitsburg, Maryland. FEMA also has nearly 4,000 standby disaster assistance employees who are available for deployment after disasters. Often FEMA works in partnership with other organizations that are part of the nation's emergency management system. These partners include state and local emergency management agencies, 27 federal agencies, and the American Red Cross.

Types of Disasters

Dam Failure. There are 75,900 dams in the United States, according to the 2005 update to the National Inventory of Dams. Approximately one-third of these pose a "high" or "significant" hazard to life and property if failure occurs.

Dam failure or levee breeches can occur with little warning. Intense storms may produce a flood in a few hours or even minutes for upstream locations. Flash floods occur within six hours of the beginning of heavy rainfall, and dam failure may occur within hours of the first signs of breaching.

Other failures and breeches can take much longer to occur, from days to weeks, as a result of debris jams or the accumulation of melting snow.

Earthquake. One of the most frightening and destructive phenomena of nature is a severe earthquake and its terrible aftereffects.

Earthquakes strike suddenly, violently, and without warning at any time of the day or night. If an earthquake occurs in a populated area, it

may cause many deaths and injuries and extensive property damage.

Although there are no guarantees of safety during an earthquake, identifying potential hazards ahead of time and advance planning can save lives and significantly reduce injuries and property damage.

Fire. Each year, more than 4,000 Americans die and more than 25,000 are injured in fires, many of which could be prevented. Direct property loss due to fires is estimated at $8.6 billion annually.

Fire spreads quickly; there is no time to gather valuables or make a phone call. In just two minutes, a fire can become life-threatening. In five minutes, a residence can be engulfed in flames.

Heat and smoke from fire can be more dangerous than the flames. Inhaling the super-hot air can sear lungs. Fire produces poisonous gases that make a person disoriented and drowsy. Instead of being awakened by a fire, the victim may fall into a deeper sleep. Asphyxiation is the leading cause of fire deaths, exceeding burns by a three-to-one ratio.

Wildfire. The threat of wildland fires for people living near wildland areas or using recreational facilities in wilderness areas is real. Dry conditions at various times of the year and in various parts of the United States greatly increase the potential for wildland fires.

Advance planning and knowing how to protect buildings in these areas can lessen the devastation of a wildland fire. There are several safety precautions that can be taken to reduce the risk of fire losses. Consideration has to be given to the fire resistance of the home, the topography of the property, and the nature of the vegetation close by.

Flood. Floods are one of the most common hazards in the United States. Flood effects can be local, impacting a neighborhood or community, or very large, affecting entire river basins and multiple states.

However, all floods are not alike. Some floods develop slowly, sometimes over a period of days. But flash floods can develop quickly, sometimes in just a few minutes and without any visible signs of rain. Flash floods often have a dangerous wall of roaring water that carries rocks, mud, and other debris and can sweep away most things in its path. Overland flooding occurs outside a defined river or stream, such as when a levee is breached, but still can be destructive. Flooding can also occur when a dam breaks, producing effects similar to flash floods.

Hazardous Materials. Chemicals are found everywhere. They purify drinking water, increase crop production, and simplify household chores. But chemicals also can be hazardous to humans or the environment if used or released improperly. Hazards can occur during production, storage, transportation, use, or disposal. An entire community is at risk if a chemical is used unsafely or released in harmful amounts into the environment.

Hazardous materials in various forms can cause death, serious injury, long-lasting health effects, and damage to buildings, homes, and other property. Many products containing hazardous chemicals are used and stored in homes routinely. These products are also shipped daily on the nation's highways, railroads, waterways, and pipelines.

Extreme Heat. Heat kills by pushing the human body beyond its limits. In extreme heat and high humidity, evaporation is slowed and the body must work extra hard to maintain a normal temperature.

Most heat disorders occur because the victim has been overexposed to heat or has over-exercised for his or her age and physical condition. Older adults, young children, and those who are sick or overweight are more likely to succumb to extreme heat.

Conditions that can induce heat-related illnesses include stagnant atmospheric conditions and poor air quality. Consequently, people living in urban areas may be at greater risk from the effects of a prolonged heat wave than those living in rural areas. Also, asphalt and concrete store heat longer and gradually release heat at night, which can produce higher nighttime temperatures known as the "urban heat island effect."

Hurricane. A hurricane is a type of tropical cyclone, the generic term for a low pressure system that generally forms in the tropics. A typical cyclone is accompanied by thunderstorms, and in the Northern Hemisphere, a counterclockwise circulation of winds near the earth's surface.

All Atlantic and Gulf of Mexico coastal areas are subject to hurricanes or tropical storms. Parts of the Southwest United States and the Pacific Coast experience heavy rains and floods each year from hurricanes spawned off Mexico. The Atlantic hurricane season lasts from June to November, with the peak season from mid-August to late October.

Hurricanes can cause catastrophic damage to coastlines and several hundred miles inland. Winds can exceed 155 miles per hour. Hurricanes and tropical storms can also spawn tornadoes and microbursts, create storm surges along the coast, and cause extensive damage from heavy rainfall.

Hurricanes are classified into five categories based on their wind speed, central pressure, and damage potential. Category Three and higher hurricanes are considered major hurricanes, though Categories One and Two are still extremely dangerous and warrant full attention.

Landslide and Debris Flow (Mudslide). Landslides occur in all U.S. states and territories. In a landslide, masses of rock, earth, or debris move down a slope. Landslides may be small or large, slow or rapid. They are activated by:

- Storms
- Earthquakes
- Volcanic eruptions
- Fires
- Alternate freezing or thawing
- Steepening of slopes by erosion or human modification

Debris and mud flows are rivers of rock, earth, and other debris saturated with water. They develop when water rapidly accumulates in the ground, during heavy rainfall or rapid snowmelt, changing the earth into a flowing river of mud or "slurry." They can flow rapidly, striking with little or no warning at avalanche speeds. They also can travel several miles from their source, growing in size as they pick up trees, boulders, cars, and other materials.

Landslide problems can be caused by land mismanagement, particularly in mountain, canyon, and coastal regions. In areas burned by forest and brush fires, a lower threshold of precipitation may initiate landslides. Land-use zoning, professional inspections, and proper design can minimize many landslide, mudflow, and debris flow problems.

Nuclear Power Plant Emergency. Nuclear power plants use the heat generated from nuclear fission in a contained environment to convert water to steam, which powers generators to produce electricity. Nuclear power plants operate in most states in the country and produce about 20 percent of the nation's power. Nearly 3 million Americans live within 10 miles of an operating nuclear power plant.

Although the construction and operation of these facilities are closely monitored and regulated by the Nuclear Regulatory Commission (NRC), accidents are possible. An accident could result in dangerous levels of radiation that could affect the health and safety of the public living near the nuclear power plant.

Local and state governments, federal agencies, and the electric utilities have emergency response plans in the event of a nuclear power plant incident. The plans define two "emergency planning zones." One zone covers an area within a 10-mile radius of the plant, where it is possible that people could be harmed by direct radiation exposure. The second zone covers a broader area, usually up to a 50-mile radius from the plant, where radioactive materials could contaminate water supplies, food crops, and livestock.

The potential danger from an accident at a nuclear power plant is exposure to radiation. This exposure could come from the release of radioactive material from the plant into the environment, usually characterized by a plume (cloud-like formation) of radioactive gases and particles. The major hazards to people in the vicinity of the plume are radiation exposure to the body from the cloud and particles deposited on the ground, inhalation of radioactive materials, and ingestion of radioactive materials.

Radioactive materials are composed of atoms that are unstable. An unstable atom gives off its excess energy until it becomes stable. The energy emitted is radiation. Each of us is exposed to radiation daily from natural sources, including the Sun and the Earth. Small traces of radiation are present in food and water. Radiation also is released from man-made sources such as X-ray machines, television sets, and microwave ovens. Radiation has a cumulative effect. The longer a person is exposed to radiation, the

greater the effect. A high exposure to radiation can cause serious illness or death.

Thunderstorms. All thunderstorms are dangerous. Every thunderstorm produces lightning. In the United States, an average of 300 people are injured and 80 people are killed each year by lightning. Although most lightning victims survive, people struck by lightning often report a variety of long-term, debilitating symptoms. Other associated dangers of thunderstorms include tornadoes, strong winds, hail, and flash flooding. Flash flooding is responsible for more fatalities—more than 140 annually—than any other thunderstorm-associated hazard.

Dry thunderstorms that do not produce rain that reaches the ground are most prevalent in the western United States. Falling raindrops evaporate, but lightning can still reach the ground and can start wildfires.

Tornado. Tornadoes are nature's most violent storms. Spawned from powerful thunderstorms, tornadoes can cause fatalities and devastate a neighborhood in seconds. A tornado appears as a rotating, funnel-shaped cloud that extends from a thunderstorm to the ground with whirling winds that can reach 300 miles per hour. Damage paths can be in excess of one mile wide and 50 miles long. Every state is at some risk from this hazard.

Some tornadoes are clearly visible, while rain or nearby low-hanging clouds obscure others. Occasionally, tornadoes develop so rapidly that little, if any, advance warning is possible.

Before a tornado hits, the wind may die down and the air may become very still. A cloud of debris can mark the location of a tornado even if a funnel is not visible. Tornadoes generally occur near the trailing edge of a thunderstorm. It is not uncommon to see clear, sunlit skies behind a tornado.

The following are facts about tornadoes:

- They may strike quickly, with little or no warning.
- They may appear nearly transparent until dust and debris are picked up or a cloud forms in the funnel.
- The average tornado moves Southwest to Northeast, but tornadoes have been known to move in any direction.
- The average forward speed of a tornado is 30 MPH, but may vary from stationary to 70 MPH.
- Tornadoes can accompany tropical storms and hurricanes as they move onto land.
- Waterspouts are tornadoes that form over water.
- Tornadoes are most frequently reported east of the Rocky Mountains during spring and summer months.
- Peak tornado season in the southern states is March through May; in the northern states, it is late spring through early summer.
- Tornadoes are most likely to occur between 3 p.m. and 9 p.m., but can occur at any time.

Tsunami. Tsunamis (pronounced soo-ná-mees), also known as seismic sea waves (mistakenly called "tidal waves"), are a series of enormous waves created by an underwater disturbance such as an earthquake, landslide, volcanic eruption, or meteorite. A tsunami can move hundreds of miles per hour in the open ocean and smash into land with waves as high as 100 feet or more.

From the area where the tsunami originates, waves travel outward in all directions. Once the wave approaches the shore, it builds in height. The topography of the coastline and the ocean floor will influence the size of the wave. There may be more than one wave and the succeeding one may be larger than the one before. That is why a small tsunami at one beach can be a giant wave a few miles away.

All tsunamis are potentially dangerous, even though they may not damage every coastline they strike. A tsunami can strike anywhere along most of the U.S. coastline. The most destructive tsunamis have occurred along the coasts of California, Oregon, Washington, Alaska, and Hawaii.

Earthquake-induced movement of the ocean floor most often generates tsunamis. If a major earthquake or landslide occurs close to shore, the first wave in a series could reach the beach in a few minutes, even before a warning is issued. Areas are at greater risk if they are less than 25 feet above sea level and within a mile of the shoreline. Drowning is the most common cause of death associated with a tsunami. Tsunami waves and the receding water are very destructive to structures in the run-up zone.

Other hazards include flooding, contamination of drinking water, and fires from gas lines or ruptured tanks.

Volcano. A volcano is a mountain that opens downward to a reservoir of molten rock below the surface of the earth. Unlike most mountains, which are pushed up from below, volcanoes are built up by an accumulation of their own eruptive products. When pressure from gases within the molten rock becomes too great, an eruption occurs. Eruptions can be quiet or explosive. There may be lava flows, flattened landscapes, poisonous gases, and flying rock and ash.

Because of their intense heat, lava flows are great fire hazards. Lava flows destroy everything in their path, but most move slowly enough that people can move out of the way.

Fresh volcanic ash, made of pulverized rock, can be abrasive, acidic, gritty, gassy, and odorous. While not immediately dangerous to most adults, the acidic gas and ash can cause lung damage to small infants, to older adults, and to those suffering from severe respiratory illnesses. Volcanic ash also can damage machinery, including engines and electrical equipment. Ash accumulations mixed with water become heavy and can collapse roofs. Volcanic ash can affect people hundreds of miles away from the cone of a volcano.

Sideways directed volcanic explosions, known as "lateral blasts," can shoot large pieces of rock at very high speeds for several miles. These explosions can kill by impact, burial, or heat. They have been known to knock down entire forests.

Volcanic eruptions can be accompanied by other natural hazards, including earthquakes, mudflows and flash floods, rock falls and landslides, acid rain, fire, and (under special conditions) tsunamis.

Active volcanoes in the U.S. are found mainly in Hawaii, Alaska, and the Pacific Northwest. Active volcanoes of the Cascade Mountain Range in California, Oregon, and Washington have created problems recently. The danger area around a volcano covers approximately a 20-mile radius. Some danger may exist 100 miles or more from a volcano, leaving Montana and Wyoming at risk.

Source Federal Emergency Management Agency. 2006. <http://www.fema.gov/about/index.shtm>

EMERGENCY MANAGEMENT PLANNING

Emergency planning has been the beneficiary of renewed interest, post September 11, as business and government have sought to adapt to new exposures made evident in 2001. An avalanche of material has been produced on emergency planning. This article will not add new material, but hopefully will encapsulate key concepts within the context of security planning.

Before creating Emergency Plans, it is imperative that a formal Security Program be developed based on a formal Risk Analysis process. Data derived in this analysis is essential for Emergency Planning. The Risk Analysis data highlights key resources, the consequences of an attack, the process by which an attack may take place, and the points of vulnerability that may be exploited by an adversary.

In reviewing the Security Risk Analysis consider the following:

1. How thoroughly did the analysis address single points of failure?
   a. Infrastructure services, such as power, water, telecommunications
   b. Critical operating systems or human resources
2. Did the Risk Assessment recommendations include any of the following:
   a. Mitigating single points of failure by introducing redundancy
   b. Application of security measures to harden the potential target to make it less attractive to an adversary

On the basis of this foundation data, the Emergency Planning process may commence. The objective is to define in step by step detail how the organization should respond, if an adversary (criminal, natural disaster, or accident) succeeds in an attack. The plan should address response protocols for implementation at each of the following stages of an event:

1. Warning: Some emergency events are preceded by a warning. If a warning is received, what protocols should be implemented?
   a. Example: Workplace Violence Event
      i. Receive notice of a domestic dispute involving an employee in which a threat is issued against

the employee by the estranged spouse
   ii. Protocol may be to initiate the Temporary Restraining Order process, alert security officers and local law enforcement authorities

2. During the Event: When an event is in progress, protocols may be implemented to minimize the exposure to harm.
   a. Example: Bomb threat
      i. Receive threat
      ii. Conduct search
      iii. Locate suspicious device
      iv. Notify police
      v. Apply bomb blanket
      vi. Evacuate immediate area
      vii. Keep people disbursed
      viii. Keep traffic arteries open for emergency response personnel
3. Immediate Post Event: When the event has ended, protocols should be implemented to care for the injured, notify authorities, preserve evidence, and minimize any future damage or harm that may result in the aftermath.
   a. Example: Critical system sabotage, resulting in a fire and shutdown of operations.
      i. Keep area inhabitants in sheltered positions, while facility engineers shutdown power systems (also, keep inhabitants in place to minimize exposure to falling debris and other structural exposures)
      ii. Attend to the injured with first aid
      iii. Rescue personnel remove remaining inhabitants
      iv. Rope off crime scene area
      v. Control access to the area
      vi. Preserve evidence
4. Clean-Up and Resumption of Operations: When law enforcement authorities have released the crime scene, begin the clean up process.
   a. Example: Continuation of above
      i. Photograph crime scene
      ii. Tag and photograph all evidence
      iii. Plot evidence location on a site floor plan
      iv. Establish evidence log and log custodian
      v. Establish evidence storage container
      vi. Interview witnesses
      vii. Physically clean up area
      viii. Repair system damage
      ix. Document and repair structural damage

These are simply examples to highlight the type of information required for each stage of an event. More importantly, the planning process should highlight issues that require resolution so they may be resolved before an event occurs.

An administrator should be selected for management of the emergency response protocols. The administrator should develop training plans, table top exercises, and other creative methods to ensure the facility population knows what to do in the event of an emergency.

When security human resources are deployed, the emergency response protocols should be incorporated into the Post Orders clearly defining the tasks to be performed by security in an event.

The Emergency Plan also must consider the magnitude of a terrorist attack and the extreme response protocols that may be necessary. Consider this: emergency response protocols for a hazardous material event usually are structured for response to an industrial level accident in which a vessel is punctured resulting in a leak. In contemplation of a terrorist attack, it may be suggested that the attack may result in much more than a puncture leak; it may result in a completely ruptured vessel. The magnitude of the release may far outstrip response protocols structured for an accident, rendering them not applicable.

This will require a considerable adjustment for traditional emergency planners. Across the country many first responders, in preparation for terrorist attacks, applied for grants to procure more training and equipment to plug leaking vessels. New exposures require new approaches. It is imperative that today's emergency planning efforts not be constrained by what has been done in the past, but use the past as a springboard for confronting new challenges.

Sal DePasquale

HIGH-RISE SECURITY AND FIRE LIFE SAFETY

According to the *Protection of Assets Manual*, ASIS International, a high-rise structure is a building "that extends higher than the maximum reach of available fire-fighting equipment. In absolute numbers, this has been set variously between 75 feet (23 meters) and 100 feet (30 meters), or approximately seven to ten stories, depending on the slab-to-slab height between floors." The exact height above which a particular building is deemed a high-rise is specified by the fire and building codes in the area in which the building is located. When the building exceeds the specified height, fire must be fought by fire personnel from inside the building rather than from outside using fire hoses and ladders.

High-Rise Assets

Assets in the high-rise setting may be tangible or intangible. Tangible assets include the people using the facility, the building itself, its fittings, and its equipment. This equipment consists of the electrical, gas, mechanical, heating, ventilating, air conditioning, lighting, elevator, escalator, communication, security, and life safety systems. In addition, within offices there is equipment such as telephones, computers, word processors, printers, typewriters, FAX machines, photocopiers, audiovisual equipment, general-use items (coffee machines, vending machines, refrigerators, microwaves, ovens, furniture) and sometimes antiques and works of art, cash, and negotiable instruments. Also, vehicles parked in the building's parking garage are tangible assets. Intangible assets include the livelihood of building users; intellectual property and information stored in paper files, reference books, photographs, microfilm, x-rays, and within computer systems and peripherals; and the reputation and status of the facility, including the ability of tenants to conduct business.

Threats to Security and Fire Life Safety

For the purposes of discussion and to address issues in a systematic way, this chapter treats security and fire life safety in high-rise structures as two different disciplines. However, at times, these subjects are so closely interwoven that they appear to be one. Before identifying security and fire life safety threats to high-rise buildings, it is important to understand what these terms mean.

Security is a noun derived from the Latin word *securus*, which means, "free from danger" or "safe." The New Webster Encyclopedic Dictionary defines security as "the state of being secure; confidence of safety; freedom from danger or risk; that which secures or makes safe; something that secures against pecuniary loss." In *Introduction to Security*, Robert J. Fischer and Gion Green write, "Security implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of such disturbance or injury."

Public security involves the protection of the lives, property, and general welfare of people living in the public community. This protection is largely achieved by the enforcement of laws by police funded by public money.

Private security, on the other hand, involves the protection of the lives and property of people living and working within the private sector. The primary responsibility for achieving this rests on an individual, the proprietor of a business employing an individual, the owner or agent of the owner of the facility where a business is conducted, or an agent of the aforementioned who specializes in providing protective services. In *Security and Administration: An Introduction to the Protective Services*, Richard S. Post and Arthur A. Kingsbury write, "In providing security for specific applications, the purpose of private security may be described as providing protection for materials, equipment, information, personnel, physical facilities, and preventing influences that are undesirable, unauthorized, or detrimental to the goals of the particular organization being secured."

Safety is a noun derived from the Latin word *salvus*, which means "safe" (salvation is also from this root). The New Webster Encyclopedic Dictionary defines safety as "the state or quality of being safe; freedom from danger." Obviously, there is very little distinction between the terms security and safety. Fire life safety, fire and life safety, fire safety, and life safety are four synonymous terms commonly in use in high-rise structures.

Security Threats

A threat is any event that, if it occurs, may cause harm or destruction of assets. In the high-rise setting, security threats come in many forms. Threats to people include murder, manslaughter, robbery, assault, assault and battery, mayhem, and sex offenses (including rape, sexual harassment, and lewd behavior). Threats to property include vandalism, trespass, burglary, larceny, sabotage, espionage, arson, and disorderly conduct.

Security threats to both people and property include fire, bombs, riots, civil disorder, hazardous materials, chemical and biological weapons, nuclear attack, and natural disasters. Some of these threats may involve terrorism.

Life Safety Threats

In the high-rise setting, life safety threats include fires, workplace violence, hostage and barricade situations, medical emergencies, trip-slip and falls, power failures, elevator malfunctions and entrapments, traffic accidents, labor disputes, demonstrations, riots, civil disorder, bombs and bomb threats, hazardous materials, chemical and biological weapons, nuclear attack, aircraft collisions, and natural disasters. Again, some of these threats may involve terrorism.

According to the *Protection of Assets Manual*, ASIS International, "The most critical threats in high-rise structures include fire, explosion and contamination of life-support systems such as air and potable water supply. These threats can be actualized accidentally or intentionally, and because they propagate rapidly, can quickly develop to catastrophic levels."

In addition to these threats, an individual may exhibit aberrant behavior, such as that caused by substance abuse. Such conduct may be a threat not only to the personal safety of the individual involved but to others as well. Also, people may attempt to deliberately injure themselves or take their own lives. Because of their very height, the possibility exists that people may jump from a high-rise, particularly if they are successful in reaching the roof. High-rises, particularly major ones, may attract people who view them as a means to gain attention for themselves. For example, protestors may attempt to drape large banners promoting their *raison d'être* over the front of a building or daredevils may perform outlandish feats to achieve notoriety.

Security of Modern High-Rise Buildings

The changes in the design and construction of high-rises since their first appearance have affected the security needs of these facilities. Modern high-rise buildings have inherent security hazards different from the earliest high-rises because of the following:

- Open-style floors with little compartmentation and fewer individual offices that can be secured have made it easier for a potential thief to gain access to business and personal property. The advent of modern telecommunications, with answering machines, portable phones, and services, has meant that the presence of a tenant receptionist to screen persons entering the office is now not always the standard. The open-style floor has also made it easier for an unauthorized person, having once gained access, to move unchallenged throughout the entire floor.
- The higher number of occupants per floor in a modern high-rise means a greater concentration of business equipment and personal items and therefore a more desirable target for a potential thief.
- The concealed space located above the suspended ceiling on each floor of many high-rises has provided a possible means of ingress to a tenant office. This space could also be used to hide unauthorized listening or viewing devices, such as microphones or cameras. The central heating, ventilating, and air conditioning (HVAC) system has provided a similar means for unauthorized listening and viewing.
- The greater number of occupants per floor means the increased potential for these individuals to be perpetrators or targets of a crime and an increased likelihood that some of these people could be injured or killed, particularly by an incident occurring close to them.

In addition to these changes, other factors have added to the security risks of modern high-rise buildings. For one thing, the tenant offices in

modern high-rises are often the headquarters of highly successful corporations that have designed and furnished their places of business in a style to reflect their status. This has resulted in very high-quality furnishings, including, in some instances, expensive works of art, and state-of-the-art business systems. The tenant employees themselves are generally well paid, often carry cash and valuables, and tend to drive and park expensive vehicles in the building parking garage. Hence, these facilities are a potential target for criminal activity.

Next, the computer revolution with its proliferation of compact business machines (such as personal data assistants and personal, laptop, and notebook computers) has resulted in equipment and proprietary information that can be carried away relatively easily by a potential thief. The computer, in itself, presents a unique set of risks because crimes can now be committed without the perpetrator ever setting foot on the premises where information is stored.

Finally, the development in the mid-1950s of completely automatic control systems for the operation of elevators eliminated the need for elevator attendants and, in effect, did away with an important access control and screening measure for high-rise buildings. With the elevator attendant gone, it is often possible for people to travel unchecked throughout a structure once they have entered an elevator. Such unchecked travel can be curtailed by the use of other security measures such as security personnel, locking off certain "secured" floors from elevator access and the installation of modern electronic access control systems in elevator cars and lobbies.

The technological advances that have occurred in the security field, particularly over the past 40 years, have mitigated some of these security risks. Centralized, microcomputer-based control of security and elevator systems has considerably extended and improved the application of basic security measures, such as some of the following:

- Locks and locking systems
- Access control devices: electronic keypads, card readers, and biometric readers
- Lighting systems
- Communication systems: intercoms, handheld radios, pagers, and portable telephones
- Closed-circuit television systems and audio/video recording equipment
- Intrusion detection systems
- Patrol monitoring devices
- Better-trained security officers

These changes have all contributed to improved and better-designed security programs.

Fire Life Safety of Modern High-Rise Buildings

Buildings constructed after World War II began to include fire safety enhancements such as fireproofing insulation sprayed directly onto steel columns, floor beams, and girders to protect these structural members from distortion due to heat. It is applied in accordance with the requirements of the local building code. If the insulation is not correctly applied (for example, if the steel is rusted and the surface has not been properly prepared or if the insulation has not been applied at the specified thickness or density) or if the insulation has been dislodged during construction or high winds, heating an exposed steel floor beam to high temperatures can cause vertical deflection (because the secured beam has no space to move horizontally when it elongates) and failure of the connection used to secure the beam to other beams or to the main girders.

In the modern core construction high-rise built of lightweight steel or reinforced concrete frames, skin-type curtain walls that support none of the weight of the building are usually found on the outside of the structure. According to Mark Gorman of URS Corp., "They are like a shower curtain—designed to keep the rain out. These curtain walls are usually glass and stone cladding supported on the structure by lightweight metal frames. Skin-type refers to a continuous wall that covers the surface like skin on a body."

In addition, curtain walls may be attached to the exterior wall columns, sometimes creating an empty space (of width varying from 6 to 12 inches) between the interior of these walls and the outer edges of the floors. If there is such a gap, it is usually filled with fire-resistant material to restrict the vertical spread of fire.

Suspended ceilings, the most common type of ceiling in high-rise buildings, create a

concealed space that often extends throughout an entire floor area. Apart from mandatory firewalls extending from a base floor slab to the floor slab of the floor above and in restrooms and corridors where fire-rated plasterboard ceilings are used for fire protection, these ceilings lack fire-stopping material. This uninterrupted space is about 30 inches in depth and consists of noncombustible acoustical ceiling tiles that are supported in a metal grid hung on metal hangers attached to the floor above. It often is used to house electrical, plumbing, and ducting systems, as well as telephone wiring conduits and computer wiring for that particular floor. In some buildings, it is also used as a return plenum for the heating, ventilating, and air-conditioning (HVAC) systems. According to Mark Gorman of URS Corp., "Hotels often do not have a suspended ceiling—the concrete floor slab above is the ceiling below, and all the electrical is cast in the slab."

Floor beams and girders are often covered with corrugated steel panels or plates and then covered with a layer of concrete to form the floor itself. According to John Seabrook, "The floors in most of the high-rise buildings erected since the sixties are much lighter in weight than the floors in the older buildings. In a typical high-rise office floor, 3 to 4 inches of concrete covers a corrugated-steel deck, whose weight is supported by I-beams or, in the case of the [World Trade Center] Twin Towers, by long 'trusses'—lightweight strips of steel that are braced by crosshatched webs of square or cylindrical bars that create a hollow space below each floor surface. This space allows builders to install heating and cooling ducts within the floors, rather than in a drop [suspended] ceiling below them—an innovation that allows the developer to increase the number of floors in the entire building."

Multiple stairwells provide primary and secondary means of egress and are often equipped with automatic stairshaft pressurization and smoke evacuation systems. Because these stairwells are located in the central core area, they are less distant from each other than those in pre-World War II buildings. Stair and elevator shaft openings are equipped with protective assemblies and horizontal openings are protected.

Floor areas tend to be larger and have a generally open-plan design, with little compartmentation using floor-to-ceiling walls and barriers. Aluminum-framed, cloth-covered foam partitioning is often used to construct cubicles to be used as individual offices. This partitioning is cheaper than the hardwood partitioning used in the past and just as effective as a sound barrier; however, it is more combustible.

The number of occupants tends to be high, and results in a high concentration of business and personal property, and hence high fire or fuel load. Much of this property (including office supplies, plastic wastepaper baskets, files, paper, and the personal computer systems that now equip most workstations) is made of synthetic materials that are flammable; they produce toxic gases that become components in the resulting smoke and gas. In the *Fire Protection Handbook*, Brian L. Marburger writes, "Over the past several years, there have been many changes in the furnishings put into buildings. At one time, desks and chairs were routinely wood. Then metal became popular. Now, any combination of wood, metal, thermoplastics, and foamed plastics can be found. In addition, the increased use of computers has also added to the fuel load." To mitigate against this threat to life safety, office furniture and interior furnishings in all offices, conference and waiting rooms, and reception and assembly areas should be of fire-resistive quality and treated to reduce combustibility.

There is the potential during fires for stack effect. In the *Fire Protection Handbook*, Wayne D. Holmes writes, "The stack effect results from temperature differences between two areas, which create a pressure difference that results in natural air movements within a building. In a high-rise building, this effect is increased due to the height of the building. Many high-rise buildings have a significant stack effect, capable of moving large volumes of heat and smoke through the building." In contrast, in *Building Construction for the Fire Service*, Francis L. Brannigan notes that pre-World War II, "Windows could be opened in buildings of this era. This provided local ventilation and relief from smoke migrating from the fire. The windows leaked, often like sieves, therefore, there was no substantial stack effect." Modern high-rise building windows provide some resistance to heat and are often made of tempered safety glass; they usually cannot be opened and are well insulated. In the *Fire Protection Handbook*, Wayne D. Holmes writes, "No manual fire-

fighting techniques are known to counter stack effect or to mitigate its effect during a fire....The only way to mitigate the potential of stack effect is to design and construct the building to minimize the effect."

Automatic fire detection systems and automatic fire suppression systems are often incorporated into building design. According to Francis L. and Maureen Brannigan, "Most new high-rise office buildings have sprinklers installed. The huge losses suffered in such fires as Philadelphia's One Meridian Plaza and Los Angeles' First Interstate Tower [First Interstate Bank Building] leave little room for argument. But there is still much opposition to any requirement for retroactive installation of sprinklers in existing buildings. While much of the opposition is financial, the specious argument that such requirements are unconstitutional has found some favor. This argument is without merit with respect to United States law. Much of the cost, particularly of a retroactive installation, is caused by hiding the sprinkler system. If the argument of overall sprinkler cost is an issue, the opposing argument is that safety requires only the cost of a bare bones system. Aesthetic costs such as hiding the sprinklers and the piping are the option[s] of the owner, not a fire protection requirement."

Summary

High-rise buildings contain many valuable assets. The terms security and fire life safety are synonymous but can be addressed separately for the purposes of systematic analysis and discussion. There are many potential security and life safety threats to the people who use these facilities on a daily basis and to the businesses, property, and information contained within them.

Geoff Craighead

Sources

Abbott, R. 1994. *Comparison of Design and Construction Techniques, Class 'E' High-Rise Office Buildings*. New York: Fire Science Institute.

Brannigan, F. 1992. *Building Construction for the Fire Service, 3rd Edition*. Quincy: National Fire Protection Association.

Brannigan, F. and Brannigan, M. Statements in a letter to the author regarding building construction for the fire service. Mar. 1995.

Fischer, R. and Green, G. 1998. *Introduction to Security, 6th Edition*. Boston: Butterworth-Heinemann.

Gorman, M. Comments to author in an e-mail regarding core and tube construction of high-rises. Mar. 2002.

Holmes, W. 2003. *Fire Protection Handbook, 19th Edition*. Quincy: National Fire Protection Association.

Marburger, B. 2003. *Fire Protection Handbook, 19th Edition*. Quincy: National Fire Protection Association.

Post, R. and Kingsbury, A. 1991. *Security Administration: An Introduction to the Protective Services, 4th Edition*. Boston: Butterworth-Heinemann.

Protection of Assets Manual. 2006. Arlington: American Society for Industrial Security International.

Seabrook, J. "The Tower Builder: Why Did the World Trade Center Buildings Fall Down When They Did?" *The New Yorker* Nov. 19, 2001.

Thatcher, V. ed. 1980. *New Webster Encyclopedic Dictionary of the English Language*. Chicago: Consolidated Book Publishers.

MEDIA CONTROL IN CRISIS SITUATIONS

An organization is much like a living organism in the sense that it reacts to external stimuli, and when the stimuli are unpleasant, as would be the case during a crisis, the organization experiences stress. An external stimulus contributing to an organization's stress in a crisis is the uncompromising search by the news media for information. A significant incident affecting the organization, such as a major accident or crime, will stimulate public interest and consequently set the news media on the trail.

At the outset of a crisis, the organization faces two critical tasks simultaneously: first, deal with the crisis, and second, communicate the facts. Great pressure is on the organization to launch an effective response and at the same time intelligently present the details of what happened and what is being done in response. The target of communications set by the organization is the public broadly, and the vehicles for getting to the target are television, radio, and press agencies.

Business people are learning to be aware of public concerns when commenting on broad

issues in which corporate interests are involved. Executives generally look ahead when making public statements. They do so to avoid the impression of not caring for public health or safety when company profit may be at risk. This can be difficult when liability is a possible outcome and legal counsel urges management to be careful in avoiding language that suggests culpability. However, if management is overly circumspect, the business may suffer public relations losses. Losses of this type include damage to public confidence and increased regulatory restrictions imposed by legislators responsive to the public mood. The long-term costs of political and regulatory responses are likely to greatly outweigh the short-term costs of accepting responsibility when it is due.

Interacting with the Media

Certain problems of a security nature can be anticipated in dealings with the media. They include access control at the scene of the incident, disruption of business operations resulting from attempts by the media to acquire information, and unauthorized release of information from sources within the organization. Also, when the chief security officer is a central persona in responding to contingencies, which is almost always the case, he or she will be sought after by the media.

Being responsive to media requests for information is especially important during emergency response operations. The usual procedure is for media inquiries to be channeled to one office or person, typically called the Public Information Office or PIO. A PIO representative is designated in advance to speak for the organization, to meet with news representatives, and to arrange and be present at media interviews of company employees. The PIO is often sensitive to the needs of the news media, particularly with respect to time. While the media are racing to report the news, the PIO is concerned about releasing details that are both accurate and considerate of the organization's view.

Incidents involving death, serious injury, substantial property loss, damage to the environment, and risk to the public constitute significant news. The PIO serves as a "control valve" for preventing the release of distorted versions and providing some modicum of protection against disclosures that may be harmful to the organization or its individual employees.

Whether business likes it or not, the media will present news in a manner intended to attract attention, and in the process will make news reporting more important than the news itself. The outcome can be distortion of facts.

When an incident of any magnitude arises, the news media will want, indeed demand, the facts. Oftentimes they will be asking for details even before the organization's management is aware of the incident. Through arrangements with governmental response agencies, such as police and fire departments, media employees learn of incidents on a real-time basis. Television, radio, and press reporters are likely to arrive at the incident scene with the first responders.

When the organization's headquarters is located a considerable distance from the site of the incident, which will frequently be the case, senior management will expect a knowledgeable manager at the scene to act as the organization's spokesperson, at least until arrival of more senior persons. The on-scene spokesperson can initially provide all available details as quickly as possible. Of concern in accidents will be precisely what happened, how, when, and where; the number of persons involved and their names; the nature and extent of deaths and injuries; and the nature and extent of property damage, including non-organizational property and the environment.

A chief security officer, especially one who also has operational safety responsibilities, may be called upon to perform spokesperson duties. Direct media contact with an operational manager is usually better, at least from the media's point of view, than contact through a PIO representative or other intermediary. Misunderstandings frequently develop whenever a critical incident is being developed by the media, and an absence of personal contact between the media and persons close to the situation contribute to misunderstanding and distrust.

A chief security officer tabbed for interview must be wary of offhand remarks that could give a wrong impression, and should also avoid leaving out important details. Being quoted out of context can be minimized by speaking in short sentences and repeating constantly the key phrases that convey the organization's point of view. This requires rehearsing, and is particularly

important in television interviews where reporters are obliged to select only the briefest, most salient comments from an interview that may have taken an hour or more to tape. If at all possible, a PIO representative should be present to listen objectively and intervene to correct errors on the spot.

Rumor and exaggeration are the organization's nemesis in a time of crisis. Accuracy, although difficult to maintain in the very early stages of an incident, is a priority. Information flowing from the scene has to be carefully weighed as to the extent of casualties and damage. A golden rule is to not release the names of persons killed or injured until the next of kin have been notified, to not speculate as to the causes of the incident, and to not mention dollar amounts concerning damage and loss. Another rule is to avoid saying "no comment." Corporate counsel may like this response because it closes off a line of questioning that could be troublesome, but use of the term suggests to the media and the public that the organization has something to hide.

The organization and the media each have a right to be wary of deception. The organization may feel it has an overriding and legitimate reason to be reserved in its response, and the media know from prior experiences that businesses have engaged in denials and half-truths. Good reporters usually can see through a lie and have it in their power to make the organization look worse for it. Reporters hungry for a headline story may be more attuned to negatives than positives. Some may have an anti-business bias or be ignorant of business needs. Fortunately, most reporters genuinely want to present a responsible view and will work with an organization that deals squarely with them.

If saying the wrong thing can hurt the organization, why not impose a policy of silence? The problem with this approach is that speculation, conjecture, and rumor take the place of facts. Fiction and fantasy rapidly fill the vacuum of official silence. By saying nothing, the organization makes itself vulnerable to unfounded perceptions. Perception takes on a reality all its own in a world strongly influenced by mass communications.

The principal cause of tension between business and the media is their different perspectives. Business operates through policies it believes are proper and is resolute in defending policies in the face of criticism. Executives are resentful when taken to task by reporters who do not understand the policies and the reasons for them. Reporters, on the other hand, feel that their function is to report what they find, even when their findings run counter to long-established business practices and beliefs.

On-Scene Functions

The PIO's contingency plan will customarily call for sending a representative to the scene of a major incident. When the incident is significantly destructive, such as an oil spill or plant explosion, the representative will almost certainly be accompanied by one or more senior managers, possibly including the organization's chief executive officer. Virtually no crisis incident is too small or unimportant to warrant senior management attention.

Some of the media-related functions that require prompt attention at the scene are:

- Verifying key details, such as casualties and damages
- Meeting and escorting reporters
- Setting up and making announcements at press conferences
- Updating and reporting developments as they evolve
- Clearing the statements and comments of management

To the extent that circumstances permit, the PIO representative will set up a press center at or close to the scene of the incident. The center could be on the organization's premises, at a hotel nearby, or at any safe and reasonably convenient place having telephone facilities. It is not necessary or even appropriate for the PIO to provide food or refreshments at press center meetings, but it is a given that news personnel will receive honest answers with least possible delay. The answers are delivered courteously and in a manner ensuring that all news personnel receive information the same way at the same time.

Verbal announcements are often supplemented with written materials designed to facilitate accurate reporting. Working from written materials, the PIO spokesperson is able to focus on facts that are fully known. Dangerous

conjecture, which will sometimes arise in the face of insistent questioning, can be avoided by commenting only on what has been put into writing.

Also, in the case of releasing the names of persons injured or killed, the chances of word-of-mouth name errors are reduced by providing a written list.

As an incident winds down, the PIO may hold one or more follow-up meetings with the news media. By then, the causes of the incident and the extent of damage may be known and open to discussion. Positive messages would include assurances to the community with respect to safety and the restoration of jobs destabilized by the incident; progress reports on assistance given to families and repairs made to property and the environment; the effectiveness of the organization's preventive and responsive actions; and credit to local response agencies that assisted in bringing the emergency under control.

The Role of the Chief Security Officer

The chief security officer has a full plate during a major incident. Depending on the nature of the incident, there can be requirements to provide first-responder medical assistance, establish access control at the incident scene, and protect people and assets exposed to continuing risk. Meeting these requirements involves coordination with many persons inside and out of the organization. Within the organization, and surely this will be a key element in contingency planning, the chief security officer interfaces with the PIO.

The services performed by a chief security officer that relate narrowly to the media fall generally under access control. Three services stand out:

- Preventing entrance to an unsafe incident scene by unauthorized personnel. After an incident has been declared safe, the chief security officer may be involved in escorting media representatives interested in taking pictures, making notes, and in some controlled situations, interviewing employees at the scene.
- Preventing close-in access to PIO representatives and senior managers at meetings with the press. Distraught relatives of victims and issue-oriented persons antagonistic to the organization may use a press meeting to physically attack the organization's spokespersons.
- Preventing access to travel conveyances utilized by senior managers. A person, deranged or motivated by revenge and/or the desire to gain attention to a cause, may attempt to place a bomb aboard or otherwise sabotage the plane or automobile used to transport key members of the organization.

The chief security officer must be prepared to support the important functions carried out by the organization's PIO during times of crisis. Security support to the PIO cannot be properly executed if it is based on a misunderstanding of the PIO function or if there is insufficient preparation in crisis management. A chief security officer simply cannot wait until an emergency occurs to determine and fill PIO needs. All of the planning for the handling of public information matters must be done well in advance.

The quality of security support is examined, to the chief security officer's credit or discredit, at the conclusion of a crisis when the organization summarizes the lessons learned. A manager who puts effort into learning PIO needs and in developing a support capability assures a quality response for the organization and a creditable rating personally.

John J. Fay

NATIONAL INCIDENT COMMAND SYSTEM ORGANIZATION

The national structure of incident management establishes a vertical progression of coordination and communication from local to state and regional to the national level. Security professionals, for the most part, will be coordinating planning issues with the local emergency operations center personnel typically located at the county or parish level. During an incident, however, security management personnel may be coordinating with or supporting incident response organizations.

Most daily incidents are handled by the local public safety authorities through established

command and control protocols. They use the ICS concept when they respond to major local incidents such as chemical spills, large fires, explosions, and other disaster situations. The first command and control entity is the incident command post and is usually under a single command element such as the fire department. When there are multiple locations that are part of the response, local leadership may activate additional incident command posts. To control the operations of the multiple numbers of incident command posts, a unified command entity may be established. This occurs when more than one agency has incident jurisdictional responsibilities or the incident crosses political jurisdictions. The agencies or local jurisdictions provide liaison representatives to the unified command location to participate in the decision-making process. The unified command entity carries out short-term operations, planning, logistics, and finance/administration functions and is focused on establishing common objectives and strategies for the execution of a single incident action plan.

When the area command is activated it usually oversees multi-incidents being managed by ICS first responders or conducts management of large incidents that cross jurisdictional boundaries. The area command does not have the direct operations responsibility that is identified with the unified command concept. It has the responsibility to set overall strategy, identify priorities, allocate critical resources to meet those priorities, and to ensure that incidents are properly managed through objectives and strategies accomplishment. The area command may develop more than one incident action plan and may become a unified area command when required. The incident command post commanders report to the area command for support and guidance.

Both the unified command and area command provide information to the local emergency operations center. That center is a full-time organization with a nucleus of personnel responsible for long-term planning and exercise production; communication operation; operational information sharing; and resource coordination, dispatching, and tracking in support of on-scene efforts. When activated to support an incident, the center is manned by state and local public and private sector liaison representatives. This additional augmentation assists in coordinating the center's activities and needs with state, federal, and appropriate private sector emergency operations centers and support sectors.

James T. Roberts, Jr.

NATIONAL INCIDENT MANAGEMENT SYSTEM

Private-sector emergency preparedness and responses of today are integrated with local community preparedness measures. Local resources and responses identified during the planning process are often available for use on a larger scale. Security planners may be tasked to work with government emergency management planners and coordinate support at different levels to ensure that their company resources assist in the most efficient and effective manner. All private sector organizations, especially those who represent critical infrastructure or key resource materials or technology, are encouraged (or required in some cases) to develop detailed emergency response and business continuity plans to include information-sharing and incident reporting measures that are compatible with the National Incident Management System (NIMS).

Homeland Security Presidential Directive/HSPD-5, issued in 2003, directed the establishment of NIMS. As developed, this system is based on incident management best practices developed by public safety practitioners at the local, state, and federal levels. The NIMS goal is to provide common nationwide command and control methodology for use by all government and non-government emergency management and public safety elements. Using the interoperability and compatibility approach fine-tuned by firefighters, hazardous materials teams, rescuers, and emergency medical teams since the 1970s, NIMS permits organizations to use core sets of concepts, principles, terminology, and technologies to jointly prepare for, respond to, and recover from domestic events regardless of the cause, size, and complexity. It establishes an organizational structure that focuses on the incident command system (ICS), multi-agency coordination systems, and unified command models. Other parts of NIMS address training; identification and management of resources; qualifications and certification; and the collection, tracking, and reporting of incident information and incident resources.

The ICS manages major incidents through focus on five major functional areas: command, operations, planning, logistics, and finance/ administration. A sixth function of intelligence gathering, analysis, and sharing may be assigned based on the type of incident being addressed by the responders. ICS gives users an on-scene, integrated, all-hazard management system which can be used for single or multiple incidents. Where the incident transcends geographical or governmental jurisdictions, use of a unified command structure may be warranted. This integration of multi-agency personnel permits coordination of and joint decisions for incident objectives, strategies, plans, priorities, and public notifications.

The strength of the ICS management stems from the characteristics of the system. These characteristics are:

- Common terminology. Standardized key terms, titles, facility and unit designations, and definitions that are used in planning, operations, and communications at all levels
- Modular organization—use of the building block concept to add needed pre-planned command, operational, and administrative elements required to meet the level of complexity for successful incident control and recovery
- Chain of command and unity of command. NIMS is based on a distinct vertical chain of command that facilitates assignment of authority and responsibility for decision-making, coordination, and issuance of orders based on information and requests that flow up and down the chain. At each level, one individual is designated as the decision-maker for all elements responsible for addressing an incident at his or her level and subordinates report to only one person.
- Establishment and transfer of command. The formal identification of who is in command of an incident, operations center, or higher command center. Shift transfer is a formal process where the incoming commander is briefed by the outgoing commander as to threat, operations, resources and other items important to the successful completion of the mission. Command staff conduct the same briefings in their respective areas to ensure continuity of operations.
- Manageable span of control. The effective span of control that varies between three and five elements with the most desirable being one supervising element for five reporting elements
- Unified command—established when there are two or more agencies with incident jurisdiction or when incidents cross political jurisdictions. Agency-designated incident commanders work from a single incident command post through an agreed upon common set of objectives, strategies, and single incident action plan.
- Management by objectives. The systematic and organized approach used by leadership to focus on achievable goals, establish specific objectives, and target the use of available resources to obtain the best results possible
- Reliance on incident management planning. The use of the continuous planning cycle that addresses prevention, preparedness, response, and recovery actions
- Comprehensive resource management. The management of those tasks that establish systems for describing, inventorying, requesting, and tracking resources; activating those systems prior to, during, and after an incident; dispatching resources prior to, during, and following an incident; and deactivating or recalling resources during or following an incident
- Pre-designated mobilization locations and facilities. The use of the planning process (or on-scene identification) of sites where operational and logistical elements are marshaled for future mission assignment and deployment
- Accountability of resources and personnel. The use of measures that require check-in of all materials, personnel, and equipment regardless of agency affiliation to a central person or section that can, in turn, advise the incident commander, area commander, or multi-agency coordination center manager of assets that are available for use
- Deployment. The orderly movement of identified elements and resources from a home base, base camp, heliport, or marshaling point to a specific operational location

- Integrated communications and information management—the use of pre-identified equipment that allows for multi-agency interoperability and is compatible vertically and horizontally
- Information and intelligence management—the establishment of an awareness system that ensures the continual process of collecting, analyzing, and disseminating intelligence, information, and knowledge to allow organizations and individuals to anticipate requirements and to react properly

Daily ICS operations are governed by the development of incident action plans (IAP) that are based on the objectives identified by leadership. The plans, usually covering a 12 hour period, provide the overall incident objectives for operational and support elements. IAP objectives are used to develop and make assignments, plans, procedures, and protocols. At the end of each period, operational results are documented and fed back into planning for use in the next 12 hour period.

James T. Roberts, Jr.

NATIONAL RESPONSE PLAN

Security practitioners that are tasked with planning for or responding to emergency incidents, whether local or national, are affected by the National Response Plan (NRP).

The NSP, released by the Department of Homeland Security in December 2004, is the central document that provides domestic emergency management guidance for all federal departments, state, and local agencies. The guidance is aimed at seamless management and coordination between departments in their actions to prevent, prepare for, respond to, and to recover from terrorism, major natural disasters, and other national emergencies. The NRP is the result of Homeland Security Presidential Directive 5 (HSPD-5) which ordered the development of new guidance that aligned all federal coordination structures, capabilities, and resources into a unified, all-discipline, all hazards approach to major incident responses.

Included in the plan are the roles and responsibilities of state, local, and tribal governments; non-governmental and volunteer organizations, the private sector, and citizen involvement. The NRP is written to generally recognize that incidents are best handled at the lowest jurisdictional level possible. As those first responder jurisdictions at the local level determine that they lack the capability to control the incident, they request additional resources from mutual aid pact agencies and the state under the first line of emergency response and support concept. When the state recognizes that the incident is beyond its long term response, it may request federal assistance. The plan also recognizes that there may be incidents of national significance where the federal government will quickly initiate actions to prevent, prepare for, respond to, and recover from those situations. In the latter case, actions will be taken in coordination with those government, non-government, and private sector entities affected.

The plan establishes the common organizational structure from incident command to local emergency operations centers to regional centers to national multi-agency coordinating centers. This structure is based on the National Incident Management System (NIMS). NIMS was initially developed for use by the fire services to determine common command and control measures that could be used by one or more agencies in incident command response. The system is now the model for use by all public safety agencies. An example of one temporary organization is the Joint Field Office (formally the FEMA disaster field office). This locally activated multi-agency center has the responsibility for coordinating federal, state, local, tribal, non-governmental, and private sector response to the following: natural disasters, national public health incidents, incidents of national significance (e.g., massive oil spills, etc.), and national special security events. The plan also establishes the parameters for requesting federal assistance under Stafford Act or non-Stafford Act circumstances.

The key components of interest to the private sector are found in the three groups of annexes to the plan. The emergency support functions (ESF) annexes are: transportation; communications; public works and engineering; firefighting; emergency management; mass care, housing, and human services; resource management; public health and medical services; urban search and rescue; oil and hazardous materials response; agriculture and natural resources; energy; public safety and security; long-term

community recovery and mitigation; and external affairs. Support annexes cover: financial management, international coordination, logistics management, private-sector coordination, public affairs, science and technology, tribal relations, volunteer and donation management, and worker safety and health. The incident annexes provide specific guidance on: biological incidents, catastrophic incidents, cyber incidents, food and agriculture incidents, nuclear and radiological incidents, and terrorism incident law enforcement and investigation.

Of particular interest for security practitioners, is Emergency Support Function #13, Public Safety and Security. This annex outlines the federal to federal and federal to state and local coordination and support tasks. It discusses non-investigative and non-criminal law enforcement, public safety, and security capabilities and resources available during potential or actual Incidents of National Significance.

Private sector entities support national response initiatives stemming from emergency support actions that are noted in the plan's ESF annexes. The primary agencies are mandated to work with, and coordinate actions with their private sector partnership committees to develop a seamless industry relationship. Individual organizations share vital information with the government, identify tasks to be accomplished, perform vulnerability assessments, develop emergency response and business continuity plans, enhance corporate readiness, implement appropriate prevention and protection plans, and provide assistance necessary to respond to and recover from an incident.

James T. Roberts, Jr.

SECURITY AND LIFE SAFETY IN THE COMMERCIAL HIGH-RISE BUILDING

The variety of ownership formulas and tenant occupancies associated with commercial high-rise buildings presents challenges in the delivery of security and life safety services. Buildings can be owned and managed by single organizations, owned by one party and managed by another, owned by groups of business entities, owned by a tenant and managed by the property manager, etc. Different organizations have differing standards of risk acceptance and differing perspectives on the very nature of security and life safety. What they share in common is an overriding concern with costs. The natural results are that the practices of security and life safety in commercial high-rises are inconsistent and poorly funded.

A commercial high-rise is defined by the National Fire Protection Association (NFPA) as "a building greater than 75 feet (23 meters) in height where the building height is measured from the lowest level of fire department vehicle access to the floor of the highest occupiable story (Section 3.3.25.6, 2000)." The Building Owners and Managers Association (BOMA) provides a less technical description. It classifies a building according to work performed within it, tenant base, size, location, structural composition, and other factors. Small commercial properties can occupy tens of thousands of square feet and have hundreds of occupants while large properties can occupy millions of square feet, hold tens of thousands of occupants, and consist of several buildings.

Persons inside a building can be numerous and varied: employees, temporary employees, visitors, contractors, vendors, people "just passing through," and undesirables such as vagrants and criminal opportunists. The internal operations of buildings vary. A tenant that provides information technology services will use equipment, materials, and supplies different from a tenant that provides counseling services.

Commercial high-rises often have retailers that provide products and services to tenants and the general public. They are usually at ground level and consist of department stores, boutiques, theaters, restaurants, fast-food shops, bars, health clubs, banks, and visitor parking areas. Great difficulties confront a security and life safety program that is mandated also to provide services to the ancillary operations.

These varying factors prevent uniformity in the operation of security and life safety programs. A program in place at one facility is certain to be different at another. There can be variances within the program as well. For one tenant, the services may not be wanted at all and for another tenant the services may be very much desired. Adding to the mix are complaints and irrational demands.

The security component of a program is concerned with protecting tenants against crime such as physical assault and theft of vehicles in the underground parking lot, theft of materials and

ing at and moving from a loading platform, receipt of package bombs in the mailroom, internal theft, and employee-to-employee violence. Typically, protection is achieved through a combination of physical safeguards and security officers working in ways specified by plans and procedures.

The life safety component is concerned with preventing and/or responding to life-threatening incidents such as fire, major accidents, hazardous materials releases, and acts of nature such as earthquakes, windstorms, and flooding. The life safety component addresses building evacuation, sheltering in place, administration of first aid, and assisting the handicapped.

Many commercial properties have critical infrastructure capabilities such as:

- Fire detection and suppression equipment
- A system for delivering water to fire-affected areas
- An uninterrupted power supply system
- Backup power generation
- Air handling system
- Pressurized stairwells
- Automatic shutdown of interfering utilities
- Emergency communication

For business continuity purposes, a commercial property can have infrastructures that provide:

- Fresh water and dispel waste water
- Work areas isolated from danger
- Heating and cooling
- Means for communicating internally and externally
- Power hookups for critical equipment such as computers
- Protection of critical business records

The regular operations of a security and life safety program are influenced by:

- Life safety and construction codes
- Budgetary restrictions
- Standards and guidelines
- What tenants say, want, expect and, most importantly, what they are willing to pay
- What the building owners want
- What the building management wants
- Findings of building vulnerability and threat/risk assessments
- Local, regional, and national concerns
- Signature status of the building
- High-profile tenants
- Proximity to high profile buildings and landmarks

The manager of a security and life safety program focuses on issues of concern to tenants. These can be incidents that have relatively low importance but occur regularly such as loitering, minor theft, and graffiti. Other incidents have high importance but occur infrequently such as fire, power blackouts, hazardous materials releases, and violent crimes.

The resources that are available to the security and life safety program manager to deal with incidents of concern fall into three categories: personnel, physical/electronic systems, and documentation. The personnel category can include security officers, contractors that service security equipment, staff employees in the building management office, maintenance and engineering employees, and tenant employees. External to the building are persons that provide first-responder services such as police officers, firefighters, and emergency medical technicians.

Tenant employees are sometimes overlooked as resources or not thought to be resources at all. The reality is that all building occupants play a part in security and life safety; for example, reporting and correcting hazardous conditions, reporting suspicious persons and activities, and helping mitigate the effects of a major disaster. Tenants often designate certain of their employees to perform these types of functions on a regular basis. Persons in this group are often called floor or fire wardens.

The physical/electronic systems category can include fences, gates, lights, bollards, locks, reinforced doors, access control systems, intrusion detection systems, CCTV systems, fire detection/suppression systems, HVAC systems, elevator systems, etc.

The documentation category can include mutual aid agreements, security and safety policies and standards, emergency management plans, notification lists, standard operating procedures, post orders, incident reports, training manuals, and manuals for operating and calibrating security hardware. Sometimes overlooked are as-built plans and engineering documents that identify critical locations such as air intake and exhaust openings, shutoff points for power and water, and electrical conduits.

Of the three categories just mentioned, the people category is most important, and within that category, security officers are most important. This is because security officers are often the first to learn of a crisis impending or in progress; they alert others to danger, summon first-responders, intervene to contain an incident and mitigate its effects, and assist persons in need of emergency care. When a major incident occurs after hours, which is often the case, security officers take on the duties of absent persons such as building management staff, maintenance and engineering personnel, and floor wardens.

Security officers are important for another reason: without them, the electronic systems serve no valuable purpose. Worth cannot be found in a CCTV system that has no human to monitor images, or a fire alarm that has no human to hear it, or an intrusion detection system that has no response force.

In conclusion, a security and life safety program for a commercial high-rise building has to be managed competently, coordinated internally, configured to meet the full range of anticipated contingencies, and sufficiently resourced.

Glen Kitteringham

III: Information Security

BUSINESS INTELLIGENCE

"Business Intelligence" is a major phrase in today's competitive marketplace; it means many things to many people—usually for marketing purposes. Definitions range from software packages to data mining techniques to technology solutions to difficult problems. In this definition, however, we deal with the operational, business process that derives largely from the experiences of intelligence professionals who translate skills, tools, techniques, and approaches from national and international intelligence operations.

Business intelligence includes competitive intelligence (CI) and competitive counterintelligence (CCI). Both specifically include the nature of competition, for it is the purpose of both to assist the firm in gaining and maintaining competitive advantage through the application of established principles not normally found in the business community.

CI and CCI have been successfully characterized and applied using cyclical approaches. They operate as interlocked cycles which both begin and end at the decision maker. The decision maker, in need of the best information possible, uses CI processes to define the actual requirements to be satisfied through legal, ethical, and effective means; to have the information evaluated and analyzed and provided in a format sufficient to take competitive actions on time.

This same decision maker is also responsible for determining those elements of competitive advantage which sets the firm apart from adversaries and commissioning those steps necessary to protect that advantage. This process includes the identification of the competitor set, their capabilities and competencies in order to paint as effective a portrait of the threat to the firm's business as possible. Once that picture emerges, testing of the firm's actual vulnerabilities to such external threats is conducted, and countermeasures developed that are consistent with the firm's environment, culture, and requirements. This process also includes an ongoing analysis of the efficacy of such selected approaches and regularly advises the decision-maker about needful changes consistent with different approaches undertaken by competitors once they encounter the countermeasures designed to thwart their intelligence collection efforts.

John A. Nolan, III

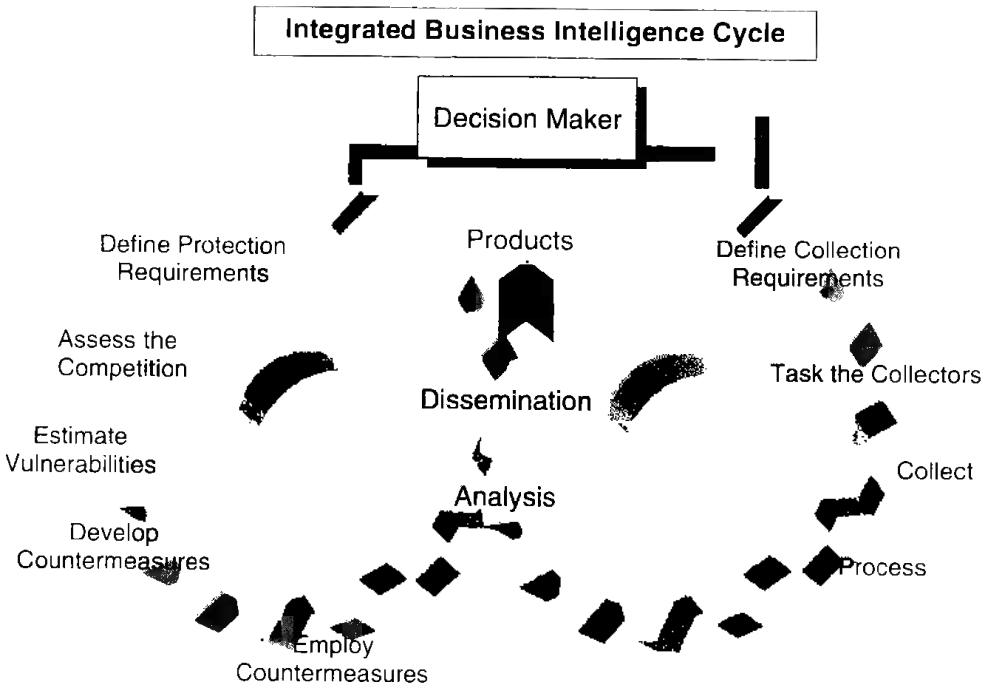


Figure 10. Information is processed as it moves through two cycles.

BUSINESS INTELLIGENCE: AN OVERVIEW

Business intelligence is both a product and a process. As a product, it is information with use and value that can be applied by decision makers to the organization's particular purposes or goals. As a process, it is a combination of ethical and legitimate activities that involve the collection, evaluation, analysis, integration, and interpretation of data obtained from open and covert sources. Industrial espionage is a loose, generic term that describes the harnessing of the business intelligence process in a manner that may or may not be entirely legitimate or which involves the use of a legitimately developed intelligence product to achieve an illegal end.

Open sources of business information are publicly available. They include information presented by the news media, public records, government reports, and reports issued by business competitors, such as annual reports and stock offerings. On the gray fringe are the competitors' internal newsletters, proposals to prospective clients, and similar documents that are usually not confidential and which would be impossible for the authoring organizations to control in any meaningful way.

For the user of open information, the caveat is extreme caution because the data is often a potpourri of fact, fiction, half-truths, and deliberate distortions. The challenge to the collector of publicly available information is to ferret out the factual portions and combine them with pieces of data obtained from other sources.

Covert sources of information include informants, paid and unpaid, witting and unwitting. They may be the targeted organization's regular, temporary, and contractor employees, as well as suppliers, vendors, clients, and other competitors. They may also be the wives, children, or friends of these individuals.

Also included are the collector's operatives who may be in-house employees or outside contractors, and may range in skill from amateur to veteran professional. Operative activities can consist of recruiting and directing informants, going undercover into the targeted organization, intercepting written communications to and from the target, maintaining visual and photographic surveillance of the target's activities, conducting audio surveillance with the use of covert listening devices, and posing as headhunters to possibly acquire from the target's key employees sensitive information that may be inadvertently leaked during a bogus job interview. The more odious tasks involve searching the competitor's trash, breaking and entering, and blackmailing the vulnerable.

The information sought by industrial spying is usually proprietary in nature, i.e., it is information owned by a company or entrusted to it that has not been disclosed publicly and has value. Trade secrets, patents, business plans, research and development discoveries, and the like are examples. Proprietary information is generally under the owner's protective shield, except when it is also classified government data entitled to protections afforded by the government.

The dark side of business intelligence has only recently come to be acknowledged as a serious threat to the viability of a business and, in a larger sense, to entire industries and national economies. As companies, industries, and nations move to dependence on technologically intense products and services, as is the case in the United States, business spying will expand and intensify. Adding fuel to this fire is the availability of national spying infrastructures that can be converted from military to business objectives.

John J. Fay

COMPETITIVE COUNTERINTELLIGENCE

Competitive Counterintelligence (CCI) is an organized and coherent process that is characterized by anticipatory and proactive steps designed to identify and neutralize attempts to obtain that intellectual property and other proprietary information which contribute materially to a firm's competitive advantage.

Just as counterintelligence as practiced by national agencies rarely seeks criminal prosecution as an outcome, CCI is also focused largely on prevention and active intervention rather than ex post facto investigation and other actions that typically must adhere to strict legal protocols. Indeed, CCI seeks not only to prevent illegal attempts to compromise a firm's information, but also to deal with the far more prevalent legal and ethical—yet just as potentially problematic—methods employed by aggressive businesses world-wide.

The Competitive Counter Intelligence Cycle

CCI is most often depicted in a circular form comprised of seven major elements:

Identification of the Critical Elements. Rather than attempting to safeguard everything, all the time, this part of the process seeks to identify those elements that provide a competitive advantage from several perspectives—what must be protected, for how long, from whom it must be protected and where it's located. This allows a focused, and concentrated picture upon which the remainder of the process depends and allows prioritization and resource allocations.

Assessment of the Adversary(ies). Here, an in-depth analysis of those companies or other actors in the marketplace (e.g., an environmental protection group that attempts to subvert sympathetic employees of an oil company into providing information that can be used to damage the firm) and the capabilities, approaches, techniques that they have been known to use—or which they can be reasonably expected to use—in gathering information about the firm. Fundamentally, this requires an understanding of how aggressively the firm operates with its internal counterintelligence assets, which kinds of constraints they place on internal or external collectors of information, and the origins of those collectors (which can range from aggressive and talented former government intelligence officers to fairly benign librarians). This assessment also takes into consideration the relationship that the opposing firm has with its own domestic (national) intelligence service and the degree of cooperation they enjoy, as well as the differences in attitudes, principles, and actions between countries and regions of the world.

Testing of the Firm's Vulnerabilities. Once there has been an identification of what might plausibly be at risk within the firm and the extent that it may be sought after—and the approaches that a business rival are known or can be reasonably postulated to undertake—the firm will attack itself by replicating such approaches as nearly as possible, thus gaining an accurate picture of the

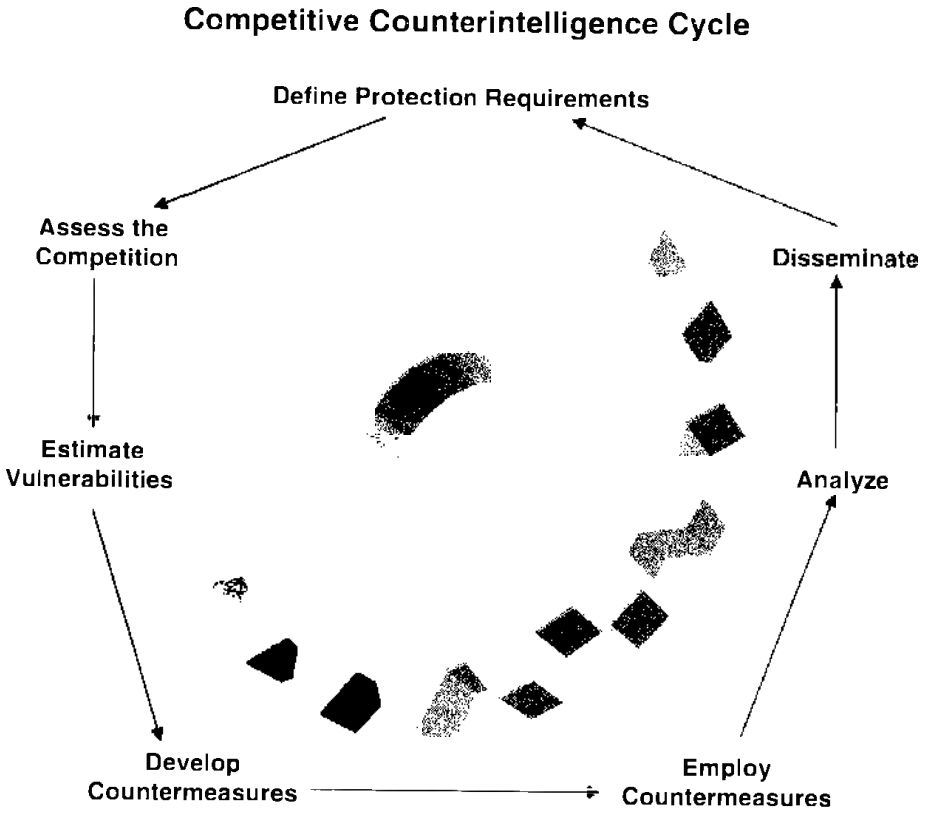


Figure 11. The competitive counterintelligence cycle is a process that begins by identifying company holdings that need to be protected; characterizes threats against the holdings; identifies weaknesses in the scheme that protects the holdings; devises protective methods for reducing or eliminating the weaknesses; implements the protective methods; evaluates the effectiveness of the protective measures; and on a regular basis informs the company's leadership of changing threat conditions. The need to adjust starts the cycle again.

extent to which present protective measures and processes need improvement or initiation. Typically, this "penetration testing" is performed by a trusted, yet outside supplier of such services in order to provide as realistic an appraisal as possible, uncontaminated by suggestions that inside knowledge of vulnerabilities has compromised the integrity of the process.

Design of Appropriate Countermeasures. Once there is a clear picture of the actual vulnerabilities, appropriate countermeasures are developed and presented with recommendations for implementation. And, beyond the obvious practical, financial, and procedural conditions, other factors such as the culture of the organization are taken into account when selecting the appropriate countermeasures.

Implementation of Countermeasures. Countermeasures take many forms and can range from very inexpensive yet effective (mostly procedural) to educational, physical and electronic or a combination. An important element of the countermeasures is the development of performance metrics that help to determine the efficacy of such standards.

Analysis of the Countermeasures. As surely as electricity will always seek and find the paths of least resistance, so too will business rivals that are intent on obtaining proprietary information. Once roadblocks are placed in their way, they will seek alternatives, thus changing the threat picture in accordance with the countermeasures arrayed against them. Regular testing and measurement according to the metrics established earlier help guard against false expectations of effectiveness.

Dissemination of the Analyses. Having started with the leadership that defined the corporate holdings that are needful of protection, the circle is completed with regular reporting as to the threat conditions as they relate to the protection of the firm's competitive advantages.

The ability of a firm to demonstrate that it has taken appropriate countermeasures to protect its intellectual property and other information assets—countermeasures consistent with the threat environment—plays a large part in any misappropriation litigation. Should there be a loss, and the firm is unable to show that they fully appreciate the value of their information and have taken such reasonable measures, the chances of being able to prevail are dramatically reduced.

CCI closely mirrors the Competitive Intelligence Cycle and when the two are combined into an integrated set of protocols, as is the case with many modern, sophisticated businesses, they are referred to as Business Intelligence. See separate entries under Business Intelligence, Competitive Intelligence, Economic Espionage, and Industrial Espionage.

John A. Nolan, III

COMPETITIVE INTELLIGENCE

Competitive Intelligence (CI) is a formalized business process that seeks to advance a firm's advantages through an increased understanding of the various forces present in, and influencing, their marketplace. CI is focused on supporting the defined intelligence needs of a decision maker, characterized in modern use as "actionable." Actionable intelligence means that which arrives in time, with the requisite degree of accuracy, and absence of bias or prejudice in order to take the most effective actions.

Fundamentally, CI has its origins in national and military intelligence principles, practices, and processes which have been under development and modification for literally thousands of years. The business applications of these processes, however, have only been recognized as a discipline since the early 1980s. Large and medium sized firms across many different industrial sectors and across much of the world have established CI functions and units. Generally speaking, the more competitive and resource-intensive the industry, the greater is the likelihood that a firm will have an established CI organization. For instance, the pharmaceutical industry houses many of the benchmark units since the risks are so great. Bringing a new drug to market may require an investment of $800–900 million and take ten years from identification of the molecule to introduction of the pill.

Most CI practitioners, whether embedded within a corporate structure or employed by the numerous consulting firms around the world, follow a well-established intelligence operational cycle. The cycle is comprised of a six-phase protocol, beginning with the *requirements definition* that defines and describes what the decision-maker needs and when it is needed. Next, the requirements are distributed as *tasking* to those who are

in a position to collect the information. The *collection activities* are then undertaken according to standards of the firm, the country, or other professional standards. In many parts of the world, the Code of Ethics of the Society of Competitive Intelligence Professionals (Alexandria, Virginia, www.scip.org) provides a framework for these collection activities. Once the information is collected, it is *processed and reported* either orally, in writing, or in an electronic format to those who can collate it and make sense of it. The *analysis* is undertaken in ideal circumstances by specialists with a unique understanding of issues that are separate and distinct from the understanding of those who collected the information. Analysts are responsible for the removal of biases, prejudice, and misconceptions which may have been present in the reporting prior to making judgments as to the implications of the intelligence and *disseminating* those estimates to the decision maker—thus completing the cycle.

In the U.S., for example, approximately 360 of the Fortune 500 have installed CI practices at organizational levels from the corporate (strategic) to the business unit (tactical), providing the intelligence needed by business leaders to make long- or short-range decisions, avoid—or at least mitigate—surprises, and to monitor the activities of significant players in the marketplace.

CI is not solely limited to information about competitors. Instead, the focus of virtually every sophisticated CI unit is quite wide and satisfies intelligence requirements about nearly every element that influences competitiveness. An easy way to depict the differences is to suggest one or two of the literally thousands of questions that relate to a company's ability to survive and prevail in the marketplace:

- *Competitor Intelligence*: What is our competitor doing today, or planning to do tomorrow that will take away market share from us?
- *Financial Markets Intelligence*: How do key investors view us and our competitors, against the conditions of the marketplace? How will changes in monetary practices in Country X affect our ability to operate there?
- *Legislative Intelligence*: What is the impact of current legislation that is being formulated

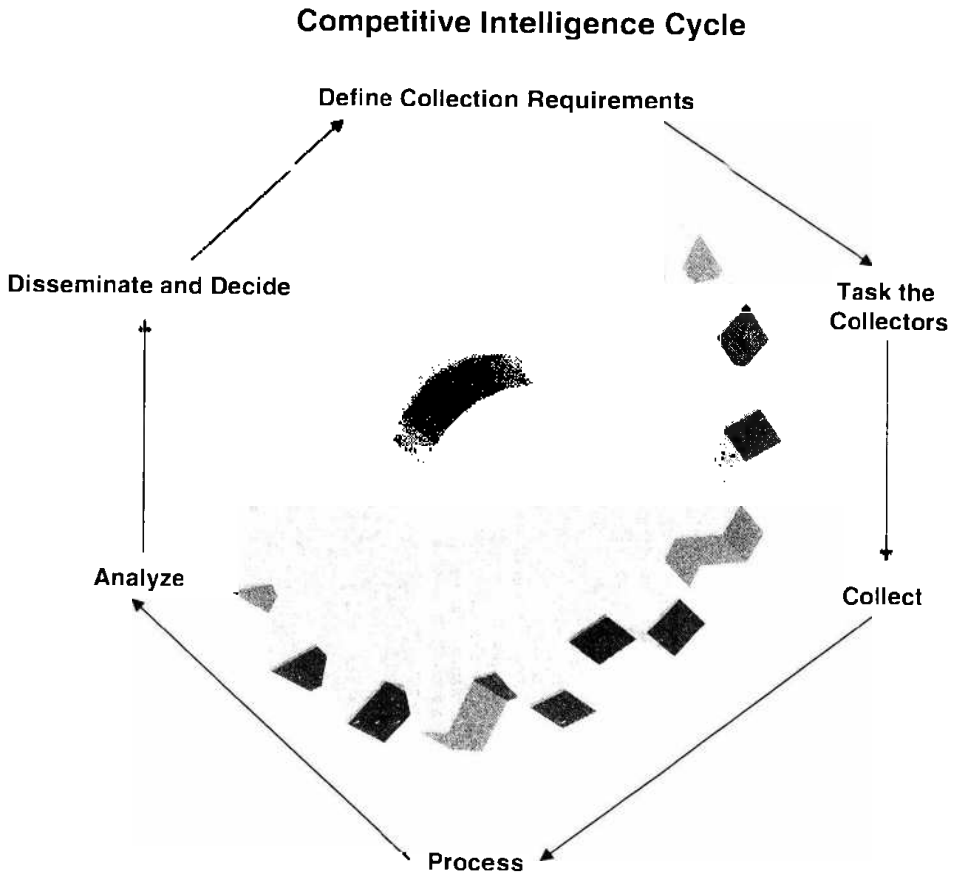


Figure 12. Information moves in a cycle from collection to dissemination.

in State Y on our operations? What can we do to influence that legislation?

- *Regulatory Intelligence:* How are planned rules issued by a state or federal regulatory agency going to affect our industry and our company? How must we change our business processes, products, or practices in order to avoid compliance problems? What will be the financial impact of those changes?
- *Customer Intelligence:* How much money has our customer set aside for this purchase? Who will make the actual decision about buying from us? How does he make his decisions and how can we get inside his decision-cycle and influence him toward us?
- *Supplier/Vendor Intelligence:* How reliable is supplier X compared to Y? How old is his manufacturing line? How financially reliable is the firm? How effective are their quality control measures? How many delivery dates have they missed in the past five years? What are their actual capacities? How well will they safeguard our proprietary information as they manufacture the sub-components of our system?

CI can be easily and broadly differentiated from other business processes such as market research, corporate libraries, data mining, and knowledge management. CI is most often about what will happen, not what has happened, thus there is little potential for literature—whether in print or electronic form—to describe what is going to happen. Rarely is CI statistically based, such as the results of a market research focus group study might be, since there are rarely multiple sources with access to the same kind of information—indeed, there may only be one such source. Uniqueness, however, does not disqualify a single source or the information as unreliable. Indeed, the aggregation and analysis of small, perhaps even unremarkable bits of information from diverse sources—none of which may represent or provide the entire answer by itself—can represent other differentiating elements. Data, information, and intelligence are compared not only in relative amounts, but also in the processes generally associated with each.

Competitive Intelligence is also different from Industrial Espionage and Economic Espionage, which cross the lines of legal and ethical practices.

John A. Nolan, III

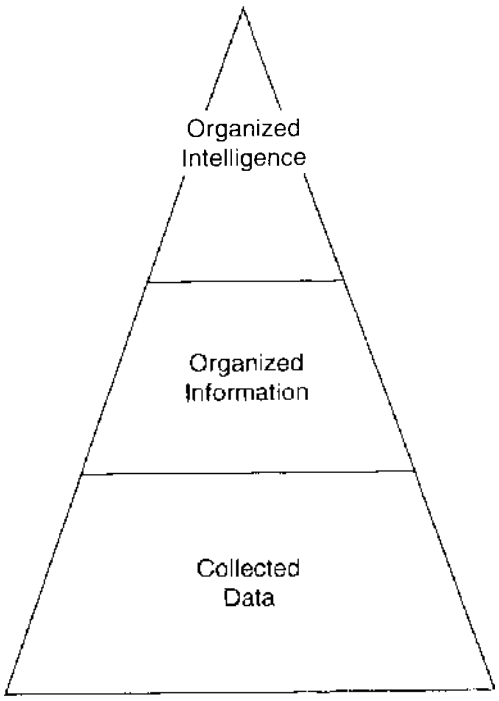


Figure 13. Mass is reduced and refined as data move up.

COMPUTER SECURITY: DISASTER RECOVERY

The focus of the disaster recovery business has been in a state of change since the mid-1980s. In past years, the industry had concentrated almost exclusively on backup capabilities that could be called into service, should a disaster occur. Now, the focus is on mitigating points of vulnerability that could result in a system loss. Finding the single point of failure, or the weakest link in the chain, is the central objective.

The disaster recovery industry has had a relatively short history that has evolved with the advent of computerization. As businesses have become dependent on systems and could not revert quickly to manual practices, it has become evident that system downtime could prove catastrophic. In the early days of disaster recovery, the emphasis was placed on establishing backup facilities; today, that is not enough.

During the past two decades, computer operations have shifted from batch processing operations to real-time environments. This shift has coincided with the concepts of "just-in-time" manufacturing and with the trend toward drastic

reductions in inventory. In batch processing environments, business operations simply required a backup operating system for disaster recovery. In real-time, however, downtime is intolerable.

In contrast to the focus on backup data procedures, today's planners must analyze the total infrastructure of computer operations, identify single points of failure, and develop strategies to mitigate exposures. This requires extensive analysis.

Computer operations require power, environmentally controlled operating facilities, telecommunications services, and skilled operating personnel, among a litany of other supporting functions. Failure of one component may mean compromise of the entire system. For businesses of today, that could mean catastrophe.

Disaster Recovery Analysis

An analysis begins by defining operating components. If the focus is computer operations, which it is in most cases, this would include each component of hardware, software, database, operating personnel, telecommunications, and the supporting infrastructure of power and environmental controls. Each component must be listed and categorized based on criticality.

Possible threats are defined next and placed in categories based on the probability of occurrence. Threats include natural disasters, accidents, criminal events, and even operational threats such as mismanagement of the system or of the people operating it. Threats are correlated with each element of the system and an order of priority established, so the most vital elements are considered first. This correlation notes which threats are applicable to specific system components and which are not.

The vulnerability of each element is defined by outlining the process by which a specific element may be subject to a specific threat. Through this process, the Achilles heel of the overall operation is identified.

In the final phase of analysis, countermeasures are selected to mitigate the exposures noted in the vulnerability analysis. This involves eliminating single points of failure and providing substantial backups for critical system components that may compromise the entire operation. Exposure mitigation may be considered the single most important aspect of disaster recovery planning.

Emergency Plans

Of course, exposures can never be completely eliminated. Consequently, emergency plans are needed that define procedures for actions to take in the event of a system loss, despite the effort to mitigate exposures. These procedures can be subdivided into the following phases as outlined below.

Phase 1: Prewarning

a. Evacuation procedures
b. System shutdown procedures
c. Identification of shelter facilities

Phase 2: During the Event

a. Endurance techniques
b. Survival techniques

Phase 3: Immediately After the Event

a. First aid accommodations
b. System shutdown procedures
c. Notification of response authorities
    1. Police
    2. Fire
    3. Rescue
    4. Utility crews
d. Security of the scene
    1. Control of access
    2. Preservation of evidence
e. Traffic control
f. Removal of injured
g. Notification of regulatory agencies
h. Summon emergency management team
i. Implement containment strategy

Phase 4: Post-Event

a. Clean-up
b. Repair
c. Alternate site operation
d. Notification to next of kin
e. Legal services
f. Mental health services

Phase 5: Resumption of Normal Operations

a. Plan for return to facilities and operation restart

Data Gathering

Following is an outline of tasks essential for developing the content of the plan:

1. Conduct interviews within the organization in order to:
   a. Identify key systems.
   b. Define shutdown and evacuation requirements.
   c. Examine feasibility of alternate site operation.
   d. Identify chain of command and succession of authority.
   e. Identify likely issues that management will need to address during the event.
   f. Define regulatory agency reporting requirements.
2. Meet with response agencies (such as police, fire, rescue services, the emergency management agency, and public utilities companies) in order to:
   a. Determine the methods of interagency communication.
   b. Note who is to be called.
   c. Identify the needs of emergency response forces.
   d. Identify routes to, from, and within the site.
   e. Define utility needs.
   f. Define action steps and responsibilities for preserving the scene.
   g. Identify key safety considerations.

Formal Document. The collected data should be presented in a formal document that addresses the following issues.

Plan Coordinator. One person should be identified as responsible for preparing the plan document, communicating it to interested parties, revising and updating the plan, and organizing training to facilitate proper execution.

Management Authority. The plan should delineate the chain of command that will apply in the carrying out of plan functions, provisions should be made for succession of authority, and the duties of key figures will be described so as to leave no doubt concerning personal accountability. This portion of the plan might also take note of legal and corporate restrictions.

Security Response. This plan element defines the tasks to be performed by security, such as facilitating access by public authorities, directing traffic, controlling spectators, preserving the scene, rendering first aid, coordinating evacuation, and making notifications to emergency response personnel.

Communications. The plan should spell out the methods for establishing and maintaining communications among the various agencies involved in responding to a disaster. A number of separate networks are likely to be utilized in moving critical messages simultaneously.

Agency Notifications. The plan should include a detailed listing of agencies that are required to be notified in a disaster. The nature of the disaster will determine the agencies to be contacted and the order of contact. The agencies likely to be identified in the plan include the Federal Emergency Management Agency (FEMA), Federal Aviation Administration (FAA), Environmental Protection Agency (EPA), and Occupational Safety and Health Administration (OSHA).

Support Services. These include hazardous waste cleanup, fire salvage, office repair, cleaning, and other specialized services that may be required to remove materials left in the wake of a major disaster. This part of a plan also addresses the use of specialized professionals such as psychologists and lawyers.

Public Relations

A strategy for dealing with news media and making next of kin notifications should be included. It will assign responsibilities for prompt collection of information of interest to the media and identify the authorized spokespersons. Families of persons injured or killed in the disaster will be informed quickly, according to procedures that respect privacy needs.

Disaster Response Equipment and Facilities. The plan should identify the equipment and facilities that will be fully or partially dedicated to disaster-response activities. These include an emergency management center, first aid-triage center, salvage and storage areas, media center, and alternate operating site. The technicians who provide the related services, such as communications coordinators and paramedics,

might also be mentioned in this section of the plan.

Alternate Site. The plan might include provisions for moving employees and equipment to an alternate location in order to maintain continuity of essential business operations. In this event, the company will need to include as response agencies (although not as emergency responders) the vendors who will provide the alternate site, transport to and set up equipment at the alternate site, provide temporary backup equipment, prepare the alternate site for operation, and so forth.

Resumption of Normal Operations. The plan should give guidance for resuming normal operations. Points to be considered include cleaning up, restoring utilities, ensuring that safety risks have been removed, and obtaining public authority approval for a return to business as usual.

Sal DePasquale

COOKIE AND SPYWARE BLOCKERS

The most widely used monitoring tool on the World Wide Web is the cookie. A cookie is a small file that generally holds some unique identifying information. When computer users visit cookie-powered websites a cookie file or several cookie files are downloaded into the cache of the web browser. The cookie identifies the computer user to the website during each visit.

Cookies were designed to help computer users by saving them time when they visited websites that require registration or a login process. The website developer also benefited by being able to serve the visitor faster and to track the frequency of visits and the preferences that a user has in browsing, shopping, or researching. The website is able to match the visitor with their profile information stored on a server.

Examples of benefits for both the user and an e-commerce site are functions like speedy check out or quick purchasing. The visitor saves time and the website saves resources by not having to serve up numerous pages to get an order for merchandise processed.

Many web marketing companies utilize cookies to bring targeted advertising methods to cyberspace. These cookies can be identified by every website that uses the services of the marketing company and data can be collected over a period of time to create a profile of individual Internet users. This allows websites to selectively display banners for products or services that the visitor had expressed interest in during their visits to various websites. Cookie-blocking software packages provide a variety of functions including:

- The ability to add servers and cookies to file and designating them as always accept, accept for session-only, or reject.
- Automatically being able to accept or reject cookies received from unspecified servers without user interaction based on designation or expiration date.
- Automatically being able to accept or reject certain types of cookies without user interaction.
- Maintenance of a list of the cookies accepted and rejected from all servers for current sessions.
- Classification of cookies already stored on the computer.

In addition to cookies are several types of invasive parasitic programs designed to install and maintain themselves on a computer without the permission of the computer user. These include web bugs, spyware spybots, adware, malware, browser hijackers, and keyloggers. Web bugs are often unseen graphic files that load with a web page. Once installed they can track activities and gather information about computer usage and send that information back to a server someplace on the Internet.

There are several symptoms that indicate a computer may have been infected with parasitic code; for example, unusually slow Internet connection, computer freezing or hanging, frequent system crashes, an unusual long time to boot-up, and an unusual level of bandwidth usage. In addition, unauthorized websites may have added an icon to the desktop or added themselves to the browser's list of favorite Internet websites.

Anti-virus and firewall protection is often bypassed by parasitic software because many of these programs are small and very stealthy. In addition, manual removal is often difficult

for computer users that do not have technical skills.

There are several software products on the market to protect computers against parasitic code. The annual costs for these products range from $30 to $50. Bear in mind, as with all protective products, staff time will be required to install and maintain the software. The functionality of anti-invasive software products can include:

- Automatic review and removal of all various forms of parasitic software.
- Automatic updates of the software with new threat detection profiles.
- Detection and removal of registry entries made by parasitic software.
- Interception of parasitic file downloads.
- Monitoring and logging of parasitic software that tries to install on computers.
- Quarantine of infected or suspicious files.
- Removal of objects or modules that hijack Internet browsers.
- System scanning to detect parasitic software.

Michael Erbschloe

Source Erbschloe, M. 2004. *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code.* Boston: Butterworth-Heinemann.

DIGITAL CERTIFICATES, DIGITAL SIGNATURES, AND CRYPTOGRAPHY

Cryptography is the study and practice of protecting information by data encoding and transformation techniques. It includes means of hiding information (encryption) and means of proving that information is authentic and has not been altered from its original form (such as a digital signature).

In the physical world, a key is the device used to open or close a lock. Thus, in cryptography the information used to "lock" data to protect it is called an encryption key, a cryptography key, or sometimes just a key when the context allows it.

The primary means of cryptographic key protection is based upon pairs of very large numbers which have a special relationship to each other, whereby you encode with one number and can only decode with the other, and vice versa. Yet you cannot figure out one number if you have the other number. These two cryptographic keys are known as a Public Key/Private Key pair, because the user makes one key public and keeps one key private. This means of protection is called Public Key cryptography, or Asymmetric Cryptography, because a different key is used to decode the information than was used to encode it. Since no secret keys are shared, public key cryptography allows two parties (or two systems) to securely communicate with each other without prior contact.

Digital Signatures

Another application of Public Key cryptography is Digital Signatures. To sign an e-mail message, a user can employ cryptographic software to perform a calculation involving the user's Private Key and the message. The result of the calculation is called a digital signature and is attached to the message. Anyone who has the user's Public Key can decode it, ensuring that the information is not altered and is indeed sent from the owner of the Private Key.

Thus, a digital signature is used to perform two types of authentication: it authenticates the sender of the message by proving who the sender was (or party to a transaction), and authenticates the information by proving that it hasn't been altered.

A digital signature is additional data that is appended to data in transit or storage. It functions similarly to a written signature to check and verify who the sender is. Second, similar to a tamper evident seal on a package, checking the digital signature also reveals whether or not the data has been altered since it was signed.

Digital Certificates and PKI

To verify a digital signature, the verifier must have access to the signer's Public Key and assurance that it corresponds to the signer's own Private Key. However, public and private key pairs are just numbers. Some scheme or strategy is necessary to reliably associate a particular person or organization to a particular key pair. The

solution is the use of one or more trusted third parties to associate an identified signer with a specific public key. That trusted third party is referred to as a Certificate Authority (CA), because it issues electronic certificates known as digital certificates.

A digital certificate is a specially formatted block of data that among other things: (1) contains the certificate's serial number, (2) identifies the certificate authority issuing it, (3) names or identifies the certificate's subscriber, (4) identifies the period of time for which the certificate is valid, (5) contains the subscriber's public key, and (6) is digitally signed by the certificate authority issuing it. By digitally signing the issued certificates, the certificate authority guarantees the authenticity of the data held in them.

The publication of digital certificates is what enables two parties (or systems) to use certificates to communicate securely without prior contact. The international standard governing digital certificates is X.509, a specification for digital certificates published by the ITU-T. FIPS 201 requires X.509 certificates.

A Public Key Infrastructure (PKI) is a security management system including hardware, software, people, processes, and policies (including Certificate Authorities (CAs) and Registration Authorities (RAs), dedicated to the management of digital certificates for the purpose of achieving secure exchange of electronic information. The term PKI is also sometimes loosely used as a reference to public key cryptography.

Digital Certificate Verification

A digital certificate is no longer valid if it has expired or been revoked. There are two methods of determining if a certificate has been revoked: checking a locally stored certificate revocation list (CRL) issued by a CA, and using the online certificate status protocol (OCSP) to obtain the real-time status of the certificate.

FIPS 201 Cryptographic Keys, Digital Certificates, and Digital Signatures

Prior to FIPS 201 (the U.S. Federal Personal Identity Verification program), the use of cryptography in physical access control systems was for encryption of Ethernet network traffic (front end system to panels, front end system to workstations, and panels to readers). FIPS 201 introduces the additional elements of digital certificates and digital signatures to provide strong authentication of the card, the data elements on the card including biometric data, and also of the individual card management's system.

FIPS 201 specifies that, at a minimum, the Personal Identity Verification (PIV) Card must store one asymmetric private key called the PIV authentication key and a corresponding public key digital certificate, and perform cryptographic operations for authentication (such as "challenge and response"). The FIPS standard states that this key must only be available through the contact interface of the PIV card, and a PIN must be provided by the user before cryptographic operations can be performed. The card must hold the X.509 digital certificate for each asymmetric key on the PIV card.

FIPS 201 requires that the generation, handling, and physical security relating to all PIV cryptographic keys shall meet certain specific requirements.

Jill Allison

Source D'Agostino, S., Engberg, D., Sinkov, A. and Bernard, R. 2005. "The Roles of Authentication, Authorization and Cryptography in Expanding Security Industry Technology," *SIA Quarterly Technical Update.*

ECONOMIC ESPIONAGE

Economic Espionage is typically practiced by professionals employed by the national intelligence services of the country where a company is domiciled. For example, a domestic French company desiring information about a competitor in another country enjoys access to the world-wide operations of the French government's intelligence services to help satisfy those information requirements.

Many, although not all, modern nations employ their intelligence services in this way. Indeed, in terms of cooperative assistance from intelligence services, countries operate across the spectrum from being wholly and actively engaged to those which keep an arms-length relationship with most businesses

unless absolutely necessary for the survival of an industrial sector, to those countries (such as the United States of America) where such cooperation has a long history of being illegal and discouraged. For example, Clinton Administration attempts during the 1990s to change the laws in order to enable American firms to obtain assistance from national resources were almost universally rebuffed by companies, the Congress, and the intelligence community itself.

Most countries that do participate in such activities base their degree of cooperation on a simple premise: if economic power and influence are fundamental to the national security, embodied by its commercial and industrial interests, then it naturally follows that resources of the state should be available to assist those companies. Beyond the philosophy, there is clear economic value to using a nation's intelligence service: by comparison with the risk, the gain is enormous. The further and further behind a country is (or is becoming) technologically, the greater the temptation to use illicit means to steal the information that represents the competitive advantage that another holds.

In its simplest formulation, consider that Company A has invested $100 million in developing and bringing to market a new technology; enjoying "first-to-market" advantage, it hopes to capitalize its second generation with revenue from the first generation's dominance. Company B, in the same industry, uses its country's intelligence service to obtain the discriminating information for $500,000. Company B can use any considerable portion of the $99.5 million difference to their own Research and Development, and leapfrog Company A by bringing the second generation to market before Company A's original investment has been repaid.

In cases such as these, there is usually a clear *quid pro quo*. Not only does the intelligence service provide assistance to its companies, it also expects and typically receives the cooperation of employees of those serviced companies when they reside in or travel to other countries and can be expected to report on matters of interest.

Countries can offer a panoply of services for their domestic companies, including but not limited to the use of human assets, overhead platforms, or signals intercepts, or a combination of all three for collection. Government analysts also assist those firms in determining the accuracy and/or utility of the information obtained by the national means and resources.

Countries that subscribe to, and practice, this close linkage between their intelligence services and business interests include Russia, China, Taiwan, Korea, India, Japan, Brazil, Israel, and France.

The amount of support by foreign intelligence services to their domestic firms reached such proportions that American industry lobbied very hard in the middle of the 1990s for protection at the national level. Most companies realized that their own, organic security apparatus was overwhelmed by the complexity and sophistication of intelligence services threats to their intellectual and proprietary information; they also realized that there was little deterrent value under the civil Trade Secrets laws; or the desire or ability of local law enforcement officials to become effectively involved in any attendant criminal prosecutions that might arise from a misappropriation.

The result was the enactment of the Economic Espionage Act of 1996, which both federalized and criminalized such conduct by foreign intelligence services representatives. Under this legislation, the U.S. Justice Department initiates investigations through the federal Bureau of Investigation and any subsequent prosecutions in federal court; and with a combination of jail time and fines in the millions of dollars range.

An unintended consequence of the Act, in which the U.S. State Department's suggested that there be penalties for domestic misappropriation by one company from another, is that there have been a greatly disproportionate number of prosecutions of American individuals and firms than there have been against foreign enterprises. By 2006, of the nearly 60 cases brought, only three have been focused on foreign intelligence services.

There is frequently a direct relationship between the closeness and resulting efficacy—with the level of dedication and sophistication of counterintelligence practices. Simply, they recognize what has worked for them and wish to keep what they have from others. Thus, the aforementioned Economic Espionage Act in the USA is not alone on the world stage. Indeed, some countries such as Korea

and Japan are far more draconian in their punishment provisions.

John A. Nolan, III

INDUSTRIAL ESPIONAGE

Often considered the catch-all phrase to describe intelligence operations in the business world, industrial espionage is actually differentiated on several levels from other approaches to obtaining information about another company.

Industrial espionage is typically sponsored by companies that push the envelope—either wittingly or unwittingly—past the limits of acceptable, ethical, or even legal conduct. In this regard, industrial espionage can range from "gray" to "black."

Gray operations include a variety of approaches that are considered to be on the fringe of ethical activities but which do not rise to the level of illegality. Examples include:

- Ruse interviews designed to trick employees of a target firm into providing information to an outsider by using social engineering techniques that capitalize on a range of vulnerabilities, e.g., a lack of employee sophistication, low level of security awareness, and a desire to assist. In a telephone call, the interviewer can pretend to be a fellow employee from another department of the same firm or a disgruntled customer, to name a few.
- Dumpster diving in which the information collector seeks to capitalize on the tendency of employees to simply throw documents or materials into the trash, with no expectation that anyone would attribute value to the trash. Constitutional constraints on unlawful search and seizure by law enforcement are well-known and cause popular beliefs that such activities are illegal. In fact, however, when private actors (not law enforcement officers) search or take trash, the Principle of Abandonment applies: throwing material into the trash clearly shows that the owner believes it no longer has any value and thus, taking something of no value is not a crime. While certainly unsavory and generally odiferous, dumpster diving is not illegal. Entering a company's property in order to gain access to a dumpster may constitute criminal trespass, yet even that is compromised when a number of companies in a building or office park use a common dumpster.

Black aspects of industrial espionage are those areas which clearly move into the range of illegal conduct. Examples are:

- Bogus employees being placed inside a competitor firm for the express purpose of stealing information, plans, intentions, products, or committing sabotage.
- Hacking into computer systems to either steal information, corrupt data files, degrade a firm's ability to conduct business, or any of the other nefarious options that systems afford in modern business.
- Bribing a knowledgeable employee into providing information that is not otherwise available through legal means.
- Blackmailing or co-opting a knowledgeable individual, usually after making the individual vulnerable to blackmailing or co-option.
- Clandestine interception of communications. These can take many forms ranging from compromising a telephone to bugging conference rooms, invading videoconferences, and the like.

Industrial espionage can be found on the domestic and international levels. The usual practitioner is not in an intelligence service or someone with an intelligence background. Depending on the degree of operational intensity, industrial espionage is practiced by various actors ranging from private investigators to outright criminals. Typically, such persons are employed by aggressive, perhaps naïve, managers at lower levels of an organization; the acts are usually not commissioned or encouraged by senior management. The objectives are usually short-term and tactical as opposed to strategic issues that are the concern of people at the top of the organization. Ethical considerations are often in the eye of the beholder.

The availability of advanced technology, to even the smallest company, has made information collection possible in myriad ways on a grand scale. Many of the new and technical collection methods exist outside of the law, and methods that were once illegal are now less so. An example is the matter of aerial photography.

A 1980s Texas ruling barred handheld photography from aircraft flying over a plant. The ruling is now essentially moot because satellites routinely and legally take photographs from the air, and do so with state-of-the-art photographic equipment.

John A. Nolan, III

MANAGEMENT OF SENSITIVE INFORMATION

Information Is Expansive

Unlike other business resources, information is expansive, with limits imposable only by time and the thinking capabilities of humans. Information may age but will not deplete; it reproduces rather than diminishes. Information is compressible and transportable at very high speeds, and can impart advantages to the holder. Many work endeavors, such as research and development, education, publishing, and marketing, are very highly dependent on information.

Information Protection Requires Barriers

In ancient times the walled city was man's way of protecting himself and his property. Walls were a key defense against armies, they kept roving bands of robbers at bay, and at night, when the gate was closed, they blocked the escape of criminals. After the sack of Rome, walls became a way of life. During the next one thousand years, which we call the Middle Ages, men and their property found refuge behind walls. It was not until the Renaissance brought a period of renewed interest in art, science, and commerce that men began to venture out from their walled cities.

The ancient walled city is analogous to the modern business corporation. Starting in the middle of the last century, when computers began to play a commanding role in processing and storing information, a businessman could feel safe because information assets were behind electronic barriers inside centrally controlled equipment located within the protected confines of a computer room—sort of like a city with three walls. Then came the computer Renaissance. Many companies moved from a centrally based approach to a system of widely dispersed personal computers, which we call a LAN or local area network.

In a typical LAN, nearly every employee has a PC at his or her work station; many have company-owned PCs at home; and some employees carry portables everywhere they go. Instead of holding information at one central location, in the custody of a handful of trusted technicians, information is made available to nearly every employee. In companies where this is the case, information assets have moved out from behind protective barriers.

Information Is Costly and Important

Information is deserving of protection for at least two reasons: (1) it is costly to acquire and maintain, and (2) it is important to the success of the business enterprise. Information fuels a business and has value in much the same sense that people, physical property, and financial assets have value. Information that an enterprise assembles for making a major business decision or developing a new product may cost many millions of dollars and be absolutely essential to viability. For example, an oil exploration company can easily spend in excess of a hundred million dollars just to get to a point that allows a sensible decision to be made about where to place the drill bit. If the decision proves correct, oil producing operations are assured, and the company stands a good chance of recouping its investment many times over.

Information Is Coveted

And, like anything of value, information is coveted. When something has value, count on the certainty that someone will be looking for an opportunity to take it away. The bad guys are not thugs and common sneak thieves; they are intelligent, clever, and ruthless people such as the professional spy that steals information without the owner ever knowing it, the executive that defects to a competitor carrying a briefcase full of proprietary secrets, or the disaffected scientist that sells R&D data.

Information Has a Limited Life

Efforts to safeguard information assets in an open environment are made difficult by a host of realities. Chief among these is a recognition that a

piece of information has a limited life, i.e., that at some point in time, which is usually sooner than later, the information will lose all or most of its value. Within the time frame of value, the owner of the information will want to extract from it the maximum worth possible. This means making the information available to users whose special talents can exploit it. Oftentimes the users of the information are numerous and are spread across a global landscape. In these circumstances, the information has been duplicated repeatedly and transmitted widely by a variety of communications media. During the time information is in a state of flux, the opportunities for compromise are many and diverse. Worse still, when compromise occurs it is difficult, if not impossible, to detect.

Information Is Difficult to Protect

Problems in protection are compounded when a company finds it necessary to share its information with outsiders, such as joint venture partners and contractors. As an example, a joint venture's operational information, which is routinely available to all partners, may be of a nature that if released to the public would affect stock prices, a result that might be good for some partners but not for other partners. When sharing information with contractors, two examples of exposures stand out. First is the risk that sensitive information entrusted to the contractor will leak out, a likelihood that increases when the contractor works for competitors. The second type of exposure is present when an outsourcing arrangement puts the contractor in control of a company's critical business data or of the systems that massage the data. In a like sense, the arrangement called partnering, which brings a company and a vendor into a mutually rewarding relationship, can result in both organizations sharing each other's sensitive business data.

Information Is Voluminous

Another reality is that companies are dealing in larger volumes of information than ever before. Great amounts of raw data are needed to make fully developed analyses, and the judgments that flow from them produce not just a favored recommendation but a range of options, each with its own set of variables and predicted outcomes. Of even greater moment is the reality that the criticality of information is increasingly on the rise. Not only is there more information, but it is high-impact information.

Factor in the reality that the means of communication are changing. The fax machine, cellular telephone, electronic mail, modem, and voice answering device are examples of changes in the way companies communicate. All of these have serious security vulnerabilities. The task of protecting information is daunting to say the least.

Operations Security (OPSEC)

Operations Security (OPSEC) is the name of a program initiated and used for the most part by the Department of Defense (DOD). Due mainly to the terrorist threat, the program moved into high gear and is now generating a considerable degree of interest on the part of security professionals in the private sector. An OPSEC program differs from an information security program. Its focus is on the concealment of sensitive activities as opposed to the protection of sensitive information.

OPSEC Process

OPSEC is the process of:

- Denying to potential adversaries information about DOD capabilities and/or intentions by identifying, controlling, and protecting evidence of plans and practices related to sensitive activities.
- Analyzing unfriendly attempts to penetrate the protective shield surrounding sensitive information.
- Concealing in-house activities that if known to an adversary would have a detrimental effect on national defense.
- Identifying seemingly innocuous information exposures that if collected by an adversary over time would have a detrimental effect on national defense.
- Finding and eliminating vulnerabilities.

The attractiveness of OPSEC to CSOs is a "get tough" approach. For the business organization it means having strict information security rules, enforcing the rules and meting out punishment for violations, and making referrals to the criminal justice system for egregious offenses.

The OPSEC approach can be harnessed to three business-survival imperatives:

- Prevent loss or compromise of privately owned technology
- Prevent business competitors from learning the intentions of the organization
- Prevent terrorist groups from characterizing the organization's most critical assets and assessing weaknesses in the protection of them

Sensitive Information

Security professionals use the term "sensitive" when referring to information that has value and is protected. The main forms of sensitive information are:

- Proprietary business and technical information
- Personal data concerning applicants, employees, and former employees
- Proprietary information owned by partners and obtained through an agreement

Access to or knowledge of sensitive information is based on a need-to-know connection to job tasks. An employee whose job is to invoice vendors does not need to know the CEO's plan to spin off a subsidiary. Jobs and groups of jobs are compartmental by nature; confining sensitive information to compartments helps prevent information leaks.

Information protection is also afforded by avoiding careless talk outside the compartment, being careful on the telephone and in sending e-mail messages, placing sensitive information in secure containers when not in use, and ensuring that sensitive documents are turned over or distributed to authorized persons only.

A few simple steps can save a very big headache. For example:

- Be suspicious of unexpected messages, especially those with a teasing subject header.
- Be leery of attachments. If in doubt, don't open.
- Don't answer SPAM or forward chain letter messages.
- Don't use vacation messages that can tip off criminal opportunists.
- Close your e-mail application when it is not in use.
- Save sensitive messages in a secure folder.
- Choose a hard-to-guess e-mail password.

Classification

Organizations assign classifications to their sensitive information. The usual classification model is a three-tiered hierarchy. The names assigned to the tiers vary from organization to organization and include SECRET, RESTRICTED, CONFIDENTIAL, PRIVATE, and PERSONAL. The names are sometimes emphasized with preceding terms so that they appear, for example, as TOP SECRET or HIGHLY CONFIDENTIAL. For the purpose of discussion here, the three tiers from top to bottom are SECRET, RESTRICTED, and PRIVATE.

SECRET. This is information the unauthorized disclosure of which could cause serious damage to the organization's business. Its use and access to it are strictly limited. Examples include:

- Trade secrets
- Plans to merge, divest, acquire, sell, or reorganize
- Information that could affect the price of shares
- Information with high political or legal sensitivity
- Information prejudicial to the interests or reputation of the organization

RESTRICTED. This is information of such value or sensitivity that its unauthorized disclosure could have a substantially detrimental effect on the organization's business. Examples include:

- Marketing strategies
- Customer files
- Agreements and contracts
- Contentious or litigable matters

PRIVATE. This is information relating to employees. Examples include:

- Salaries, bonuses, and wages
- Health and medical matters
- Disciplinary actions
- Job performance

For convenience, sensitive information can be referred to in a project context, e.g., a project to construct a new building might be called Project Phoenix, and information related to that endeavor might be called Project Phoenix information. In this example, only certain types of information, such as financial data, are classified. Another project might be so hush-hush that all information relating to it is classified.

Sensitive information can also be regarded as falling under the "ownership" of a particular employee such as the originator, the person who assigned a classification to it, or the person who holds primary responsibility for putting the information to work.

Ownership carries with it a responsibility to change or remove the classification as needed. (Ownership does not mean that an employee has rights to the information.)

An important task of the CSO is to learn which information is sensitive and which is not. The CSO has to know which is which because classification is assigned to sensitive information only. The classification program will collapse of its own weight if overburdened. If all of an organization's information was declared sensitive, there would be no need for classification, and to the extent that non-sensitive information is given a classification, the effectiveness of the classification program is diminished.

The CSO's task of separating the sensitive from non-sensitive cannot be done without input from managers and supervisors. This is the case because the CSO, like all other employees, has access to sensitive information on a need-to-know basis. The CSO does not need to know where a drill bit is to be placed, only that a body of information exists concerning drilling. Using the three-tiered matrix discussed earlier, the manager or supervisor has decided if classification is merited and if so, selected the appropriate classification level. The CSO merely verifies that the process was followed and that the body of information still merits protection.

A CSO will think what would happen if particular information was to fall into unfriendly hands. A number of possible scenarios can lead the thinking process to an identification of what should be protected, the adversaries, the probable nature of attempts by adversaries to acquire the information, the exposures of the information to the hypothesized attempts, and an estimate in dollars of the value of the information.

Marking. Classified information, regardless of form, is marked, distributed, copied, mailed, transported, stored, and destroyed in accordance with established procedures. The procedure for marking a document might require every page to bear in the top right corner the word "RESTRICTED," stamped in upper case letters, red in color, and not smaller in height than one-half of an inch and not taller than one inch.

Awareness. The operation of an awareness program is within the purview of the CSO. The program is continuous, uses many forums, reaches out to employees at all levels, and emphasizes the duty of everyone to protect the organization's sensitive information. An awareness program sometimes includes an orientation session before an employee is granted access to classified information, one or more refresher sessions throughout the duration of the employee's access, and a debriefing at the time the employee's access is removed. These sessions, which are ordinarily conducted by the employee's supervisor, can include the signed acknowledgments by the employee and warnings as to personal consequences of violations.

The awareness program is also directed at preventing careless talk and release of details about plans, strategies, and other sensitive matters. Prior approval may be required when an organizational matter is to be discussed by an employee in a speech, article, or presentation.

Clean Desk Policy. A clean desk policy is the name given to a work rule that requires employees to:

- Place classified materials under lock and key when not in use. Materials of chief concern are classified correspondence, maps, photos, diskettes, and compact disks.
- Not leave keys unattended or hidden.
- Destroy unneeded classified materials.
- Switch off, disconnect, or lock PCs when not in use.

Confidentiality Agreement. This safeguard is intended to prevent unauthorized disclosure of classified information by employees, consultants, contractors, and other outside parties that have business ties to the organization. Confidentiality agreements can be crafted to apply to

sensitive information generally or to certain forms of information specifically.

Non-Competition Agreement. A non-competition agreement grants protection to an employer from the unauthorized use of the employer's intellectual property by a current or former employee. It typically incorporates one or more of three basic conditions:

- Restrictions on competition by departing employees
- Definitions of what constitutes property that the employer can legally protect from use by others
- Requirements that employees are obligated to cooperate with the employer in efforts to protect its intellectual property

Proprietary Information

Proprietary information is information owned by a company or entrusted to it that has not been disclosed publicly and has value. Information is considered proprietary when:

- It is not readily accessible to others.
- It was created by the owner through the expenditure of considerable resources.
- The owner actively protects the information from disclosure.

Very critical forms of proprietary information are intellectual properties. Most countries recognize and grant varying degrees of protection to four intellectual property rights: patents, trademarks, copyrights, and trade secrets.

Patents. These are grants issued by a national government conferring the right to exclude others from making, using, or selling the invention within that country. Patents may be given for new products or processes. Violations of patent rights are known as infringement or piracy.

Trademarks. These are words, names, symbols, devices, or combinations thereof used by manufacturers or merchants to differentiate their goods and distinguish them from products that are manufactured or sold by others. Counterfeiting and infringement constitute violations of trademark rights.

Copyrights. These are protections given by a national government to creators of original literary, dramatic, musical, and certain other intellectual works. The owner of a copyright has the exclusive right to reproduce the copyrighted work, prepare derivative works based upon it, distribute copies, and perform or display it publicly. Copyright violations are also known as infringement and piracy.

Trade Secrets. These can be formulas, patterns, compilations, programs, devices, methods, techniques, and processes that derive economic value from not being generally known and not ascertainable except by illegal means. A trade secret violation in the vocabulary of the law is a misappropriation resulting from improper acquisition or disclosure. The key elements in a trade secret are the owner's maintenance of confidentiality, limited distribution, and the absence of a patent.

The Paris Convention is the primary treaty for the protection of trademarks, patents, trade names, utility models, and industrial designs. Established in 1883, the convention is the oldest of the international bodies concerned with the protection of intellectual properties. It is based on reciprocity, i.e., it grants the same protections to member states as those granted to its own nationals, and provides equal access for foreigners to local courts to pursue infringement remedies.

Data Protection

Data are a valuable corporate asset. Consider these examples:

- In the minerals extraction industry, finding ores depends on data. It is no exaggeration to say that before a single shovel is placed into the ground, hundreds of millions of dollars will have been spent collecting and interpreting seismic and other scientific data.
- Hotels routinely build patron-oriented information databases that enable them to provide personalized service.
- Retailers collect data to help their managers monitor the flow of products moving from manufacturing plants to warehouses, stores, and ultimately purchasers. The process makes sure that sellable items are on

the shelves in the right stores, at the right time, and in the right quantities.

- Transportation firms routinely track movement of packages, even to the extent of allowing customers to access the information.
- Manufacturers have refined data-dependent "just in time" techniques to ensure that source materials reach the beginning of the production line not a day sooner or later than required and that the final products leave the plant already sold.

Today's successful organizations are very competent at collecting and making good use of data. Only a few, however, are fully competent in protecting their data assets. These are growing in value and volume. In some circles information moves from owner to owner, not unlike the way money moves in financial markets. Three dynamics seem to be at play: knowledge has become an economic resource, information technology is expanding, and the number of people familiar with information technology is growing by leaps and bounds.

Knowledge is emerging as an economic resource. Production in the United States is moving away from a dependence on capital, natural resources, and blue-collar labor. One hundred years ago, the Nation's wealth derived from oil, coal, minerals, ores, and farmlands. Today's wealth derives from the creation and use of knowledge, and the raw materials that create knowledge are in the form of data.

A second dynamic is information technology. New computer hardware and software come on line every day in dazzling arrays. All functions and sub-functions of business are addressed in the information technology marketplace. The Internet, company intranets, and multi-company extranets open doors wide for the collection and dissemination of huge volumes of information. Critical data, such as client lists and strategic plans, are moved around the globe in the blink of an eye by e-mail, fax, and cellular phone.

A third dynamic is the increasing ability of the average employee to work competently and comfortably with data. Add to this a very large and rapidly growing new employee class called information workers. In some companies, the entire workforce consists of people who work only with data.

Data protection is a challenge not easily met. For example, how does an organization balance the need to use data and the need to protect it from harmful disclosure? The clash between use and protection is problematic. An operations manager will consider data an essential resource to be fully exploited, therefore requiring it to be accessible at all times. He/she will say, "If data can't be used, our bottom line suffers." The manager is right; the value of the data is directly related to its use.

The CSO may agree with the operations manager but feel compelled to point out: "If our data are damaged, lost or compromised, the company may fail." The CSO's concern appears valid in light of at least one study. An insurance company found that 40 percent of companies that experienced major data loss as the result of disaster (e.g., fire, flood, hurricane, and terrorist action) never resumed business operations and a third of the companies that initially recovered went out of business within two years.

The CSO can enhance data protection by following commonsense suggestions:

- Stay on top of the issue
- Keep pace with data-related technology, not necessarily at the detail level, but certainly at a level that permits a clear understanding of the risks
- Look for countermeasures that take advantage of new techniques and leading edge technology
- Maintain a frank and ongoing dialogue with data managers about risk avoidance, and don't be preachy or harp on a shortcoming unless you have a solution in mind
- Spread the word among supervisory employees that data protection is their responsibility

John J. Fay

PROPRIETARY INFORMATION: A PRIMER FOR PROTECTION

In 1780, a drunken pattern maker working for James Watt, the inventor of the steam engine, bragged at the local pub that circular motion could be obtained from a reciprocating engine. When challenged, the man chalked a rough sketch on the bar top. James Pickard, a button maker,

NON-DISCLOSURE AGREEMENT

Effective Date: _____

Participant: _____

In order to protect certain confidential information that may be disclosed by Discloser ("DISCLOSER") to the "Participant" above, they agree that:

1. The confidential information disclosed under this Agreement is described as: _____
   _____
   _____
2. The Participant shall use the confidential information received under this Agreement for the purpose of: _____
   _____
3. The Participant shall protect the disclosed confidential information by using the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, dissemination, or publication of the confidential information as the Participant uses to protect its own confidential information of a like nature.
4. The Participant shall have a duty to protect only that confidential information which is (a) disclosed by DISCLOSER in writing and marked as confidential at the time of disclosure, or which is (b) disclosed by DISCLOSER in any other manner and is identified as confidential at the time of the disclosure and is also summarized and designated as confidential in a written memorandum delivered to the Participant within 30 days of the disclosure.
5. This Agreement imposes no obligation upon the Participant with respect to confidential information that becomes a matter of public knowledge through no fault of the Participant.
6. The Participant does not acquire intellectual property rights under this Agreement except the limited right of use set out in paragraph 2 above.
7. DISCLOSER makes no representation or warranty that any product or business plans disclosed to the Participant will be marketed or carried out as disclosed, or at all. Any actions taken by the Participant in response to the disclosure of confidential information by DISCLOSER shall be solely at its risk.
8. The Participant acknowledges and agrees that the confidential information is provided on an AS IS basis.

   DISCLOSER MAKES NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE CONFIDENTIAL INFORMATION AND HEREBY EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL DISCLOSER BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH OR ARISING OUT OF THE PERFORMANCE OR USE OF ANY PORTION OF THE CONFIDENTIAL INFORMATION.
9. Upon DISCLOSER's written request, the Participant shall return to DISCLOSER or destroy all written material or electronic media and the Participant shall deliver to DISCLOSER a written statement signed by the Participant certifying same within 5 days.
10. The parties do not intend that any agency or partnership relationship be created between them by this Agreement.
11. All additions or modifications to this Agreement must be made in writing and must be signed by both parties.
12. This Agreement is made under and shall be construed according to the laws of the State of Massachusetts.

DISCLOSER

_____
Authorized Signature

_____
Name

_____
Title

PARTICIPANT

_____
Authorized Signature

_____
Name

_____
Title

_____
Address

Figure 14. This is an example of an agreement between a "discloser" (the owner of confidential information) and a "participant" (such as a partner, contractor, or vendor).

realized the possibilities and obtained a patent ahead of Watt. The case was eventually heard in the courts, and Pickard's claim was upheld, although there was no doubt that Watt was the inventor. This early example supports the security manager's often stated thesis that proprietary information is subject to compromise when protective measures are not in place or not being followed. The loss of proprietary information can have a direct relationship to the bottom line, and when loss is severe it can mean the difference between success or failure of the organization.

Legal scholars tell us that in order to recover damages resulting from the theft of proprietary information, it must be demonstrated that the owner:

- Clearly regarded and identified the information as proprietary in nature
- Had a clear policy that required employees to treat the stolen information as proprietary
- Actively took steps to protect the information

A first step, then, is to identify the genuinely critical information. Too often, the more sensitive critical information is ignored while costly measures are directed at protecting information that has little value. A rigorous approach is appropriate when determining what types of information are worth safeguarding.

A good way to start is to think what would happen if particular information was to fall into unfriendly hands. A number of possible scenarios can lead the thinking process to an identification of what should be protected, the adversaries, the probable nature of attempts by adversaries to acquire the information, the exposures of the information to the hypothesized attempts, and an estimate in dollars of the value of the information.

This thinking process asks probing questions that relate to criticality and vulnerability. What information, in what form, is critical to the company or to a key operation? How much of that information is vulnerable to exploitation? In what ways is the information vulnerable and to whom? What is the worth of the information, what are the replacement costs and the costs of lost business opportunity? How much is the company willing to spend to protect information?

The answers will not be arrived at easily. They will emerge only after key managers have been interviewed, pertinent business data have been collected and analyzed, and an estimate made of threats and threat capabilities.

Information Classifications

When the truly sensitive information has been differentiated from non-sensitive information, an understanding of it will be helped by defining it in one or a very few categories and assigning to each category a descriptive designator. The designators can be anything, except that companies involved in safeguarding government classified information are not authorized to utilize the government's designators, i.e., TOP SECRET, SECRET, and CONFIDENTIAL, or any combination thereof, e.g., "Company Confidential."

In setting up a classification scheme there will be a temptation to keep it simple, which is certainly sensible, but the aim for simplicity should not go so far as to dictate that every form of sensitive information will be placed in a single classification. If one looks at the sum of all sensitive information residing in a business organization, at least two major groups stand out: that which deals with purely business matters and that which deals with matters relating to employees on a personal level. Thus, a two-level system would be a good choice, especially since it would be relatively easy to differentiate between business information and personal information.

If we look, however, at the business information category we may see that certain types of information (e.g., trade secrets) are clearly more important than others. The information that we perceive to have a lesser sensitivity may still be too sensitive to exclude from protection. Thus, a three-level system may be a better choice than the one- or two-level systems.

Systems that use a single classification level tend to be inflexible, and those that use more than two classification levels tend to be complex and difficult to manage. If there is a need for security protections that cannot be provided within the organization's existing system, the answer may be to use code names, such as Project X or Operation A, to denote the special protections that apply to those very limited groups of information applicable to the project or operation.

Designations and definitions for a three-level scheme might be as follows:

ABC SENSITIVE. Information that, if revealed in any manner to unauthorized persons, could unquestionably damage the operational, competitive, or financial position, or public image of the company or any other party to which the company owes a duty of protection. Examples include production figures, takeover or merger plans, litigation strategies, trade secrets and formulas, and marketing plans.

ABC RESTRICTED. Information that, if disclosed in an unauthorized manner, would be prejudicial to the interests of the company or which would cause embarrassment to or difficulty for the company. This category of information would include information of commercial value, or which is subject to legal or confidential agreement, or contains controversial or contentious views. Examples include financial statements, bid proposals, succession plans, and reports of investigation.

ABC PRIVATE. Information that is private to the individual and is only to be opened by the addressee. Examples include personal health reports, salary data, and performance ratings.

Proprietary Information Program

The authority for administering protection to information is derived from policy, that is, a statement of management. A policy will state the business necessity for information protection, the goals and objectives of the policy, the means for achieving the goals and objectives, and will identify the entities and positions affected by the policy. A policy is broad, provides direction, and sets a tone. A policy is carried out by directives, commonly referred to as procedures, that are much more specific and detailed. The activities generated by the policy and the procedures can be called a program; in this case, a proprietary information program. The major elements of the program could include the following:

Access. Decisions will need to be made as to the entitlements or privileges of access. Will access be limited to the need to know or will there be some flexibility in making proprietary information accessible for some other reason? Choices on access may not be controllable if the information falls within the purview of the National Industrial Security Program. In this case, that proprietary information to which some recipients do not have a need to know should be placed in an addendum that can be protected in the proprietary information program.

How will access rights be documented and how often will they be reviewed? Will job applicant and employee screening be a decision point in granting access? A consideration will be the reality that the likelihood of compromise increases as the number of persons having access increases. On the other hand, information is valuable to the organization to the extent it is used. A balance must be struck between the protection of information and the use of it.

Accountability. The program may impose accountability on persons and on supervisors of persons. Receipts, log books, a numbering system, and periodic inventories may be instituted for all or just the more sensitive categories. A missing item should automatically trigger an investigation, a report of investigative findings, and recommendations to prevent recurrence.

Classification and Declassification. Who will have classification authority? The choices can be the originator of the information, the head of the department in which the information originated, a manager one level above the originating department, a classification of information coordinator, a classification team representing a number of organizational interests, and so on. For reasons of stability and continuity, the classification authority should be vested in positions as opposed to persons because positions tend to be constant whereas persons are subject to attrition and turnover.

Other issues to be settled are whether or not classification authority can be delegated; and what criteria are to be used in determining if classification is warranted and, if so, determining the appropriate classification level. In this latter regard, strict rules should be in force to prevent non-sensitive information from being classified and sensitive information from being assigned inappropriately high classifications.

Declassification should be automatic when the information is no longer sensitive. The same

mechanisms in place to apply classifications would be correct for removing them. Periodic review of classified holdings can help in purging materials that should no longer be subject to special handling and control. A related consideration is downgrading and upgrading of classifications. The management may find it helpful to lower or raise classifications relative to changes in sensitivity.

Communications and Transmissions. The unnecessary distribution of proprietary information outside the circle of those members of staff directly concerned with it wastes time and effort, and leads inevitably to compromise and possible damage to the organization's interests. For this reason, the distribution of proprietary information must be kept as low as possible. This can be helped by circulating one copy among the essential addressees, using the established transmission controls (e.g., receipting, numbering, marking, sealing, double-enveloping, and encrypting) suitable to the classification, rather than by distributing to each addressee a separate copy.

Detailed instructions should be prepared and followed with respect to the distribution of proprietary information via mail channels within the organization, postal and non-postal channels outside of the organization, electronic mail, telex, facsimile, and computer systems that communicate with one another.

Computer Systems. Organizations are increasingly dependent upon computer systems, and the data these systems store, process, and transmit can be of vital importance. The policy and practices for protecting proprietary information will need to reflect the differences in computer systems, which can range from small and simple desktop devices to large and complex mainframe equipment.

Protection is more than just physically safeguarding the hardware, software, and data storage media; it involves backup and recovery, and passwords for accessing files and moving through protected computer gateways and networks.

The manner of protecting computer-related proprietary information can also be influenced by data protection legislation. Obtaining protection under a law designed to protect owner rights might require the owner to register or to meet standards concerning computer access, data retrieval, and storage. This can vary between jurisdictions, therefore a review by the company's legal function would be in order.

Destruction. The general rule is to destroy classified documents by burning, shredding, or pulping when no longer required. Printing ribbons, cassette tapes, microfiche, microfilm, and the like should be destroyed as efficiently as documents. With proper equipment, destruction can be done entirely in-house, it can be contracted to an outside vendor (whose integrity should be verified), or by a combination of both approaches. Generally speaking, the more sensitive categories are destroyed in-house while less sensitive proprietary information is destroyed by vendors (if volume is an issue).

Education and Awareness. The proprietary information policy must be clear and unambiguous. It must be thoroughly announced when initiated and be continuously reinforced thereafter. The methods for developing awareness can include orientations at time of hire, formal initial training, refresher training, newsletters, posters, and verbal reminders by supervisors at meetings and in discussions with subordinates.

Enforcement. The protection of the proprietary information program will be crippled when it does not have a means for enforcing policy and taking action against violators. Those persons given enforcement responsibilities must accept them, must be able to spot violations, must be able to intervene to correct the violations, and must be able to document the violations and refer them to management for the appropriate disciplinary action. Disciplinary actions should correspond to the severity of the violation.

Legal Review. The policy and implementing procedures should be reviewed initially and periodically by legal counsel to ensure that the program protects ownership rights to proprietary information and that liabilities to the organization are not created by the manner of administering the program.

Management Support. The program can be only as good as the support it receives from management. Support is evidenced when management treats proprietary information according to the rules followed by other employees,

affirms enforcement and disciplinary actions, and speaks in support of information protection. For the program to succeed, enforcement must be effective; and for enforcement to be effective, management must be entirely supportive.

Marking. The practice of marking can include applying to the sensitive material a stamp or legend that identifies the classification, a number or code, or other distinctive mark; placing a classified document into a specially marked folder or covering the front page of the document with a specially marked cover sheet; and numbering the pages of the document. Related to marking is the preparation of classified documents for transmittal by using a return receipt method, inserting inner envelopes within outer envelopes, and sealing envelopes and packages with tamper-resistant and tamper-revealing tape.

A stamp or legend should be applied regardless of format, i.e., documents, drawings, transparencies, film, or tape. It should be carefully constructed as to form and legal content to ensure no misunderstanding about ownership.

Non-Disclosure Agreements. Employees, contractors, and others who will have access to proprietary information in the normal course of their employment should be required at time of hire (and periodically thereafter) to sign an agreement pledging them to not violate the organization's rules regarding proprietary information. The agreement may relate to protection of such information generally and/or it may relate to a particular kind of information, such as work on a research project.

When a signatory to an agreement leaves employment, a debriefing is made to remind the individual of non-disclosure obligations that may continue. It is helpful at the debriefing to obtain a signed acknowledgment of the continuing obligations. Implied in this step is the prospect of legal action for a failure to comply.

Policy and Procedures Review. A review of the policy and its associated procedures should be made at regular intervals to bring them in line with changes that may have occurred since the policy and procedures were first written or last reviewed. Changes can be forced upon the program by external forces, such as the enactment of a law, or by internal forces, such as a major shift in the management's philosophy.

Releases of Information. The disclosure of proprietary information through the press, radio, television, publications, teaching, public speaking, and the like may be permitted by policy providing, of course, that permission is obtained in advance.

Requests for releases of information should be channeled to a knowledgeable person or designated office so that a review can be made of the information to be released. The information is likely to be in the form of financial and operating reports, technical papers, and promotional materials for use at trade shows and seminars.

Reproduction. Unsupervised copying machines present an opportunity for the unauthorized reproduction of proprietary information. Reasonable steps should be taken to guard against improper use of copying equipment. When proprietary information is being copied according to the existing rules, a responsible member of the department charged with protection of the information should oversee the copying operation to ensure that no extra copies have been left on the machine or in trash bins nearby. Other questions come into play: Should subcontractors be hired to reproduce proprietary information? Who can approve reproduction? Should in-house copying be done in one or a few designated areas?

Storage. Generally speaking, proprietary information not in use is stored in containers that correspond to their classification levels as established in the company's proprietary information policy. For example, materials with the highest classification might be stored in a steel safe fitted with a combination lock, materials in the second highest classification stored in a metal filing cabinet fitted with a locking bar, and materials in the lowest classification stored in a locked desk or credenza. The composition and construction of storage containers can be adjusted in relation to whether the facility is protected around the clock by roving security officers or whether the facility is equipped with an intrusion-detection system.

For large volumes of proprietary information, such as might be the case in an organization involved in research, a central library may be appropriate. The library holdings might be recorded on computers, and check out of

files by authorized users might be managed by a computer-assisted technique, such as bar coding.

Lonnie R. Buckels and
Robert B. Iannone

(Note: Since co-authoring this article, Lonnie Buckels passed away.)

TECHNICAL SURVEILLANCE COUNTERMEASURES INSPECTIONS

Intense competition and rapidly evolving markets are just a few of the external forces that are changing the ways we do business. Upper managers are pushing decision situations down the corporate ladder to operational managers, the operational managers are spread across large expanses of geography, and the decisions they make are based on great amounts of detail pulled from many centers of expertise. Businesses are working hard to generate meaningful information, to open the information to greater numbers of key players, and to maintain a working dialogue with affected groups in widely separated places.

Business information, including the most sensitive possessed by an organization, is valuable to the extent it is put to work. Although a security manager would like sensitive information to be constantly kept under lock and key, the reality is that information exists to be used. Further, in a fast-track environment many types of information will have a relatively short life span, meaning that it must be put to advantage fairly quickly in order to wring value from it.

The security dilemma is that when information is in the process of being used, with attendant value flowing from such use, it is most vulnerable to compromise. The attendant loss flowing from compromise can be many hundreds of times greater than the utilitarian value attached to the moment of use. This is the problem and the challenge to the security manager.

When is sensitive information at greatest risk? Experience tells us that those who are determined to acquire someone else's secrets will focus on two opportunities: when secrets are brought into the open for discussion, such as at a conference, and when they are transmitted from one place to another, such as messages across an electronic network. In short, sensitive information is at risk when it is being communicated.

The risk is considerably heightened when the business sphere is global. The dollar stakes are higher and political aims are often intertwined. We see, for example, the extraordinary ambitions of Eastern Bloc countries and former Soviet republics to establish business ties with the non-Communist world. The newcomers to Western-style democracy are discovering that capitalism is fueled by technology and until they develop a technological base and become producers and suppliers instead of consumers, they will be junior partners in the economic alliances they wish to forge.

A picture can be drawn that the American business sector, situated as a major repository of technology, is a natural target for those who desperately need technology to become competitive but lack the time and the resources to develop it on their own. An era of industrial espionage on a global scale is being ushered in, and the United States is among the few who have the greatest to lose.

The communications networks that support international commerce are notoriously vulnerable to surreptitious attack, and although efforts have been undertaken by governments to establish some modicum of secure transmissions, the principal protection must come from the network users. Self-protection has even more validity with respect to sensitive information disclosed at conferences and meetings. The owner of the information is the exclusive protector.

This section discusses a form of self-protection called the TSCM inspection, that is, making an organized search for technical surveillance devices. The places of search are typically at corporate offices and off-site meeting places. They include at the corporate offices the chief executive officer's suite, executive conference and dining rooms, the telecommunications center, and the telephone switching room, and off site the search activity might be of the facilities at a resort hotel where a senior management meeting has been scheduled. Findings from the inspection become the basis for taking steps to counter actual or potential surveillance attempts.

A handful of major corporations retain on staff one or a few technicians whose primary duties involve making TSCM inspections. The technicians are usually highly trained and are supplied with an array of electronic sensing equipment. Most companies, however, choose

to obtain the inspection service from a TSCM provider. The guidance here is applicable to either situation, although written for the security manager who engages a provider.

The first contact made by the security manager to the TSCM provider should be via a communications medium separate from the site that is to be inspected. The idea is to not disclose to those targeting you that you are about to inspect the phone line or area that has been compromised.

The TSCM provider will want certain details in advance of the inspection. For example:

- The number of phones, identity of manufacturer, and model numbers
- The number and size of rooms
- The location of rooms relative to each other
- The number of floors and buildings involved
- The type of ceiling, for example, fixed or moveable
- The types of audiovisual and communications devices, computers, and other special electronic equipment on site
- The forms of electronic communications and networks in use at the place to be inspected, including local area networks, microwave links, and satellite teleconferencing facilities

The security manager should expect the TSCM provider to supply all equipment required to carry out a comprehensive inspection. The equipment used should be the products of manufacturers that are recognized by TSCM professionals. The following described pieces of equipment should be expected of any TSCM provider selected for consideration:

- Time domain reflectometer capable of evaluating telephone systems cables, terminals and equipment utilized by the telecommunications system to be examined
- Tuneable receiver or spectrum analyzer with sufficient sensitivity to be capable of detecting extremely low powered devices and continuous coverage from 10 kilohertz to 21 gigahertz and a capability to analyze power lines, and provide a panoramic visual display of any video signal present, with a capability to extend frequency coverage as may be required by circumstances. Older equipment with frequency coverage that does not extend coverage to 5 gigahertz and above is obsolete to address current and evolving threats.
- Non-linear junction detector for detecting hidden tape recorders, non-operating transmitters, and remotely controlled transmitters. This instrument can also aid in detecting devices that use transmission techniques that go beyond the frequency range of countermeasures receivers.

Thermal imaging equipment for thermal signature spectrum analysis is used for locating operating video and audio transmitters though ceiling tiles and sheet rock walls by detecting their thermal (heat) signature. Additionally this methodology can help detect differences in ceiling and wall construction with the potential to indicate current or previous placement of pin-hole cameras, microphones, etc. Thermal imaging equipment can also help evaluate AV systems components to insure system components are not powered up when the system is deactivated. Thermal imaging equipment utilized must have sufficient sensitivity to resolve thermal signatures of eavesdropping devices through standard sheet rock walls.

TSCM technicians must be thoroughly grounded in countermeasures work, be current in their knowledge of state-of-the-art equipment, and be schooled and experienced in telephone systems to be examined. All detected signals must be identified as either legitimate or suspect. The source of a legitimate signal might, for example, be an FM broadcast station. A suspect signal would be one that is found to emanate from the area being inspected and cannot be attributed to a legitimate source.

Electronic emissions from computers, communications equipment, and teleconferencing facilities should be evaluated to determine their vulnerability to interception. The TSCM provider must be sufficiently competent to both detect readable emissions and formulate sensible, cost-effective recommendations to prevent exposure of sensitive data to unauthorized parties.

Telephones and telephone lines within the area under inspection should be examined with a time domain reflectometer, a TSCM audio-amplifier, and other specialized analyzers as required. These instruments check for com-

promises to telephone cables and terminals as well as devices that allow listening of conversations over the telephone and within the office or area nearby, even when the phone is not in use. Telephone satellite terminals and frame rooms, as well as station and distribution cables in the areas of concern should be inspected. Telephone systems should be evaluated for potential programming problems.

A thorough physical search should be made, with particular attention to areas adjoining rooms where sensitive communications occur. The walls between the rooms require careful inspection, and exiting wires need to be examined, including in some cases, electrical testing of wires for audio signals. Ceilings, radiators, ducts, electrical outlets and switches, picture frames, furniture, lamp fixtures, and plants all deserve the TSCM technician's attention.

All walls, ceilings, and furniture need to be evaluated with thermal imaging equipment to detect heat signatures from operating eavesdropping devices as well as differences in wall or ceiling density that may indicate current or previous pinhole camera, microphone or other device placement. All AV equipment needs to be evaluated to insure that powered down systems do not have components that have been compromised to remain on picking up room conversations that may be routed out of the area of concern.

Selected objects, such as desks, tables, chairs, and sofas, can be examined with a non-linear junction detector. This instrument uses a low-power microwave beam to detect energy reflected from electronic components such as diodes, transistors, and integrated circuits. These components are integral to radio transmitters, tape recorders, and other eavesdropping devices. Also, microwave transmitters, remotely activated transmitters, and transmitters that operate on infrared and ultrasonic principles can be spotted with a non-linear junction detector.

At the conclusion of the inspection, the TSCM provider should meet with the security manager to verbally discuss the work performed, the findings, and the recommendations. A fully detailed written report should be submitted within 10 days.

Safeguarding proprietary information is a concern for all companies of substance. TSCM inspections can be a security manager's tool for reducing the organization's exposure to loss or compromise of valuable information as well as providing assurance to management, customers, partners, and regulators concerning their information protection efforts.

Richard J. Heffernan

WEBSITE BLOCKING SOFTWARE

There are several good reasons to block certain types of websites. Pornography websites, for example, are notorious for planting web bugs on the computers of people that visit sites. Other types of sites have been blamed for spreading worms and viruses including many websites in Russia and China. Other websites have been known to collect information about visitors by placing spyware on their computers and then selling that information to marketing companies.

Many organizations have had problems with employees visiting pornographic websites during working hours. There have been situations where this behavior has resulted in sexual harassment lawsuits being filed by female employees.

Although there are many good reasons to use website blockers there can also be unintended consequences for using blocking software. One of the more famous incidents involved blocking websites that had the word breast on any of the pages. This resulted in dozens of websites offering information about breast cancer being blocked.

The technology that supports the popular website blockers and Internet filters that parents use to keep their kids from visiting inappropriate websites, such as those offering pornographic images, has found its way into many organizations. Website blocking software is relatively inexpensive and can be installed on a computer for as little as $30 per year. Bear in mind, however, that installation and maintenance does require staff time which can drive up the per computer costs rather dramatically.

Website blockers allow system administrators to block websites in a number of ways including:

- Setting blocking preferences on specific categories.
- Blocking websites by creating a list of allowed or blocked sites.
- Checking for offensive text based words and phrases.

The Internet usage patterns of employees can be tracked and recorded in an event log that keeps a list of websites that each user visited or attempted to visit. This information can be reviewed by supervisors or IT staff. Website blocking software packages offer several features that make administration easier and less time consuming including:

- Filters and lists can be updated automatically on a subscription basis.
- Supervisors or other designated personnel can be authorized to override blocked websites.
- Administration functions and responsibilities can be delegated and assigned.
- Many products have an easy to use web-based interface.
- Administrators can create custom categories of websites to be blocked.
- Filters can be set for specific users or groups just like file access is set.
- Filters can be set to be turned off or on based on a schedule for times of the day or days of the week.
- Blocking functions can be set to a monitor only mode and provide a warning to users about the appropriateness of the website they are visiting.
- Some products support several languages including English, French, Italian, Spanish, Danish, Swedish, German, Dutch, Portuguese, and Japanese.

Website blockers and content filters generally provide administrators with a wide variety of reports to analyze web surfing activities and e-mail usage. Reports can be provided in a format that can be viewed on a computer screen or printed. Administrators can use pre-configured reports or customize their own reports. Some products allow reports to be produced on-demand or administrators can be scheduled to run during off-peak hours and then can be e-mailed to designated recipients in various file formats. The content of reports can include the following items:

- AOL Chat Rooms and IRC chat usage
- AOL Instant Messenger, MSN Instant Messenger, Yahoo Messenger usage
- Attachments that are viewed or opened
- Bandwidth consumption by user or time-of-day
- Blocked activities by category or with extensive detail
- Blocked connections
- Filtering categories by user or time-of-day
- Filtering modes by user or time-of-day
- FTP requests and session details
- Hotmail, Yahoo email, AOL Internet e-mail, NetZero web-based e-mail, ATT Worldnet web based e-mail, and Netscape web based e-mail usage
- Kazaa & Kazaa Lite, Gnucleus, Limewire, and other peer to peer system usage
- Microsoft Exchange usage
- Most active users
- Most popular file types, FTP sites, newsgroups, and secure websites
- Newsgroups participation
- Reports for usage by individuals, departments, or other groups
- SMTP/POP3 e-mail usage
- Specific URLs visited
- The name of all files downloaded using peer to peer systems
- The text of all searches conducted within peer to peer systems
- The total number of visits to specific websites
- Top 10 blocked users
- Top sites requested by user or time-of-day
- Visits to secure websites

Michael Erbschloe

Source Erbschloe, M. 2004. *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code*. Boston: Butterworth-Heinemann.

IV: Investigation

ARSON

In most types of crime, an investigation will follow the known fact that a crime was committed. Arson is an exception. An investigation must take place before it is even known that arson occurred.

Arson Motives

Willful and malicious intent is an essential element in proving the offense of arson. The establishment of a motive adds weight to evidence tending to prove intent. Common motives are fraud, crime concealment, revenge, jealousy, spite, sabotage, intimidation, suicide, excitement, and pyromania.

Proving the element of intent in a building fire can be advanced when the following questions are answered through the inquiries of the investigator:

- Were alarms or communications systems tampered with?
- Was property removed prior to the fire?
- Were interior and exterior doors and windows open or closed?
- Was the ventilating system tampered with?
- Was the fire department called immediately?
- Were flammable materials in the building?
- Was internal fire fighting equipment in working condition?
- Was there any evidence of tampering?

In respect to proving intent regarding an automobile fire, the investigator needs to address these questions:

- Were payments being made regularly?
- Was the lien holder or finance company about to repossess the vehicle?
- Was the vehicle the subject of a domestic problem, such as divorce?
- Was the owner dissatisfied with the vehicle?
- Were accessories removed from the vehicle prior to the fire?
- Did the owner or prior owner have an insurable interest?

Accelerant Indicators

The detection, recovery, and analysis of fire accelerants are of major concern to the arson investigator. The areas most likely to contain residue of liquid fire accelerants are floors, carpets, and soil, since, like all liquids, they run to the lowest level. In addition, these areas are likely to have the lowest temperatures during the fire and may have had insufficient oxygen to support the complete combustion of the accelerant. Porous or cracked floors may allow accelerants to seep through to the underlying earth. Other places where accelerants may be discovered are on the clothes and shoes of the suspect.

Because scientific laboratory equipment cannot always be brought to the scene of a suspected arson, the investigator must rely upon a personal ability to detect the possible presence of accelerants through smell and sight. The sensitivity of the human nose to gasoline vapor appears to be on the order of 1 part per 10 million. As such, the nose is as sensitive as any of the currently available vapor detection equipment. Experienced arson investigators will agree that their noses are as sensitive to gasoline as the equipment available to them. However, not all flammable liquids are gasoline. A factor called olfactory fatigue and the possibility of an arsonist using a strong smelling substance to mask the presence of an accelerant are further reasons why a determination of arson should not rest solely upon detection by smell.

In addition to the sensitivity of the human nose, there are certain visual indicators of arson. These indicators reflect the effects on materials of heating or partial burning, which are used to indicate various aspects of a fire such as rate of development, temperature, duration, time of occurrence, presence of flammable liquids, and points of origin. The interpretation of burn indicators is a principal means of determining the causes of fires. Interpretation of burn patterns is a most common method of establishing arson.

Alligator Effect. This is the checkering of charred wood, giving it the appearance of alligator skin. Large, rolling blisters indicate rapid, intense heat, while small, flat alligator marks indicate long, low heat.

Crazing of Glass. This indicator is seen in the formation of irregular cracks in glass due to rapid, intense heat. Crazing suggests a possible fire accelerant.

Depth of Char. The depth of burning wood is used to determine length of burn and thereby locate the point of origin of the fire.

Line of Demarcation. This is the boundary between charred and non-charred material. On floors or rugs, a puddle-shaped line of demarcation is believed to indicate a liquid fire accelerant. In the cross section of wood, a sharp, distinct line of demarcation indicates a rapid, intense fire.

Sagged Furniture Springs. Because of the heat required for furniture springs to collapse from their own weight and because of the insulating effect of the upholstery, sagged springs are believed possible only in either a fire originating inside the cushions or an external fire intensified by a fire accelerant.

Spalling. This is the breaking off of pieces of the surface of concrete, cement, or brick due to intense heat. Brown stains around the spall indicate the use of a fire accelerant.

A tool for helping the arson investigator cover all bases is a comprehensive checklist.

Arson Checklist

Information that can be used to establish the fact that a fire occurred:

- Date and time of the burning
- Address or location where burning occurred
- Description of the building structure or premises, including the kind of construction material; the age or approximate age; the dimensions or approximate dimensions
- Fire station that received the alarm
- Time that the fire station received the alarm
- Fire apparatus, if any, that attended the fire, and the time that the fire apparatus was officially in operation
- Time that the fire apparatus was withdrawn from the burning, or the time that the fire department declared the burning extinguished
- Official designation of the incident by fire department records

Information that establishes a loss and ownership:

- Value of the property
- Insurance coverage on the property, or of items and articles of particular value; data as to mortgages, liens, loans, and the financial status of the suspect; and any action, pending or past, against the suspect or against any member of the suspect's family
- Inventory of stock, fixtures, equipment, and other items of value within the premises, and the damage as a result of the fire
- Name of the occupant at the time of the fire; and if the dwelling was vacant, the length of time that the premises had remained unoccupied
- Alterations or changes made in the building while it was occupied by the last tenant, such as the addition of partitions, electric wiring, or stoves
- Evidence that any articles were removed from the premises or were recently repaired, altered, or adjusted in any way
- Evidence indicating who was responsible for the security of the building: who possessed the keys to the building, and who could have had additional keys made
- Information as to whether windows or doors were normally closed and locked; whether some windows were, of necessity, left unlocked although they were closed; or whether some, or all, of the windows were normally left open
- Name of the owner of the property
- Name of the insured

Information and evidence that can be used to establish that arson occurred:

- Name of the person who discovered the fire and the person's observations concerning the location(s) in the building where burning or smoke were observed
- Time that the fire was discovered
- Circumstances under which the fire was first discovered

- Name of the person who turned in the alarm
- Means by which the fire was reported
- Time interval between the discovery of the fire and the report to the fire department
- Weather data, such as the atmospheric temperature and the direction of the wind at the time of the burning, and information concerning any electrical storms that may have occurred at that time
- How the burning occurred, if known
- Type of burning, e.g., flash fire, explosion, smoldering fire, or rapidly spreading fire; the approximate intensity of the burning; and whether there were separate fires
- Presence, color, and odor of smoke during the fire
- Color, height, and intensity of the flames
- Direction of the air currents within the building during the burning, as deduced from partially burned wallpaper, depth of charring, or soot deposits
- Quantity of air within the building during the fire, as revealed by the heaviest concentrations of smoke and soot
- Direction in which the burning spread
- Significant noises that were noticed before or during the burning
- Name of the person who was in the building at the time of the burning or who was in the building last
- Area that suffered the greatest damage
- Physical evidence discovered
- Evidence of possible devices or means by which the burning was started, e.g., candle, match, timing device, or flammable material (mechanical, electrical, chemical, or combination of the three)
- Blistered paint, charred wood, melted metal, glass, or other material that may be found at the suspected or known point of origin
- Presence among the debris of peculiarly colored ashes and clinkers, or traces of paraffin, saturated rags, waste, excelsior, or other fire spreaders
- Identification of the material burned, e.g., oils or chemicals. (Laboratory examination of samples of soot may supply this information.)
- If a death occurred, all pertinent data and facts revealed by the autopsy
- Photographs or sketches of the scene, interior and exterior, taken during the burning and after the burning was extinguished, supplemented with notes and evidence
- Photographs and impressions of evidence of forced entry at any of the doors, windows, hatches, skylights, or other points of entry
- Condition and location of fire-fighting equipment, such as hoses, extinguishers (full or empty), damaged alarm mechanisms, and sprinkler systems
- Information from inspections of the premises that may have been made prior to the fire. (Such data may be obtained from city or local fire departments, insurance carriers, city or local construction permits and accompanying inspections, and from insurance underwriting groups.)
- Evidence of the careless storing or placing of flammable materials such as gasoline, paint, oils, chemicals, lighter fluid, and cleaning fluid
- Location and condition of all electric lights, drops, extensions, appliances, and fuses
- Condition of electric wiring, including exposed wiring; evidence of recent repairs, inside and outside; evidence of splices, connections or alterations, and when, if known, such alterations were made and by whom; load carried by the wires; prescribed load of the fuses through which the lines were fed; and testimony as to whether or not heat was ever noticed in the wires or terminals before the fire
- Number and type of machines, if any, in the room or building; when they were last used; the amount of power they consumed; and when they were last tested and serviced
- Number of electric motors in the room or building; how they were safeguarded against dust, debris, and tampering; their horsepower, voltage, and purpose; whether they were of the "open" or "sealed" type; the length of time they were generally in operation, and their defects, if any
- Condition of gas pipes, bottled gas pipes, steam pipes, air pipes, and water pipes
- Number and type of stoves within the room or building; whether fires were in the stoves; the kinds of fuel used; the locations of the sources of fuel in relation to the stoves;

whether the stoves were self-insulated; when the ashes were last removed; where removed ashes were placed; when the stoves were last cleaned or serviced; and whether they had pilot lights or similar continually burning flame
- Glass objects that may have accidentally caused the fire by concentrating the rays of the sun
- Facts pertaining to any suspicious items or devices that may have been found among the debris
- Methods used to extinguish the burning, e.g., water, foam, and carbon dioxide

Conclusion

Unfortunately, arson investigations are sometimes inadequate or not performed at all. This is often due to a shortage of arson-trained investigators generally. Even when a skilled investigator is on the case, evidence of the crime is likely to have been destroyed by the fire or by the suppression of the fire. As a result, many fires are declared to have innocent origins when in fact they were deliberately set.

John J. Fay

BEHAVIOR ANALYSIS INTERVIEW

Every investigator evaluates the behavior displayed by the person being interviewed (whether a victim, witness, or suspect) and draws some conclusion as to that person's truthfulness. This article profiles the behavioral characteristics indicative of a person who is telling the truth, as well as those characteristics that are suggestive of a person who is withholding information. Before describing the typical behaviors exhibited by truthful and deceptive subjects, some cautions must be emphasized. There is no single verbal or nonverbal behavior that automatically means that a person is lying or telling the truth. Each behavior displayed must be considered in the context of the environment and in comparison to the subject's normal behavior patterns.

The evaluation of behavior symptoms should take into consideration the subject's intelligence, emotional and psychological health, sense of social responsibility, and degree of maturity. Judgment as to a subject's truthfulness or deception should be based on the overall behavioral pattern displayed, and not upon any single observation or activity.

Nonverbal and Verbal Behavior

With these cautions in mind, the nonverbal and verbal behavior of a person during questioning may provide very valuable and accurate indications of truthfulness or deception.

Attitude. Truthful individuals usually display an attitude that can be characterized as concerned, composed, cooperative, direct, spontaneous, open, and sincere. On the other hand, a person who is lying may appear to be overly anxious, defensive, evasive, complaining, guarded, or, in some cases, unconcerned.

Posture. In a non-supportive environment, one in which the investigator and subject are sitting in chairs facing each other about 4½ to 5 feet apart, without any desk or barrier between them, the truthful subject is likely to sit upright (but not rigid or immobile) and frontally aligned with the investigator. The truthful subject will oftentimes lean forward as a sign of interest and participation, and when the subject changes posture the movement is usually casual and relaxed. By contrast, the deceptive subject may maintain a very rigid and immobile posture throughout the interview. There may be a lack of frontal alignment, slouching in the chair, and a closed, barriered posture with arms folded across the chest and legs crossed. In som e cases, the deceptive subject may exhibit very rapid and erratic posture changes.

Significant posture changes are likely to occur when key questions are introduced and deceptive answers given. The deceptive subject's movements are attempts to relieve or reduce internal anxiety experienced when confronted with questions that pose a personal threat and when making untruthful responses that are potentially detectable as lies. The truthful person will not usually experience this same level of high anxiety and will therefore not exhibit these same pronounced posture changes.

Gestures. In addition to significant posture changes, deceptive suspects also engage in a variety of other tension-relieving activities that

include grooming gestures and supportive gestures. Examples of grooming gestures include stroking the back of the head, rearranging jewelry or clothing, dusting the pants or lint picking, and adjusting or cleaning glasses. Supportive gestures consist of placing a hand over the mouth or eyes when speaking, hiding the hands, and holding the forehead with a hand for an extended period of time. Deception may be indicated when a suspect repeatedly engages in any of these nonverbal activities while making verbal responses.

Eye Contact. Deceptive persons oftentimes do not look directly at the investigator when they answer critical questions—they look down, over to the side, or up at the ceiling. They feel less anxiety if their eyes are focused somewhere else than on the investigator. Truthful persons, on the other hand, are not defensive and can easily maintain eye contact with the investigator.

Verbal Indicators. Generally speaking, a truthful person will answer questions in a direct, spontaneous, and sincere manner. The truthful subject will use realistic words, such as steal, embezzle, and forge, while the deceptive person will use euphemisms such as take, misuse, and write. The truthful person will exhibit a reasonable memory, not qualify the answers, and volunteer helpful information. Conversely, the deceptive subject may delay a response or repeat the question before giving the answer. The deceptive suspect may also anticipate a question and offer an answer quickly, even before the question is completed. The deceptive person will oftentimes exhibit a remarkable memory (remembering too much or too little detail) and preface answers with such phrases as "To tell you the truth," or "As far as I can recall," or "To the best of my knowledge."

Behavior-Provoking Questions

The Behavior Analysis Interview (BAI) combines the use of traditional investigative questions as well as a series of behavior-provoking questions. The BAI was developed by John E. Reid and Associates, Inc., Chicago. Theoretical models were developed, statistically tested, and validated for the predicted differences in the responses given by truthful and deceptive subjects to the behavior-provoking questions. More than 30 behavior-provoking questions have been developed and utilized in the BAI technique.

First, let's differentiate between behavior-provoking questions and investigative questions that are routinely asked as part of the investigative process. These routine investigative questions are designed to elicit factual information with respect to the who, what, when, where, why, and how of the matter under investigation. The behavior-provoking questions are intended to ascertain the subject's perspective of the issue under investigation, as well as to identify areas of anxiety that will be manifested in visible and detectable signals.

As the suspect responds to each investigative question, the investigator should carefully record and evaluate the suspect's version of events. Simultaneously, the investigator will be looking for nonverbal and verbal signals (as outlined above) that accompany these questions to identify areas of anxiety and possible deception that will require further inquiry or investigation.

To illustrate the behavior-provoking questions, five of these questions are presented in a hypothetical investigation into the theft of credit cards from a bank's mail room.

1. The purpose question: "What is your understanding of the purpose for this interview?" The truthful responder will provide an accurate description of events; may use descriptive language such as steal; and may mention numbers of cards stolen and/or victims' names, if known. The deceptive subject's response may be vague and nonspecific. The response may include non-descriptive language, such as "the incident," or "something happened," or qualifiers, such as "apparently" or "evidently" or "may have." Details are absent concerning the number of cards stolen or victims' names.
2. The you question: "Over the past several weeks we have had a number of credit cards disappear from the bank; specifically, the mail room. If you had anything to do with stealing these missing credit cards, you should

tell me now." A truthful response is likely to be a direct, contracted, and unequivocal denial, e.g., "No, I didn't steal any credit cards." Broad, all encompassing language may be used: "Absolutely not! I haven't stolen anything from here." The deceptive response may be a non-contracted and unemotional denial ("I do not know anything about this") or an evasive response ("I didn't even know credit cards were missing") or an objection ("Why would I risk my job by doing something like that?").

3. The knowledge question: "Do you know for sure who did steal any of the missing credit cards?" A truthful subject will often volunteer information, "Not for sure, but I have some ideas." Concern or anger may come out, "I wish I did know, but I just don't have any idea." The deceptive subject may give an unemotional denial, "No, I do not." The subject does not offer spontaneous thoughts or feelings.
4. The suspicion question: "Who do you suspect may have stolen these missing credit cards?" The truthful subject will give the question careful thought, and when offering a suspicion, will cite a reason for the suspicion. A deceptive response is "I don't have any idea." without giving the question any careful thought. The deceptive person may name improbable suspects, such as employees without opportunity or access.
5. The vouch question: "Is there anyone who you work with that you feel is above suspicion and would not do anything like this?" The truthful subject will give the question thought and typically eliminate possible suspects. The deceptive subject will not vouch for others because in so doing the field of suspects is narrowed, which would have the effect of increasing the suspect's chance of exposure.

Joseph P. Buckley, III

Source Inbau, F., Reid, J., Buckley, J., and Jayne, B., ed. 2001. *Criminal Interrogation and Confessions, 4th Edition*. Gaithersburg: Aspen.

BURGLARY: ATTACKS ON LOCKS

A door lock is usually all that prevents movement into a protected area, whether commercial or residential. Occasionally, a door lock will be supplemented with a padlock. Most door locks are key-operated. They consist of a cylinder or other opening for inserting a key that mechanically moves a bolt or latch. The bolt (or deadbolt) extends from the door lock into a bolt receptacle in the door frame.

The cylinder part of a lock contains the keyway, pins, and other mechanisms. Some locks, called double-cylinder locks, have a cylinder on each side of the door and require a key for both sides. With a single-cylinder lock, a thief may be able to break glass in or nearby the door and reach inside to turn the knob to release the lock. The disadvantage is that a key to the lock on the inside of the door must be readily available for emergency escape, such as during a fire.

The key-in-knob lock works on the same principles as the cylinder lock except, as the name implies, the keyway is in the knob. In the single key-in-knob lock the keyway is almost always on the outside door knob and a push or turn button for locking/unlocking is on the inside knob. The double key-in-knob lock has a keyway on the outside and inside knobs, which increases security but also decreases safety.

From the standpoint of forced entry, the cylinder lock is somewhat resistive in that it cannot be ripped easily from the door because it is seated flush or close to the surface. One model of the cylinder lock features a smooth, narrow ring around the neck of the cylinder. The ring moves freely so that even if it can be grasped by a tool, it cannot be twisted. The cylinder lock is vulnerable to a burglary tool called the slam hammer or slam puller. The device usually consists of a slender rod with a heavy sliding sleeve. One end of the rod has a screw or claw for insertion into the keyway. The other end has a retaining knob. When the sleeve is jerked away from the lock, striking the retaining knob, the lock cylinder or keyway is forcibly pulled out.

By contrast, the key-in-knob lock is somewhat more vulnerable because the knob itself can be hammered off; pried off with a crowbar; or pulled out by a grasping tool, such as channel lock pliers. Once the inner workings of the lock are exposed, the burglar can retract the bolt to open the door.

Probably one of the simplest attack techniques is slip-knifing. A thin, flat, and flexible object, such as a credit card, is inserted between the strike and the latch bolt to depress the latch bolt and release it from the strike. Slip-knifing of sliding windows is accomplished by inserting a thin and stiff blade between the meeting rail (stile) to move the latch to the open position; slip-knifing of pivoting windows is done by inserting a thin and stiff wire through openings between the rail and the frame and manipulating the sash operator.

Springing the door is a technique in which a large screwdriver or crowbar is placed between the door and the door frame so that the bolt extending from the lock into the bolt receptacle is pried out, enabling the door to swing open. A 1-inch bolt will hinder this attack.

Jamb peeling is the prying off or peeling back the door frame at a point near the bolt receptacle. When enough of the jamb is removed from the receptacle, the receptacle can be broken apart or removed, allowing the door to swing open. A metal or reinforced door frame is the antidote.

Sawing the bolt is inserting a hacksaw blade between the door and the door frame and cutting through the bolt. The countermeasure is to use a bolt made of a saw-resistant alloy or a bolt that is seated in such a way that it will freely spin on its side, thereby taking away the resistance needed for the saw blade to gain purchase.

Spreading the frame involves the use of a jack, such as an automobile jack, in such a way that the door jambs on each side of the door are pressured apart to a point where the door will swing free from the bolt receptacle. A reinforced door frame and a long deadbolt are countermeasures.

Kicking in the door is a primitive, but effective technique. In this case, the attack is against the door so that even the best locking hardware will have little deterrent effect. The countermeasure is a metal door or a solid wood door, at least 1¾-inches thick, installed in a wooden door frame at least 2-inches thick, or a steel door frame. An escutcheon plate can be used to shield the bolt receptacle.

A more sophisticated attack technique is lock picking. It is seen infrequently because of the expertise required. Lock picking is accomplished by using metal picks to align the pins in the cylinder as a key would to release the lock. The greater the number of pins, the more difficult it is to align them. A cylinder should have at least six pins to be resistive to lock picking.

The high-security form of the combination lock requires manipulation of one or several numbered dials to gain access. Combination locks usually have three or four dials that must be aligned in the correct order for entrance. Because only a limited number of people will be informed of the combination, the problems associated with compromised mechanical keys and lock picking are removed. Combination locks are used at doors and on safes, bank vaults, and high-security filing cabinets; in most cases, the combination can be changed by the owner on an as-needed basis.

With older combination locks, skillful burglars may be able, often with the aid of a stethoscope, to discern the combination by listening to the locking mechanism while the dial is being turned. Another attack method is for the burglar to take a concealed position at a distance from the lock and with binoculars or a telescope observe the combination sequence when the lock is opened.

The combination padlock has mostly low-security applications. It has a numbered dial and may be supplemented with a keyway. On some models, a serial number impressed on the lock by the manufacturer will allow the combination to be determined by cross-checking against a reference manual provided by the manufacturer to dealers. Although a convenience, it is a risk to security.

In a technique called padlock substitution, the thief will remove the property owner's unlocked padlock and replace it with a similar padlock. After the property owner locks up and leaves, the thief will return, open the padlock and gain entry. The preventive measure is to keep padlocks locked even when not in use.

John J. Fay

Sources

Fennelly, L.J. 1982. *Handbook of Loss Prevention and Crime Prevention*. Boston: Butterworth-Heinemann.

Purpura, P.P. 1984. *Security and Loss Prevention*. Boston: Butterworth-Heinemann.

CRIME ANALYSIS

What cannot be measured cannot be managed. This is a commonly accepted business paradigm, yet its acceptance within the security industry is

not as far reaching as one would expect. Data-driven security is fast becoming an accepted business practice and refers to using measurable factors to drive a security program. While not all elements of a security program lend themselves to measurement, many components can be measured effectively. A key component of a data-driven security program is the quantitative threat assessment, or more specifically, a crime analysis. Crime analysis is key to successful operational management as it broadens management's vision and increases its effectiveness with a wealth of information.

Statistics are used in planning for the future. Crime and security statistics guide security surveys, help in the selection of countermeasures, measure program effectiveness, and alleviate the risks and costs relating to those risks. The use of information regarding crimes and other security incidents helps security decision makers plan, select, and implement appropriate security measures that address the actual risks of the facility. Security decision makers, after assessing the crime problem, can select the most effective countermeasures including the cost of implementation and maintenance.

Budget justification is also accomplished through the use of statistics since effective security measures will reduce the risks, and a return on investment can be calculated. Typically, internal security incident reports are used to determine security weaknesses and problem areas, as well as to select crime countermeasures, calibrate countermeasure effectiveness, and consider future budget needs. Crime statistics, available from local law enforcement agencies, are also utilized extensively in determining concrete security risks. Though internal security reports and police crime data may overlap, it is incumbent upon security decision makers to consider both in determining a facility's true risk.

Security decision makers need not be mathematicians to fully utilize statistical information; rather they need only a basic understanding of the various methods to use such data along with a touch of personal computer and spreadsheet software knowledge. A common application of statistics in the security arena is the use of security reports and crime data to determine the risks to a facility, including its assets and personnel.

The use of statistics extends beyond planning security at an existing facility. Statistical data may also be used to select and plan security at new facilities. For example, the real estate department of a company may provide the security decision maker with a list of potential new sites, one of which will be selected based on, among other things, the risks posed at the location. In this role, the security decision maker serves as an advisor to the real estate department by conducting crime analyses of the proposed sites as well as performing security surveys to select the location that poses the least or a tolerable level of risk. In this scenario, the security decision maker will gather and analyze crime data for similar businesses in the area surrounding each site to determine the security problems. The sites that have the least crimes can be evaluated further by means of a security survey. After the sites have been narrowed down by risk and surveys completed, the security decision maker has the necessary information to advise the real estate department.

Threat assessments are the backbone of security surveys and risk analysis and often define the scope of work to be performed in a security survey. Before conducting a security survey, security decision makers will have a thorough understanding of the crime and security-incident history of the facility. This information guides the security decision maker as he conducts the survey and looks for crime opportunities that can be blocked with security measures.

Crime analysis is the logical examination of crimes which have penetrated preventive measures, including the frequency of specific crimes, each incident's temporal details (time and day), and the risk posed to a property's inhabitants, as well as the application of revised security standards and preventive measures that, if adhered to and monitored, can be the panacea for a given crime dilemma.

While the above definition of crime analysis is holistic, it can be dissected into three basic elements:

- Logical examination of crimes which have penetrated preventive measures
- Frequency of specific crimes, each incident's temporal details (time and day), and the risk posed to a property's inhabitants
- Application of revised security standards and preventive measures

Examining crimes perpetrated at company facilities is commonplace in today's business

environment. In larger companies, there may be a person or group of people working under the risk management or security departments who are solely dedicated to the function of crime analysis. In smaller companies, the crime analysis function is carried out by someone who also has other security management duties. Crime analysis may also be an outsourced function, whereby company personnel simply utilize crime data that a contractor has collected, entered into a database, and possibly provided some analytical work up or the tools to do so.

The second element is the analytical component. Crimes are analyzed in different ways depending on what one is trying to accomplish. Most commonly, facilities are ranked based on the crime level or rate. Generally, facilities with more crime or a higher crime rate are given a larger piece of the security budget, while less crime-prone sites are given less money. Crimes are also analyzed on a facility-by-facility basis allowing security decision makers to select appropriate countermeasures.

Crime analysis is used to assess and select appropriate countermeasures. Crimes that are perpetrated on a property can usually be prevented using security devices or personnel; however, it should be noted that all measures are neither cost effective nor reasonable. Certainly, a criminal perpetrator would be hard pressed to steal an automobile from a small parking lot patrolled by 20 security officers, though that type of security extreme is not reasonable, nor inexpensive. Crime analysis guides security decision makers in the right direction by highlighting the types of crimes perpetrated (crime specific analysis), problem areas on the property (spatial analysis), and when they occur (temporal analysis) among others. Using this information, it is much easier to select countermeasures aimed directly at the problem.

Why would a security decision maker need to know how crime occurs? By understanding the factors that lead to crime, coupled with a comprehensive study of crime on the property, security personnel can be assisted in blocking opportunities for crime and creating effective crime prevention programs.

Crime analysis seeks to answer the questions: What? Where? When? Who? and How?

Answers to these questions help us better understand the particular nature of crime on a given property and formulate specific responses. The *What* question tells us what specifically occurred. For example, was the crime against a person or property, violent or not, completed or attempted? The *What* also distinguishes between types of crime that require different solutions such as whether a reported robbery was actually a burglary.

Where answers the location-specific question. Did the crime occur inside the walls of the location, in the parking lot, in the alley way behind the site? If the incident occurred inside, did it occur in a public area or a controlled area? Determining the precise location assists property managers in creating additional lines of defense around targeted assets. For example, if the crime analysis indicates that a vast majority of loss at a small grocery store is occurring at the point of sale, then little will be accomplished by installing a lock on the back office where the safe is located. In this example, the crime analysis will rule out certain measures, but by the same token, crime analysis will also spotlight certain solutions, such as increased employee training or updated accounting systems at the point of sale.

The answer to the *When* question gives us the temporal details of each incident. Knowing when crimes are most frequent helps in the deployment of resources, especially costly security measures such as personnel. Temporal details include the date, time of day, day of week, and season that a crime occurred.

Who answers several important questions that help a property manager create an effective crime prevention program. Who is the victim and who is the perpetrator? Knowledge of the types of criminals who operate on or near a given property assists property managers select the best measures to reduce crime opportunities. For example, gambling casinos have used closed circuit television (CCTV) for some time to track known gambling crooks. Also important are the potential victims of crime. Ted Bundy and Jeffrey Dahmer, like other more common criminals, select particular types of victims. Thus, an understanding of the people that may be targeted focuses a property manager's attention. For example, a residential apartment complex that caters to recently released hospital patients has larger responsibility to provide a safe environment given the fact that the clientele is not usually capable of self-protection. The oldest example of the *Who* question dates

back to premises liability law where innkeepers were often found to be responsible for the safety of a guest when crime was foreseeable. People on travel are usually not aware of the area in which they are staying and they also have little control over the security measures that they can take to protect themselves inside a hotel room.

How is the most consequential question to be answered by the crime analysis. How a crime is committed often directly answers the question, "How can the crime be prevented in the future?" More specific *How* questions may also be asked. How did the criminal access the property? If we know that a criminal has accessed the property via a hole in the back fence of the property, efforts can be taken to immediately repair the fence. Other specific questions reveal the method of operation (MO). How did a criminal enter the employee entrance of an electronics store to steal a television? How did a burglar open the safe without using force? How did the car thief leave the gated premises without knowing the exit code? Obviously, the list of examples is unlimited and property managers need to ask many questions about the criminal's actions as soon as possible to learn the most effective solutions. It is true that often the *How* will be the most difficult question to answer. This leads into a problematical area as crime sources can be divided into two categories, internal and external. Internal sources of crime can be employees and other legitimate users of the space such as tenants. They are called legitimate users of the space as they have a perfectly valid reason for attending the location, but in the course of their regular activities, they also carry out criminal activities.

With these answers, security decision makers are better armed to attack the crime problem. Some would argue that security is more of an art than a science. While they are correct, the business of security is not an art. The security department is a business unit, not unlike other business units within a company that must justify their existence. Crime analysis is a critical component for demonstrating a return on security investments.

In today's corporate environment, it is important for all departments to show bang for the buck, and this philosophy applies to the security organization all too much as often their budget is among the first to be cut. Showing a return on investment simply means that security measures are either paying for themselves, or better, adding to the bottom line. Return on investment is important as it helps the security decision maker justify costs and obtain future budget monies. Some security programs will not pay for themselves while others actually become a profit center. Regardless of a security measure's ability to be quantitatively assessed, security decision makers should strive to calculate a return on investment.

Karim H. Vellani

DNA ANALYSIS

DNA is the basic genetic material within each living cell that determines a person's individual characteristics. Since the early 1980s, DNA testing has been used in AIDS and genetic disease research, bone marrow transplants, and in anthropological investigations. In forensics, DNA testing is typically used to identify individuals, using only small samples of body fluids or tissue—such as blood, semen, or hair—left at a crime scene.

DNA Testing Methodologies

DNA testing includes two major components when used for forensic purposes. The first involves the molecular biological techniques that allow analysts to directly examine a DNA sample. The second component has to do with population genetics—how to interpret DNA tests to calculate the degree to which different samples are associated. Such population studies help to determine the results of the analytical work.

DNA tests investigate and analyze the structure and inheritance patterns of DNA. Many methodologies exist, and new ones are constantly being developed. The particular test used will depend on the quantity and quality of the sample, the objective of the test, and the preferences of the laboratory conducting the procedure. All tests, however, are designed to isolate certain nucleotide sequences—the polymorphic segments of the DNA molecule carrying marked, recurring distinctions—and these variable segments provide the basis for discriminating among individuals' DNA.

In a forensic environment, two common analytical methods used to detect the polymorphic DNA in human samples are the Restriction Fragment Length Polymorphism (RFLP) and Polymerase Chain Reaction (PCR) techniques. The RFLP method identifies fragments of the DNA chain that contain the polymorphic segments, produces a DNA "print" of the fragments, and measures the fragment lengths. The PCR-based methods seek to determine the presence of specific alleles (alternative forms of genes that occur in different individuals), thus indicating specific genetic characteristics.

Restriction Fragment Length Polymorphism. RFLP requires the presence of as little as 50 to 100 nanograms of DNA—an amount of DNA that may be present in a single hair follicle. The distinct stages in developing a DNA print using RFLP will be portrayed here by describing the analysis of a blood sample.

First, white cells containing the DNA are separated from the blood sample by use of a centrifuge, and the cells are ruptured to extract the DNA strands. The DNA strands are then cut, or digested, using restriction endonucleuses (REs)—enzymes derived from bacteria that catalyze the cutting process. A particular enzyme will cut the DNA strands at the same nucleotide sequence (restriction site) each time. By cutting a person's DNA in the same place, the several alternate forms (alleles) of a gene are separated from each other. A specific allele will be of the same size and molecular weight as others of its type. The polymorphism, or individuality, of a person will be detected on the basis of differences in DNA fragment lengths.

At this point in the process, all of the DNA fragments are mixed together. Using a technique called electrophoresis, the polymorphic fragments are separated by length. The DNA is placed at one end of a plate containing agarose gel, with a positive electrode placed at the other end. DNA carries a negative electrical charge; therefore the DNA will move toward the positive electrode. The distance that an individual fragment of DNA travels depends on the amount of its electrical charge, which is determined by its length and molecular weight. Thus, fragments of the same length and weight will travel the same distance while large DNA fragments will move more slowly than smaller fragments. This process sorts the DNA into bands based on length and weight and these length-dependent bands are the basis for DNA identification.

After electrophoresis, the next step calls for transferring the DNA fragments in the gel to a nylon membrane. In a technique called "Southern blotting," a chemical reagent (such as sodium hydroxide) acts as a transfer solution and a means to separate the double-strand fragments into single-strand fragments.

Using the zipper analogy, the strands are unzipped, exposing the building blocks. The unzipped DNA fragments are now fixed on the nylon membrane, where they are exposed to radioactive DNA probes—laboratory-developed (thus, known sequences), DNA nucleotide fragments which carry a radioactive "marker." The probes seek out the sequence that they match and attach themselves to the complementary split DNA strands.

The probes are made radioactive so that the DNA sequences to which they become attached can be visibly tracked. The nylon membrane is placed against a sheet of X-ray film and exposed for several days. When the film is developed, black bands will appear at the point where the radioactive DNA probes have combined with the sample DNA. The result, called an "autoradiograph" or "autorad" looks much like the bar codes found on items in supermarkets and department stores.

The final step is the band pattern comparison. Genetic differences between individuals will be identified by differences in the location and distribution of the band patterns, which correspond to the length of the DNA fragments present. The actual measurement of the band patterns being compared can be done manually or by machine, but often DNA identification depends upon expert judgment.

Polymerase Chain Reaction-Based Techniques. PCR is not only an analytical tool, but also an amplification technique often used when the available amount of DNA material is insufficient for proper analysis, or when the sample is degraded by chemical impurities or damaged by environmental conditions. PCR is an in vitro process that causes a specific sequence to repeatedly duplicate itself, mimicking its natural replication process. Short pieces of purified DNA, called primers, are used to build a foundation upon which the sample DNA can build. The primers must have sequences that complement

the DNA flanking the specific segment to be amplified. The sample DNA is heated to separate the double helix, producing two single strands. By then lowering the temperature, copies of the primers bind to the DNA sample's flanking sequences. A heat-stable DNA polymerase (an enzyme) is then introduced to the DNA sample causing the primers to synthesize complimentary strands of each of the single strands. This process is repeated for generally 25 cycles, amplifying the original DNA sequence approximately a million times. The amplified DNA can then be analyzed by any one of several methodologies.

Functions of DNA Testing

DNA testing provides a basis for positive identification, but it is not expected to become a suitable technology for validating identification in security settings. DNA analysis would be inappropriate in situations where a nearly immediate determination must be made as to whether a person seeking entry to a particular area, or seeking to conduct a particular transaction is, in fact, authorized to do so. The chemical analysis required to make a DNA comparison takes weeks, not minutes. DNA testing is increasingly used to determine paternity and, in forensic settings, it has been most prolifically and successfully used to identify or exonerate a suspect.

Paternity Determinations. In determining paternity, DNA has proven to be extraordinarily useful. Each chromosome contains nucleotides identical to those of each parent, as well as the nucleotides that distinguish the individuality of the person. If samples from the child and from one of the parents are available, the nucleotides of the child that are different from the known parent's DNA must have come from the unknown parent's DNA. If a sample from the suspected, but unknown, parent supplies all the "missing" nucleotides without any superfluous nucleotides, one can conclude that the suspected individual is, in fact, the other parent.

Identification of Suspects. The forensic promise of DNA typing is substantial. Samples of human skin, hair follicles, blood, semen, or saliva containing cells or other tissues found on a crime victim or at a crime scene can be examined to identify the DNA pattern. That pattern can be compared with DNA from a suspect to make a "positive identification," or to exonerate a suspect. DNA examination techniques sometimes permit the use of extraordinarily small samples of human tissues or fluids, such as a few hairs or a single spot of blood. Moreover, DNA is durable and is relatively resistant to adverse environmental conditions such as heat or moisture. DNA degrades slowly in a decomposing body, lasting sometimes for years and allowing samples to be analyzed for some time after the death of an individual. Although some experts debate the percentage of usable tissue and fluid samples that are retrieved from all crime scenes, DNA analysis will have the greatest effect on violent crime cases, such as murder and rape, where hair, blood, semen, or tissue evidence is frequently found.

Source "Forensic DNA Analysis." 1991. *Bureau of Justice Statistics, U.S. Department of Justice.*

EVIDENCE TYPES

Physical Evidence

Evidence is anything that tends to prove or disprove a fact. Within that general definition, physical evidence is any material substance or object, regardless of size or shape. Generally, there are three categories of physical evidence.

- Movable Evidence. Items that can be transported or moved, such as weapons, tools, and glass fragments.
- Fixed or Immovable Evidence. Items that cannot easily be removed, such as walls of a room, trees, and utility poles.
- Fragile Evidence. Items that are easily destroyed, contaminated, or will easily deteriorate.

Evaluating Physical Evidence. In many cases the success or failure of an investigation depends on the investigator's ability to recognize physical evidence and derive understanding from it. This process of evaluation begins with the initial report of a crime and concludes when the case is adjudicated. Evaluation is usually carried out in concert with laboratory technicians, a prosecuting

attorney, other investigators, experts in certain fields, and other persons whose knowledge contributes to a better understanding of physical evidence and its relationship to the many facets of the case.

Identification. Evidence must be marked for identification as soon as it is received, recovered, or discovered. Identification markings help the investigator identify the evidence at a later date. Markings are normally made by placing initials, time, and date on the items. If it is not practical to mark evidence, it is placed in an appropriate container and sealed. The container is then marked for identification.

Identification markings are supplemented by the use of an evidence tag. An evidence tag is filled out at the time the evidence is acquired. Entries on the tag are made in ink, and the tag accompanies the evidence from the moment it is acquired until it is relinquished. An evidence tag is not a substitute for marking evidence, but is an administrative convenience for locating evidence while it is in custody.

Chain of Custody. Chain of custody begins when an item of evidence is received. The number of persons who handle an item of evidence should be kept to a minimum. All persons who handle an item are considered links in the custody chain and such persons must receipt for each item whenever a transfer is made. An investigator in possession of evidence is personally liable for its care and safekeeping.

Three factors influence the introduction of evidence at trial:

- The object must be identified.
- Relevancy must exist.
- Continuity or chain of custody must be shown.

Rules of Evidence

The rules for presenting evidence in a criminal investigation are as varied as the types of evidence. Let us look at them.

Opinion testimony is a conclusion drawn by a witness, hence the term opinion testimony. Another form of testimonial information is hearsay evidence. Hearsay is a statement that is made other than by a witness. Hearsay cannot be entered into evidence unless the maker of the statement can be cross-examined.

Privileged communication is confidential information between two persons recognized by law as coming within the so-called privileged relationship rule. The following relationships are generally recognized: a husband and wife, an attorney and client, a physician and patient, and a law enforcement officer and informant.

Character evidence is evidence introduced by either defense or prosecution witnesses to prove the accused's good or bad character. Character evidence is usually introduced only when the defense raises the issue of the accused's character.

Direct evidence is evidence presented by a person who actually witnessed something. Contrast this with circumstantial evidence, which is evidence that proves other facts from which a court may reasonably infer the truth.

Admissibility is a characteristic or condition of evidence. To be admissible, evidence must be material, relevant, and competent. Evidence is material when it plays a significant part in proving a case. Examples of material evidence might be fingerprints of the accused that were found on the murder weapon, an eyewitness account of how the accused committed the crime, or stolen property found in the possession of the accused. Evidence is relevant when it goes directly to the proof or disproof of the crime or of any facts at issue. Examples of relevant evidence might be a death certificate or a medical examiner's report. Evidence is competent when it is shown to be reliable. Examples of competent evidence might be accurate business records or the testimony of an expert fingerprint examiner.

Burden of proof is a rule which holds that no person accused of a crime is required to prove his or her innocence. The prosecution must prove the guilt of a defendant beyond a reasonable doubt. Reasonable doubt means the jury must believe the charges to be true to a "moral certainty." On the other hand, the accused must prove his or her contentions. Such defenses as self-defense, insanity, and alibi are affirmative defenses that must be proved by the accused.

A presumption is a conclusion that the law says must be reached from certain facts. Presumptions are recognized because experience has shown that some facts should be accepted or presumed true until otherwise rebutted. For example, defendants are presumed to be sane

at the time the crime was committed, and at the time of trial, in the absence of proof to the contrary. Presumptions are of two classes: conclusive and rebuttable. A conclusive presumption is one that the law demands be made from a set of facts, e.g., a child under 7 years of age cannot be charged with a crime. A rebuttable presumption can be overcome by evidence to the contrary, e.g., presumption of death after being unaccounted for and missing for 7 years.

Rules of Exclusion

In general, rules of exclusion deal with conditions in which evidence will not be received. They limit the evidence a witness may present to those things of which he had direct knowledge, i.e., what he saw, smelled, tasted, felt, or heard.

All evidence, direct and circumstantial, if relevant, material, and competent is admissible provided it is not opinion testimony, hearsay evidence, or privileged communication. There are exceptions regarding the admissibility of opinion testimony and hearsay evidence. An exception to the rule against opinion testimony can be made when no other description could be more accurate. For instance, a witness is allowed to testify on such matters as size, distance, time, weight, speed, direction, drunkenness, and similar matters, all of which require the witness to state an opinion. There is no requirement for the witness to be an "expert" when testifying to facts such as these.

Exceptions to the rule against hearsay can be made for the dying declaration and the spontaneous declaration. The admissibility of a dying declaration is limited to homicide cases. Because of the seriousness of homicide, a dying declaration is an exception. A dying declaration is admissible either for or against the accused. The statement must have been made when the victim believed he was about to die and was without hope of recovery. The admissibility of the declaration will not be affected as long as the victim dies; otherwise, the issue would not arise since there would be no charge of homicide.

The spontaneous declaration, a statement made under conditions of shock or excitement, may be admitted as another exception to the hearsay rule. Normally, such a statement is made simultaneously with an event or act and there is not time or opportunity to fabricate a story. It is generally accepted that the statement will be admitted if it precedes, follows, or is concurrent with the act. The statement cannot have been made in response to a question and must pertain to the act that produced it. The spontaneity of the statement is sufficient guarantee of truthfulness to compensate for the denial of cross-examination.

In prosecutions for sexual offenses, evidence that the victim made a complaint within a short time after the offense occurred (i.e., a fresh complaint) is admissible in certain cases. The fact that the complaint was made is relevant for corroborating the testimony of the victim. The statement may relate only to who and what caused the conditions, and merely indicate the credibility of the victim as a witness.

An official statement in writing made as a record of fact or event by an individual acting in an official capacity (called a "business record") is admissible to prove the truth of a matter. Records are of two types: private and public. To introduce private records, someone associated with the business must introduce them. He must show that the company kept records, that the record produced was one of these records, and that the record was the original or certified copy of the original. Public records are usually introduced by presenting certified copies.

A confession is a statement or complete acknowledgment of guilt. An admission is a statement which does not amount to a complete acknowledgment of guilt, but links the maker with a crime. Admissions are forms of hearsay. A court is inclined to apply the same rules of admissibility to admissions as for confessions.

John J. Fay

FORENSICS: FBI IDENTIFICATION AND LABORATORY SERVICES

The FBI's Identification Division contains the largest collection of fingerprint identification data in the world available to law enforcement agencies. Services of the division include furnishing standard forms, such as fingerprint cards, for submitting identification data; searching of fingerprint cards; making name checks to locate identification records; sending fugitive notices to enforcement agencies; making latent print examinations; examining fingers of deceased persons for possible identification; and

assisting in the identification of persons killed in major disasters.

The Laboratory and the Technical Services Divisions of the FBI have capabilities in a wide range of forensic sciences: (1) document analysis, (2) scientific analysis, and (3) analysis of audio/video recordings and electronic devices. Competent expert testimony and technical assistance are provided in special situations, such as kidnapping cases, airline disasters, and photographic problems.

These divisions maintain standard reference files and collections of typewriter standards, automotive paint, firearms, hairs and fibers, blood sera, safe insulation, shoe prints, tire treads, watermark standards, safety paper standards, checkwriter standards, office copier standards, and National Motor Vehicle Certificate of Title File.

Files of questioned material consist of the National Fraudulent Check File, Bank Robbery Note File, Anonymous Letter File, National Motor Vehicle Certificate of Title File, Pornographic Materials File, National Stolen Art File, and National Stolen Coin File.

In the laboratory's National Automobile Altered Numbers File (NAANF) are surface replica plastic impressions of altered vehicle identification numbers found on stolen cars, trucks, and heavy equipment. The purpose of this file is to have a central repository for specimens of altered numbers so that comparisons can readily be made to identify recovered stolen vehicles and to link such vehicles with commercialized theft rings.

A related reference file is the National Vehicle Identification Number Standard File (NVSF), which contains standards of Vehicle Identification Number (VIN) plates from each factory of the major manufacturers of American automobiles. The purpose of the file is to enable the FBI Laboratory to determine whether or not a submitted VIN plate is authentic. Additionally, it gives the laboratory the capability, in the event that bogus VIN plates are being prepared in an automobile factory, to identify the factory and the machine used in making the bogus plates.

Engineering Section Capabilities

The Engineering Section of the Technical Services Division is responsible for the development, procurement, and deployment of many types of technical equipment used in support of the FBI's investigative activities. In addition, this section has the capability of examining evidence of an electrical or electronic nature, conducting analysis of magnetic recordings, and providing expert testimony regarding findings. Engineering Section capabilities include the following.

Authenticity Determination. This analysis is made in cases involving allegations of tape tampering and/or alteration by a defense expert, and when the legitimacy of the recording cannot be established through chain of custody and testimony.

Signal Analysis. In this test, various analyses are conducted to identify, compare, and interpret non-voice sounds on original tape recordings, including telephone dialing, gunshots, and radio transmissions.

Speaker Identification. This test uses the spectrographic (voice-print) technique to compare the recorded voice of an unknown individual to a known recorded voice sample of a suspect. Decisions regarding speaker identification by the spectrographic method are not considered conclusive, since there is limited scientific research regarding the reliability of the examination under the varying conditions of recording fidelity, interfering background sounds, sample size, voice disguise, restrictive frequency range, and other factors commonly encountered in investigative matters.

Sound Recording Comparisons. This is an aural examination to determine if a recovered "bootleg" tape recording contains the same material as a copyrighted commercial tape.

Tape Duplication. This service provides standard format copies of unusual or obsolete tapes or disc recordings.

Tape Enhancement. This is the selective suppression of interfering noise on audio recordings, or the audio track of video recordings, to improve the voice intelligibility.

Telephone toll fraud examinations are made to identify:

- "Blue Box" and "Black Box" devices, which receive toll-free long distance telephone calls.

- "Red Box" devices, which allow free pay telephone calls.

Interception of Communications Examinations include identification of:

- Wire tap devices attached to telephone lines, which monitor, record, or transmit telephone conversations as a radio signal to a remote location.
- Infinity transmitter devices, which allow a room conversation to be monitored by a remotely activated microphone on a telephone line.
- Telephones which have been modified to monitor a room conversation when the telephone is not in use.
- Miniature transmitters, concealed microphones and recorders designed to surreptitiously intercept oral communications.

Other examinations include identification of devices used to defeat "burglar alarm" systems, FM radio transceivers, scanners and tracking devices, and electronic devices of unknown use or origin believed to have been used in the commission of a crime.

The FBI's services in these areas are available to all federal agencies, U.S. attorneys, military tribunals, in both civil and criminal matters, and to all duly constituted state, county, and municipal law enforcement agencies in the United States in connection with their official criminal investigative matters only. These services, including the loan of experts if needed as expert witnesses, are rendered free of cost to the contributing agency.

As a general rule, Laboratory Division examinations are not made if the evidence is subjected elsewhere to the same examination for the prosecution. Additionally, in order to more effectively and efficiently utilize its resources, the laboratory will not accept cases from other crime laboratories that have the capability of conducting the requested examination(s).

Because of the nature of the evidence submitted for fingerprint examinations, the previously mentioned Laboratory Division restriction does not apply. Therefore, the Identification Division will examine fingerprint evidence even if it has been or will be subjected to examination by other fingerprint experts.

Blood and Other Body Fluids

Forensic serology involves the identification and characterization of blood and other body fluids on items associated with a crime or crime scene. Evidence from violent crimes, such as murder, rape, robbery, assault, and hit-and-run usually bear body fluid stains.

Blood examinations aid investigations:

- By locating the possible crime scene. Identification of human blood similar in type to that of the victim can assist investigators in identifying the crime scene.
- By discovering a crime. Occasionally, the identification of human blood on a highway, sidewalk, porch, or in a car is the first indication that a crime has occurred.
- By identifying the weapon used. The grouping of human blood found on a club, knife, or hammer can be of considerable probative value.
- By proving or disproving a suspect's alibi. The identification of human blood on an item belonging to a suspect who claims that the blood is of animal origin refutes an alibi, whereas the identification of animal blood can substantiate the alibi.
- By eliminating suspects. The determination that the human blood on items from the suspect is different in type from that of the victim may exculpate the suspect. Blood similar to that of the suspect can help corroborate a suspect's claim of having a nosebleed or other injury.

Testing can determine whether visible stains do or do not contain blood. The appearance of blood can vary greatly depending on the age of the stain and the environmental conditions (such as temperature, light, and humidity) to which it was subjected. Chemical and microscopic analyses are necessary to positively identify the presence of blood in a stain and to determine whether blood is of human or non-human origin, and if non-human, the specific animal family from which it originated.

Human blood can be classified according to the four groups of the International ABO Blood Grouping System and other blood grouping systems, including red blood cell enzyme and serum protein systems, which are analyzed by electrophoresis.

The age of a bloodstain or the race of the person from whom it originated cannot be conclusively determined, and using conventional serological techniques it is not possible to identify human blood as having come from a particular person.

An investigation can also be aided by the examination of semen, saliva, and urine.

Semen. The identification of semen by chemical and microscopic means on vaginal smears, swabs, or on the victim's clothing may be of value in corroborating the victim's claims. Enzyme typing is possible on semen stains of sufficient size and quality.

DNA analysis may allow for positive personal identification of the semen source. If DNA analysis is unsuccessful and the depositor is a secretor, grouping tests may provide information concerning the depositor's ABO blood type.

Saliva. A saliva sample from a known source may be used in conjunction with the liquid blood from the same source to establish the secretor status of the individual. Saliva from a questioned source may provide information as to ABO blood type of the depositor.

Known saliva samples should be submitted from both the suspect(s) and victim(s) in sexual assault cases, and in cases where a saliva examination may provide probative information (e.g., a cigarette butt found adjacent to a homicide victim's body).

Urine. Urine may be qualitatively identified by chemical testing. Absolute identification of a stain as urine is not possible; however, no routinely reliable forensic techniques are available that provide blood group information from urine.

Secretors and Secretor Status. Secretors (which represent approximately 75 percent of the U.S. population) are individuals who have in their non-blood body fluids (e.g., semen, saliva, and vaginal fluid) detectable amounts of substances that are chemically similar to the antigens located on red blood cells, which confer ABO blood type.

It is because of this that the ABO blood type of a secretor can often be determined from a non-blood body fluid stain from that individual. Nonsecretors (the remainder of the population) do not exhibit these blood group substances in their non-blood body fluids.

The Lewis blood grouping system can be utilized to determine secretor status from a liquid blood sample. If, however, the secretor status cannot be determined from the known blood, then the known saliva sample can be examined.

Limitations on Seminal and Saliva Stains. Sometimes semen is mixed with urine or vaginal secretions from the victim. This can make interpretation of grouping tests more difficult inasmuch as the blood group substances from the victim's body fluids could mask the blood group substances in the semen.

To make a meaningful comparison of grouping test results on questioned semen and saliva stains, the investigator will need to obtain known liquid blood and known dried saliva samples from the victim and suspect.

Saliva on cigarette butts is often contaminated with dirt. Saliva on cigar butts is not groupable. Ash trays should not be simply emptied into a container. Rather, individual cigarette butts should be removed from the ash and debris, and packaged separately. In view of the difficulties involved in cigarette saliva grouping and the circumstantial nature of any successful result, it is often more judicious for the investigator to request latent fingerprint examinations of cigarette butts in lieu of serological examinations.

It is not necessary to submit known semen samples from the suspect in rape cases because the information necessary to make comparative analyses can be gleaned from the suspect's known blood and known saliva samples.

Rape Case Considerations

In light of recent developments in forensic DNA technology, the collection and preservation of serological evidence in a rape case warrants special consideration The forensic serologist can often provide the investigator with information beyond the fact that "semen is present" on an item if the proper samples are obtained, preserved, and submitted to the laboratory in a timely manner.

Body cavity swabs should be collected from the victim as expeditiously as possible following the assault. Once dried and packaged, these swabs should be frozen until they are submitted to the laboratory.

DNA Examinations

Deoxyribonucleic acid (DNA) is analyzed in body fluids and body fluid stains recovered from physical evidence in violent crimes. DNA analysis is conducted utilizing the restriction fragment length polymorphism (RFLP) method or other appropriate DNA methods. Evidence consists of known liquid and dried blood samples, portions of rape kit swabs and extracts, and body fluid stained cuttings from homicide, sexual assault, and serious aggravated assault cases.

The results of DNA analysis on a questioned body fluid stain are compared visually and by computer image analysis to the results of DNA analysis on known blood samples as a means of potentially identifying or excluding an individual as the source of a questioned stain. As such, this technique is capable of directly associating the victim of a violent crime with the subject or the subject with the crime scene, similar to a fingerprint. The implementation of this technique in the laboratory represents a significant advance in forensic serology.

Chemicals

Toxicological Examinations. A toxicological examination looks for the presence of drugs and/or poison in biological tissues and fluids. The toxicological findings show whether the victim of a crime died or became ill as the result of drug or poison ingestion, or whether the involved persons were under the influence of drugs at the time of the matter under investigation.

Because of the large number of potentially toxic substances, it is necessary (unless a specific toxic agent is implicated prior to examination) to screen biological samples for classes of poisons.

Examples of these classes and the drugs and chemicals that may be found within these classes are as follows:

- Volatile compounds, e.g., ethanol, carbon monoxide, and chloroform
- Heavy metals, e.g., arsenic, mercury, thallium, and lead
- Inorganic ions, e.g., cyanide, azide, chloride, and bromide
- Non-volatile organic compounds, e.g., most drugs of abuse and other pharmaceuticals, as well as pesticides and herbicides

Drug and Pharmaceutical Examinations. The forensic laboratory will determine if materials seized as suspected drugs do in fact contain controlled substances. In addition, the laboratory can examine a wide variety of items, such as boats, aircraft, automobiles, clothing, luggage, and money, for the presence of trace quantities of cocaine, heroin, phencyclidine (PCP), etc. A pharmaceutical examination will identify products for the purpose of matching recovered products with stolen products, or for proving that pharmaceuticals were switched.

Arson Examinations. The gas chromatography technique is used to determine the presence of accelerants or other substances introduced to a fire scene to facilitate destruction. Debris collected from the scene of a suspected arson can be analyzed to learn if a distillate was used to accelerate the fire and, if so, testing can classify the distillate by product, such as gasoline, fuel oil, or paint solvent. Debris most suitable for analysis will be absorbent in nature, e.g., padded furniture, carpeting, plasterboard, and flooring.

General Chemical Examinations. Qualitative and quantitative analyses can be made of miscellaneous chemical evidence. Quality analysis is helpful in cases involving theft or contamination of chemical products, malicious destruction, and assault. Analysis of writing inks can match questioned documents with known ink specimens obtained from typewriter ribbons and stamp pads. In consumer product tampering cases, analysis can determine the presence and nature of contaminants, adulterants, and alterations to containers. Chemical examinations can be useful in evaluating tear gas and dyes in bank robber packets, constituents determination in patent fraud cases, and flash and water soluble paper in gambling and spy cases.

Document Examinations

The questioned document field includes examinations of handwriting; hand painting; typewriting; mechanical impressions, such as checkwriter imprints, embossed seals, rubber stamps, and printed matter; photocopies; paper; altered documents; obliterated writing; indented writing; charred documents; and others.

Handwriting and Hand Printing. Writers can be positively and reliably identified with their writings. Other characteristics, such as age, sex, and personality, cannot be determined with certainty from handwriting. A handwriting identification is based upon the characteristics present in normal handwriting. It is not always possible, therefore, to reach a definite conclusion in the examination of handwriting. Some of the reasons for inconclusive results are:

- Limited questioned writing.
- Inadequate known samples.
- Lack of contemporaneous writing, such as when a long period of time has elapsed between preparation of the questioned writing and the known samples.
- Distortion or disguise in either the questioned writing or the known writing. In this situation, the normal handwriting characteristics are not present.
- Lack of sufficient identifying characteristics in spite of ample quantities of both questioned and known writing.

Three types of forged writings are commonly examined:

- Traced Forgery. Produced by tracing over a genuine signature, this forgery cannot be identified with the writer. A traced forgery can, however, be associated with the original or master signature from which the forgeries were traced if it is located.
- Simulated Forgery. Produced by attempting to copy a genuine signature, this forgery may or may not be identifiable with the writer, depending on the extent to which normal characteristics remain in the signature. Samples of the victim's genuine signature should also be submitted for examination.
- Freehand Forgery. Produced in the forger's normal handwriting with no attempt to copy another's writing style, this forgery can be identified with the writer.

Typewriting Examinations. Questioned typewriting can be identified with the typewriter that produced it. This identification is based upon individual characteristics that develop on the type face and on other features of the machine during the manufacturing process and through use.

Photocopier Examinations. Photocopies can be identified with the machine producing them provided samples and questioned copies are relatively contemporaneous. Two sets of questioned photocopies can be identified as having been produced on the same machine, and possible brands or manufacturers can be determined by comparison with a reference file maintained at the laboratory.

Mechanical Impression Examination. Questioned printed documents can be compared with genuine printed documents to determine if counterfeit. Two or more printed documents can be associated with the same printing, and a printed document can be identified with the source printing paraphernalia such as artwork, negatives, and plates.

A checkwriter impression can be identified with the checkwriter that produced it, and examination of a questioned impression can determine the brand of checkwriter producing it. A rubber stamp impression can be identified with the rubber stamp producing it, and an embosser or seal impression can be identified with the instrument that produced it.

Paper Examinations. Torn edges can be positively matched, the manufacturer can be determined if a watermark is present, and paper can be examined for indented writing impressions. Indentations not visible to the eye can be brought up using appropriate instruments. Some watermarks provide dating information, indicating the date of manufacture of the paper.

Writing Instruments. Chemical analysis can determine if the ink of two or more different writings is the same or different formulation. The same analysis can be conducted with an ink writing and a suspect pen. The examinations do not identify a specific pen, only that the inks are the same formulation. Ink dating examinations can also show the earliest date a particular ink was produced.

True Age of a Document. The earliest date a document could have been prepared may sometimes be determined by examination of watermarks, indented writing, printing, and typewriting. Chemical analysis of writing ink may determine the earliest date the formulation was available.

The Federal Bureau of Investigation (FBI) Laboratory maintains reference files of known standards that can be compared with questioned materials submitted for analysis.

Typewriter Standards. These consist of samples of many styles of both foreign and domestic; they permit determination of possible brands or manufacturers of typewriter from examination of questioned typewriting.

Watermark Standards. This file is an index of watermarks found in paper; it enables determination of the paper manufacturer.

Safety Paper Standards. These are samples of a variety of safety papers which enable determination of paper manufacturer when used in production of fraudulent documents, such as checks and birth certificates.

Checkwriter Standards. Sample impressions from many checkwriters allow determination of checkwriter brand or manufacturer from examination of questioned impression.

Shoe Print and Tire Tread Standards. A collection of sole and heel designs and tire tread designs helps determine the manufacturer of shoes and tires from prints or impressions left at the crime scene.

Office Copier Standards. A collection of samples from and information about many brands of photocopiers and office duplicating machines assists in determining possible brands and manufacturers of a questioned photocopy.

Explosives Examinations

Explosives examinations are visual and microscopic analyses of bomb remains, commercial explosives, blasting accessories, military explosives, and ordnance items. Tool mark examinations of bomb components are also possible.

Bomb remains are examined to identify bomb components, such as switches, batteries, blasting caps, tape, wire, and timing mechanisms. Also identified are fabrication techniques, unconsumed explosives, and overall construction of the bomb. Instrumental examination of explosives and explosive residues are carried on in conjunction with bomb component examinations. All bomb components are examined for tool marks, where possible tools used in constructing the bomb are identified for investigative purposes.

Explosive Reference Files. The FBI Laboratory maintains extensive reference files on commercial explosives, blasting accessories, and bomb components. These files contain technical data plus known standards of explosive items and bomb components, including dynamite, water gels, blasting agents, blasting caps, safety fuse, detonating cord, batteries, tape, switches, and radio control systems.

Firearms

Firearms identification is the study by which a bullet, cartridge case, or shotshell casing may be identified as having been fired by a particular weapon to the exclusion of all other weapons.

The firearms examiner will provide one of three conclusions: (1) that the bullet, cartridge case, or shotshell casing was fired by the weapon; or (2) was not fired by the weapon; or (3) there are not sufficient microscopic marks to make a positive identification.

Bullets. Marks on bullets can be produced by rifling in the barrel of the weapon by a flash suppressor or possibly in loading. When a bullet and/or fragment bearing no microscopic marks of value for identification purposes is encountered, it is often useful to perform a quantitative analysis and compare the results to the similarly analyzed bullets of any recovered suspect ammunition (e.g., cartridges remaining in the suspect firearm, cartridges in suspect's pockets, partial boxes of cartridges in suspect's residence, etc.). When two or more lead samples are determined to be compositionally indistinguishable from one another, a common manufacturer's source of lead is indicated. Lead composition information, in conjunction with other circumstantial information, is often useful in linking a suspect to a shooting. Compositional analysis of shot pellets and rifled slugs can provide similar useful circumstantial information.

Cartridge Cases or Shotshell Casings. Marks on a fired cartridge case or shotshell casing can

be produced by breech face, firing pin, chamber, extractor, and ejector with a fired cartridge case. The examiner may be able to determine the specific caliber, type, and, possibly, make of the weapon that was fired. A fired shotshell casing can reveal gauge and original factory loading. Wadding can indicate gauge and possibly manufacturer. From shot, the examiner can determine size.

Extractor or ejector marks on a fired cartridge or casing that match with a specific weapon means only that the cartridge or casing had been loaded into and extracted from that specific weapon. To conclude that the cartridge or case was actually fired by the specific weapon, the examiner must rely on a firing pin impression or breech face and chamber marks.

Gunshot Residues. Gunshot residues on clothing may be located, depending on the muzzle-to-garment distance, in two ways: (1) by microscopic examination of the area surrounding the hole for gunpowder particles and gunpowder residues, smudging, and singeing; and (2) by chemical processing to develop a graphic representation of powder residues and lead residues around the hole. Test patterns can be compared with those produced at various distances using the suspect weapon and ammunition like that used in the case.

When a person discharges a firearm, primer residues can be deposited on that person's hands in varying amounts. These amounts are dependent upon the type, caliber, and condition of the firearm, and the environmental conditions at the time of the shooting. Residue samples can be collected from a suspect's hands and analyzed for the presence of the chemical elements antimony, barium, and lead, which are components of most primer mixtures. The analytical technique used to analyze these hand samples is dependent upon the type of hand samples collected from the suspect's hands.

Washing the hands and various other activities on the part of the shooter can remove substantial amounts of residue. Therefore, it is imperative to obtain samples as soon after the shooting as possible. Samples obtained more than 6 hours after a shooting are generally of little value and normally will not be analyzed.

Samples obtained from the hands of victims of close-range shootings (within approximately 10 feet) are generally of no value since it is not possible to differentiate between residues deposited on the hands of a shooter and victim of a close-range shooting. Therefore, samples from the hands of victims are not normally accepted for analysis.

Shot Pattern. The distance at which a shotgun was fired can be determined. It is necessary to fire the suspect weapon at various distances using the same type of ammunition involved in the case being investigated.

Hairs and Fibers

Hair and fiber examinations are valuable in person-to-person violence cases, such as rape and murder cases, because they can assist in placing the suspect at the scene of the crime by determining the interchange of hairs or fibers between the victim and suspect. Similarly, these examinations can be helpful in connecting a suspect to surreptitious crimes, such as burglary and auto theft, and in identifying the scene of the crime. Hairs or fibers found on knives, jimmy bars, and the like can identify the weapons or instruments of crime, as well as automobiles involved in hit-and-run cases. Victim and witness testimony can also be corroborated by the discovery of hairs and fibers.

Hairs. Examination of a hair can determine if it is animal or human; if animal, the species from which it originated (dog, cat, deer, etc.), and if human, the race, body area, how removed from the body, damage, and alteration (bleaching or dyeing).

The finding from a hair examination is good circumstantial evidence, but not positive evidence. An examination can conclude whether or not a hair could have originated from a particular person based on microscopic characteristics present in the hair. Age cannot be determined, but gender may be determined depending on the condition of the hair's root.

Fibers. Examination of a fiber can identify the type of fiber, such as animal (wool), vegetable (cotton), synthetic (human-made), and mineral (glass). The usual purpose of a fiber examination is to determine whether or not questioned fibers are the same type and/or color, and match the microscopic characteristics of fibers in a

suspect's garment. Like hairs, fibers are not positive evidence, but are good circumstantial evidence.

Fiber examinations can include analyses of fabrics and cordage. A positive identification can be made if a questioned piece of fabric can be fitted to the known material. Composition, construction, color, and diameter of fibers are the points of comparison. Cordage or rope left at the scene of the crime may be compared with similar materials, and in some cases the manufacturer can be identified if the material contains a unique tracer.

The same principles of examination can be applied to botanical specimens, where plant material from a known source is compared with plant material from a questioned locale.

Finally, identifications can be made through comparisons of teeth with dental records and X-rays with corresponding bone structures. Examinations may be made to determine if skeletal remains are animal or human. If human, the race, sex, approximate height and stature, and approximate age at death may be determined.

The presence of a suspect at the crime scene can be established from a comparison of wood from the suspect's clothing or vehicle, or possession of wood from the crime scene. The specific wood source can be determined from side or end matching and fracture matching.

Miscellaneous Examinations

Related examinations include button matches, fabric impressions, glove prints, feathers, knots, and identifying the clothing manufacturer through a label search.

Materials Analysis

These examinations entail the use of instrumentation, such as infrared spectroscopy, X-ray diffractrometry, emission spectrometry, and gas chromatography/mass spectrography (GC/MS), for identification or comparison of the chemical compositions of paints, plastics, explosives, cosmetics, tapes, and related materials.

Automobile Paints. It is possible to establish the year and make of an automobile from a paint chip by use of the National Automotive Paint File, which contains paint panels representing paints used on all makes of American cars and many popular imported cars such as Mercedes Benz, Volkswagen, Porsche, Audi, BMW, Renault, Honda, Subaru, Datsun, and Toyota. A very careful search of the accident or crime scene should be made to locate small chips because:

- Paint fragments are often found in the clothing of a hit-and-run victim. Therefore, the victim's clothing should be obtained and submitted to the laboratory whenever possible.
- Paints may be transferred from one car to another, from car to object, or from object to car during an accident or the commission of a crime. Occasionally it is better to submit an entire component, such as a fender or bumper, if the paint transfer is very minimal.

Non-Automobile Paints. Paint on safes, vaults, window sills, door frames, etc., may be transferred to the tools used to open them. Therefore, a comparison can be made between the paint on an object and the paint on a tool.

Cosmetics. Unknown or suspected cosmetics and/or makeup can be compared with a potential source in assault cases, such as rape. The investigator should be alert to the possible transfer of such materials between victim and suspect.

Plastics/Polymers. It is not possible to specifically identify the source, use, or manufacturer of plastic items from composition alone, but comparisons such as the following can be made:

- Trim from automobiles, depending upon the uniqueness of the composition, is compared with plastic remaining on property struck in a hit-and-run type case.
- Plastics comprising insulation on wire used in bombings, wiretapping, and other crimes are compared with known or suspected sources of insulated wire.
- Plastic/rubber tapes from crime scenes are compared with suspected possible sources.
- Polymers used in surgical cloth-backed tape are compared with sources.
- Miscellaneous plastic material from crime scenes is compared with possible sources.

Tape. A positive identification can be made with the end of a piece of tape left at the scene of the crime and a roll of suspect tape. If no end match is possible, composition, construction, and color can be compared as in other types of examinations.

Metallurgy

Metals or metallic objects may be metallurgically examined for comparison purposes and/or information purposes. Determinations to ascertain if two metals or two metallic objects came from the same source or from each other usually require evaluations based on surface characteristics, microstructural characteristics, mechanical properties, and composition.

Surface Characteristics. These are macroscopic and microscopic features exhibited by a metal surface, including fractured areas, accidental marks or accidentally damaged areas, manufacturing defects, material defects, fabrication marks, and fabrication finish. The fabrication finish reveals part of the mechanical and thermal histories of how the metal was formed, e.g., if it was cast, forged, hot-rolled, cold-rolled, extruded, drawn, swaged, milled, spun, or pressed.

Microstructural Characteristics. These are the internal structural features of a metal as revealed by optical and electron microscopy. Structural features include the size and shape of grains; the size, shape, and distribution of secondary phases; non-metallic inclusions; and other heterogeneous conditions. The microstructure is related to the composition of the metal and to the thermal and mechanical treatments that the metal has undergone; it therefore contains information concerning the history of the metal.

Mechanical Properties. These characteristics describe the response of a metal to an applied force or load, e.g., strength, ductility, and hardness.

Composition. This is the chemical element makeup of the metal, including major alloying elements and trace element constituents. Because most commercial metals and alloys are nonhomogeneous materials and may have substantial elemental variation, small metal samples or particles may not be compositionally representative of the bulk metal.

Broken and/or mechanically damaged (deformed) metal pieces or parts can be examined to determine the cause of the failure or damage, i.e., stress exceeding the strength or yield limit of the metal, material defect, manufacturing defect, corrosion cracking, and excessive service usage (fatigue). The magnitude of the force or load that caused the failure can be determined, as well as the possible means by which the force or load was transmitted to the metal and the direction in which it was transmitted.

Burned, heated, or melted metal can be evaluated to determine the temperature to which the metal was exposed; the nature of the heat source that damaged the metal; and whether the metal was involved in an electrical short-circuit situation.

Rusted or corroded metal can be examined to estimate the length of time the metal has been subjected to the environment that caused the rust or corrosion, and the nature of the corrosive environment.

Cut or severed metal can be tested to identify the method by which the metal was severed—sawing, shearing, milling, turning, arc cutting, flame cutting (oxyacetylene torch or "burning bar"), etc.; the length of time to make the cut; and the relative skill of the individual who made the cut.

Metal fragments can be analyzed to reveal the method by which the fragments were formed. If fragments had been formed by high-velocity forces, such as an explosion, it may be possible to determine the magnitude of the detonation velocity. It may also be possible to obtain an identification of the item that was the source of the fragments. In bombings, timing mechanisms can often be identified as to type, manufacturer, and model; determinations are sometimes possible as to the time displayed by the mechanism when the explosive detonated and as to the relative length of time the mechanism was functioning prior to the explosion.

Examination of nonfunctioning watches, clocks, timers, and other mechanisms can be revealing as to the condition responsible for causing the mechanism to stop or malfunction, and whether the time displayed by a timing mechanism represents a.m. or p.m.

For items unidentified as to use or source, it may be possible to identify the use for which

the item was designed, formed, or manufactured, based on the construction of and the type of metal in the item. The manufacturer and the specific fabricating equipment utilized to form the item might be revealed, as well as the possible sources of the item if an unusual metal or alloy is involved. Lamp bulbs that are subjected to an impact, such as from vehicles involved in an accident, can be examined to determine whether the lights of a vehicle were incandescent at the time of the accident.

Objects with questioned internal components can be exposed to X-ray radiography to non-destructively reveal the interior construction and the presence or absence of defects, cavities, or foreign material.

Mineralogy

Mineralogy includes materials that are mostly inorganic, crystalline, or mineral in character. Comparisons will, by inference, connect a suspect or object with a crime scene, prove or disprove an alibi, provide investigative leads, or substantiate a theorized chain of events. These materials include glass, building materials, soil, debris, industrial dusts, safe insulation, minerals, abrasives, and gems.

Glass Fractures. Glass, a non-crystalline, rigid material, can be excellent physical evidence. Fracture patterns can provide valuable information as to direction of breaking force. A physical match of two pieces of glass results in an opinion that they came from a common source to the exclusion of all other sources.

Penetration of glass panes by bullets or high-speed projectiles produces a cone pattern from which the direction and some idea of the angle of penetration can be determined. The type of projectile can also sometimes be determined. By an examination of stress lines on radial cracks near the point of impact, the direction of the force used to break the glass can be determined. This determination depends on identification of the radial cracks and the point or points of impact. By fitting glass pieces together with microscopic matching of stress lines, the laboratory examiner can positively identify the pieces as originally having been broken from a single pane, bottle, or headlight. If pertinent portions of a bottle, headlight, or taillight can be fitted together, the manufacturer and type may be determined for lead purposes.

When a window breaks, glass particles shower toward the direction of the force 10 feet or more. Particles, therefore, can be found in the hair and on the clothing of the perpetrator. Particles can also become embedded in bullets and/or objects used to break windows. Particles of broken glass from a hit-and-run vehicle are often present on the victim's clothing; many times the driver of a hit-and-run vehicle will emerge from the vehicle to determine what was hit or how seriously the victim was injured; consequently, broken glass from the accident may often be found embedded in the driver's shoes.

By microscopic optical and density comparisons, glass particles can be identified or compared with glass from a known source. The laboratory expert cannot identify the source to the exclusion of all other sources; however, it can be stated and demonstrated that it is highly improbable that the particles came from a source other than the matching known source; if two or more different known sources can be matched, the conclusion is greatly enhanced.

Soils, Dust, and Debris. Soil is any finely divided material on the surface of the earth and may contain such human-made material as cinders, shingle, stones, glass particles, paint, and rust. Soil, as a category, includes debris and industrial dusts, as well as natural soils.

Soil varies widely from point to point on the surface of the earth and even more with depth. For example, industrial dust specimens or soil near factories are often distinctive, and debris may contain particles characteristic of a specific area. Soil cannot be positively identified as coming from one source to the exclusion of all others, but the laboratory expert can associate questioned soil with a most probable source, conclude that a source cannot be eliminated, or that a point or area could not be the source of the questioned soil. Such conclusions have proven extremely valuable in the proof of criminal cases. Soil specimens will often consist of shoe prints, tire marks, burial sites, or mud taken from an area where a transfer of soil to the suspect is logical.

Safe Insulation and Building Materials. Safe insulation is found between the walls of fire-resistant safes, and in vaults and safe cabinets. It is readily transferred to tools and clothing.

Samples of insulation collected at the scene can be compared to apparel, shoes, and tools confiscated from the suspect. The same principles apply where unlawful entry through a roof or wall may cause particles to adhere to the suspect or the tools used.

Photographic Examinations

Infrared, ultraviolet, and monochromatic photography can be utilized to assist in rendering visible, latent photographic evidence that is not otherwise visible to the unaided human eye. Examples of this type of evidence include alterations and obliteration to documents, invisible laundry marks, and indented writing.

Bank Robbery Film. The laboratory can examine this film to:

- Attempt enhancement of poor quality photographic exposures and/or prints.
- Compare in detail the unknown subject's clothing as depicted in the film with the clothing obtained from a suspect.
- Determine the individual's height as depicted in the film. Height is determined preferably from a height chart, but it can also be done mathematically, often to within an inch.
- Compare facial features of the unknown subject in the film with those in a known photograph of a suspect.

Miscellaneous Photographic Examinations. Various other types of photographic examinations can be conducted such as:

- Comparison of film or prints to determine if they were taken by a specific camera.
- Determine the type and date of Polaroid film, as well as preparing a print from the "throw-away" portion.
- Determine if photographs have been altered.

Considerable information can usually be obtained from photographic evidence, using hundreds of various techniques. If photographic materials are in question, they should be forwarded to the laboratory with a clear narrative as to what information or examination is desired.

Reference Files

The FBI Laboratory maintains a number of reference files that can be used for comparison purposes in the evaluation of forensic evidence.

National Motor Vehicle Certificate of Title File. Samples of genuine state motor vehicle certificates of title, manufacturer's statement of origin, and vehicle emissions stickers assist in determination of authenticity of questioned certificates. This file contains photographs of fraudulent documents to assist in association of questioned material from different cases with a common source.

National Fraudulent Check File. A computerized file contains images of fraudulent and counterfeit checks, which helps associate fraudulent checks from different cases with a common source and assists in identification of fraudulent check passers.

Anonymous Letter File. A computerized file contains images of kidnapping, extortion, threatening, and other anonymous communications. This file is matched with questioned documents from different cases with a common source.

Bank Robbery Note File. Images of holdup notes are used to link notes used in various robberies with a common source.

National Stolen Art File. This is a listing of stolen and recovered artwork, mostly paintings, reported by law enforcement agencies. Because artwork does not bear a serial number, entries in the file are based upon a description of the artwork. When available, an image of the artwork is stored, which can be recalled for reference. During a file search, both data and image will appear simultaneously. The minimum value of stolen and recovered artwork for inclusion in the file is $2,000.

National Stolen Coin File. This is a computerized listing of stolen and recovered coins reported by law enforcement agencies. Because coins do not have serial numbers, entries in the file are based upon a description of the coin along with a photograph when available. During a file search, both data and image will appear simultaneously. The minimum value of stolen

and recovered coins for inclusion in the file is $2,000.

Pornographic Materials Files. A collection of evidentiary pornographic materials, printed and video, helps in determining proof of interstate travel of pornographic material, and assists in determining production and distribution channels, as well as identity of actors.

These consist of materials submitted in connection with investigations of violations of the White Slave Traffic Act, Interstate Transportation of Obscene Materials, and sexual exploitation of children statutes. This computerized file contains over 50,000 records of commercially produced pornographic materials, and the inventory of items is in every medium including video tapes, 8-millimeter movies, books, magazines, and photographs.

These files provide reference materials for laboratory examiners, data searches for investigations (investigative lead information regarding subject, companies, or specific pornographic products), and "charge out" materials for limited courtroom use and undercover operations.

Shoe Print and Tire Tread Evidence

Shoe print and tire tread evidence found at the scene of a crime can provide important evidence for investigation and eventual prosecution of a case. For three-dimensional impressions, casts should always be made immediately following appropriate photography of the impressions. For two-dimensional impressions, the original impression is most valuable and should be retained and preserved whenever possible and practical, such as when the impression is on glass, paper, or some other retrievable surface.

Shoe and tire reference materials are maintained in the laboratory to assist in the determination of the make or manufacturer of a shoe or tire that made a particular impression. This is useful in some cases to help locate suspects or suspect vehicles.

When known shoes or tires are obtained, comparisons are made between those items and the questioned shoe prints or tire impressions. Comparisons can be made between the physical size, design, manufacturing characteristics, wear characteristics, and random accidental characteristics. If sufficient random characteristics are present, a positive identification can be made.

Tool Mark Identification

Tool mark examinations are microscopic studies to determine if a given tool mark was produced by a specific tool. In a broader sense, they also include the identification of objects that forcibly contacted each other, were joined together under pressure for a period of time and removed from contact, and were originally a single item before being broken or cut apart. The inclusion of these latter areas results from the general consideration that when two objects come in contact, the harder object (the tool) will impart a mark on the softer object. Saws, files, and grinding wheels are generally not identifiable with marks they produce.

The tool mark examiner can conclude that: (1) the tool produced the tool mark, (2) the tool did not produce the tool mark, or (3) there are not sufficient individual characteristics remaining within the tool mark to determine if the tool did or did not produce the questioned mark.

Several comparisons can be made between a tool and a tool mark. Examination can be made of the tool for foreign deposits, such as paint or metal; for comparison with a marked object; establishment of the presence or nonpresence of consistent class characteristics; and microscopic comparison of a marked object with several test marks or cuts made with the tool. Examination of the tool mark can determine the type of tool used (class characteristics); the size of tool used (class characteristics); unusual features of the tool (class or individual characteristics); the action employed by the tool in its normal operation, and/or in its present condition; and most importantly, if the tool mark is of value for identification purposes.

Fracture Matches. Fracture examinations are conducted to ascertain if a piece of material from an item, such as a metal bolt, plastic automobile trim, knife, screwdriver, wood gunstock, or rubber hose, was or was not broken from a like damaged item available for comparison. This type of examination may be requested along with a metallurgy examination if questioned items are metallic in composition.

Marks in Wood. This examination is conducted to ascertain whether or not the marks in a wood specimen can be associated with the tool used to cut it, such as pruning shears and auger bits. This examination may be requested along with a wood examination.

Pressure/Contact. Pressure or contact examinations are conducted to ascertain whether or not any two objects were or were not in contact with each other, either momentarily or for a more extended time.

Plastic Replica Casts of Stamped Impressions. Plastic replica casts of stamped numbers in metal, such as altered vehicle identification numbers, can be examined and compared with others, as well as with suspect dies.

Locks and Keys. Lock and key examinations can be conducted to associate locks and keys with each other. Such associations are useful in establishing a conspiracy or link of commonality between or among individuals. It is often possible to illustrate this through their possession of keys that will operate a single, lockage instrumentality (e.g., vehicle, safe house, or padlock). Laboratory examination of a lock can determine whether an attempt has been made to open it without the operating key.

Restoration of Obliterated Markings. Obliterated identification markings are often restorable, including markings obliterated by melting of the metal as evidenced by welding marks or "puddling."

Obliterated markings can also be restored on materials other than metal, such as wood, plastics, and fiberglass. Because different metals and alloys often require specific methods for restoration of obliterated markings, the laboratory should be contacted for number restoration procedures for field processing of items too large or heavy for submission.

Conclusion

FBI experts will furnish testimony regarding evidence they have examined. In the interest of economy, however, their testimony should not be requested if it is to be duplicated by another prosecution expert. It is realized that exceptions to this general policy may be required in a given instance.

Source "Laboratory Services." 1992. *Federal Bureau of Investigation.*

HUMAN FACTORS IN INTERVIEWING

Human factors strongly influence interviews. The skilled interviewer recognizes this critical point and strives to understand and deal with the motives, fears, and mental makeup of the interviewee. The line of questions and interview techniques are selected on the basis of an assessment made by the investigator of the interviewee's psychological makeup.

Perception

The average person does not possess strong perceptive skills, and among different people are different skill levels. This point has been illustrated many times in controlled situations where a single event is observed by several persons. As each person recounts his/her observations of the event, we are surprised at how many different versions are offered of the same incident. Why is this so? Psychologists tell us that perception is conditioned by:

- Differing abilities to see, hear, smell, taste, and touch.
- The location of the viewer in relation to the incident at the time of occurrence. Distance and geographical perspective affect vision.
- The amount of time intervening between occurrence and interview.
- The number and nature of events that occur during the interval between occurrence and interview.

What are the implications of these factors? Well, for one thing, the interviewer should attempt to discover if the person being interviewed has physical disabilities that impair the senses. If it is known, for example, that a witness has a vision problem, the investigator should be careful in accepting at full value statements that are based on what the witness saw. It is far better to discover problems in a witness's perception at the outset of an

investigation than to have such problems exploited at time of trial by the defendant's lawyer.

It might be helpful during an interview for the investigator to ask the interviewee to place himself or herself on a map or a sketch that depicts the physical layout of the scene at the time of the incident. The position of the interviewee in relation to other persons and objects can help the investigator evaluate how much the person could have seen, heard, or smelled. This technique also discourages fanciful elaboration by the person being interviewed.

Because human memory erodes over time, interviews should be conducted as quickly as practical. Memory not only fades, but becomes colored, either consciously or unconsciously, by what the witness is exposed to after the incident. Remarks made by other witnesses or newspaper accounts may cause an interviewee to fill in memory gaps with inaccurate details. A witness may form an own opinion of guilt or innocence and shape his/her testimony accordingly. This possibility is reduced when the interview is conducted soon, that is, before the witness has time to form personal judgments that distort the truth. Prompt interviewing also affords a suspect less time to formulate an alibi or to "get the story straight" with fellow accomplices.

A person who is subjected to stressful, exciting, or injurious events after observing an incident is likely to forget details. To illustrate, assume a pedestrian observes a speeding motorist strike another pedestrian and drive away from the scene. The witness is caught up in a series of actions, such as giving first aid assistance to the injured, that interfere with recollection.

Prejudice

It is not unreasonable to expect every interviewee to be prejudiced to some degree. The strength and targets of prejudice vary among people. The investigator should be alert to prejudice and deal with it when it surfaces. One way to keep information from being distorted by prejudice is to require detailed, specific answers during an interview. If allowed to talk in generalities, a prejudiced person will make statements that are partially accurate and partially misleading. By remaining within a narrow line of discussion aimed at a specific issue, the investigator forces the interviewee to respond with information that is free of bias.

Hostility

Suspects are naturally reluctant to talk, and we expect them to be uncooperative and resistive to interviewing. Sometimes we are surprised (and dismayed) when we discover that witnesses and even victims show an unwillingness to talk. Finding the reason for hostility is a first step in overcoming it.

Fear of Self-Involvement

The fear of self-involvement is a common obstacle to information collection. Many citizens are unfamiliar with investigative methods and are afraid to assist. Also, a person may have committed a separate offense at some previous time and is fearful it will come to light. Some persons think that crimes that do not happen to them directly are not their business, or they believe that the misfortunes that befall victims are of the victims' own making. Many people are very private, disliking publicity in general, and some people fear reprisal. The investigator who knows the underlying reason for resistance is better able to work around it.

Inconvenience

Disruption of lifestyle is not pleasant. We are all pretty much animals of habit and we dislike it when the routines of our daily lives are upset because we are kept waiting or inconvenienced by an unexpected event. Some people will actually disclaim knowledge of criminal matters because they wish to avoid questioning. We are also aware of witnesses being required to wait several days in courthouse hallways and then not be called to the stand. Even when a witness is compensated for lost time, there is a residue of resentment against a process that penalizes citizens in the name of civic duty.

Resentment

With some people resentment runs deep and wide. It may manifest itself in a dislike for authority generally. Resentment can appear in the form of blind loyalty to the accused person. We are talking here not of the American

tradition that pulls for the underdog, but of the unreasoning attitude that criminals are victims of a repressive society.

Personality Conflicts

Occasionally an interviewee and interviewer will get along beautifully right from the start. More often an interviewing session will begin with mixed feelings and, through the normal give and take of interpersonal communications, a foundation of mutual respect and cooperation will develop. Sometimes, but infrequently, interviewer and interviewee will for one reason or another find it impossible to communicate at all. When this happens the conflict usually has its roots in the attitudes of the interviewee. A successful interviewer will compensate by demonstrating friendliness, showing respect for the interviewee, and using the right words at the right time. In those cases where the investigator is unable to overcome a basic personality conflict, the best course of action is to voluntarily withdraw in favor of another questioner. This should not be regarded as failure, but recognition of a human factor that must be accommodated in the interest of achieving a successful investigative outcome.

John J. Fay

IDENTITY THEFT

According to the Federal Trade Commission over 11 million consumers had their identities stolen and misused in 2004. While the number of victims in 2005 has not yet been officially tallied, it is estimated that one in every 31 consumers was a victim. According to James Van Dyke of Javelin Strategy & Research Inc., a California-based research firm, contrary to popular wisdom the Internet is not the problem. Van Dyke and others objectively argue that the Internet may be a consumer's best fraud-fighting tool. His study reveals that the Internet has gotten a bad rap and the risk it poses to consumers may be grossly exaggerated. "The very thing consumers are most afraid of is actually the thing that makes [them] safer," reports Van Dyke. Those who noticed the fraud quickly by viewing their accounts online usually were able to cut their losses. Van Dyke's study also showed that consumers who spot fraud online suffer an average theft of only about $500 while consumers who spot the problem by other means suffer average losses closer to $4,500.

Van Dyke's study also suggests personal data is most often stolen offline—from an employer or trash bin. Only 12 percent of the victims in his study reported they believed their information was stolen electronically. Stolen or lost wallets, checkbooks, and mail remain the principal mechanisms by which thieves obtain the identities of others. FTC attorney Lois Greisman said, "The crime [identity theft] is not growing" and that "We're seeing a leveling off and that's where you're going to see your first signs of improvement. I'd like to say this is a positive signal."

Fraud investigators have long known that most identity thieves do not typically use public records or computers to steal identities. Moreover, while the crime itself is particularly offensive, under most circumstances the victims suffer little to no harm until the thief uses the stolen identity to commit a more serious crime. Thus, to many it seems that fighting identity theft by restricting access to public records is like attempting to stop telephone fraud by eliminating the public's access to telephones.

Historical Perspective

Identity theft is not a new crime. For centuries criminals have assumed the names and identities of others to hide and escape the long arm of the law. Over the ages, smugglers, pirates, and political revolutionaries have used aliases to protect their true identities and further their endeavors. The use of physical disguises and false identities continues to aid criminals to this day. However, only during the last two decades has the crime of identity theft entered our lexicon and captured our attention. Only since the advent of the desk-top computer and the Internet has identity theft been easy and profitable.

While losses due to identity theft are estimated to be in the billions of dollars, the actual economic impact is difficult to calculate. The Federal Trade Commission (FTC), along with other researchers, frequently lumps ID theft and credit card fraud together. For example, in the

FTC 2002 survey ID theft victims were defined as those who had suffered a stolen and misused credit card, lost money from a personal checking/savings account by way of fraud, or had at any time been the victim of a telephone, Internet, or insurance fraud. Such broad definitions tend to distort reality and limit meaningful analysis. Adding additional complexity is the fact that many victims never report the crime. Businesses particularly are hesitant to make public disclosures when losses occur. In many cases only when it is absolutely necessary is any disclosure made at all. Moreover, the media is rarely sympathetic to the business that becomes a victim, further disincentivizing the well-meaning enterprise. The press abounds with shocking tales of hapless employers who lose personal information on employees, customers, and even shareholders.

It is easy to see that large losses of personal information cause problems for both the individual whose information is lost but also the party that lost it. In some instances, it would appear, the public relations damage to the organization can far exceed the sum of the hard dollar losses suffered by the individual victims. It is also apparent that as small computers and other similar technologies play a greater role in business and are able to hold greater and greater amounts of information, the potential exposure will continue to grow.

How Identity Theft Occurs

In 2002 Ernst & Young reported that over 47 percent of surveyed organizations had been significantly affected by fraud in the previous year. The study concluded that 13 percent of the losses were over $1 million. "Corporate scandals ripped from today's headlines are forcing executive management worldwide to take a closer look at the policies and procedures they have in place to control and mitigate incidents of fraud," said David L. Stulb, in a study conducted by Ernst & Young's North American Global Investigative Services Group. The study says that 51 percent of the organizations surveyed were recovering a greater proportion of fraud-related financial losses than in prior years, an increase from 29 percent. The report also revealed that 60 percent of reporting companies had trained their staff on guidelines relating to fraud-related behavior, but a third of those responding to the survey admitted that their staffs would not actually be able to recognize fraudulent activity if confronted with it. The report also disclosed that over half of the surveyed organizations had established policies and guidelines for dealing with fraud-related behavior. This is an important finding. While the number of victim organizations is still significant, more organizations are doing more about it.

Troubling, however, was the study's findings that some 85 percent of the worst frauds were by insiders on the payroll. This corresponds to the experience of this paper's author regarding large-scale identity theft. What seems to be true is that the more access employees are granted, the greater potential exposure of losses for the employer. The reader will be served remembering this when designing a prevention strategy.

Identity thieves often work in one or more of the following ways:

1. They open new credit card accounts, using the victim's name, date of birth, and Social Security number. When they use the credit card and don't pay the bills, the delinquent account is reported on the victim's credit report and collection efforts against the victim ensue.
2. They call the victim's credit card issuer and, pretending to be them, change the mailing address on the credit card account. Then the imposter runs up charges on the account. Because the bills are being sent to an incorrect address, the victim may not immediately realize there's a problem.
3. They establish cellular phone service in the victim's name or use the victim's identity to rent or purchase real estate.
4. They open a bank account in the victim's name and write bad checks on that account.

Regardless of what is done with stolen identity, the criminal must first obtain it. As indicated above, the Internet is not the primary source of identities that are stolen and misused. Most are stolen from employers. Because employers typically maintain personal information on large numbers of people (usually employees),

attractive targets exist. Employers are also sometimes careless. Improperly storing information or failing to properly protect it, will give thieves easy access to large volumes of personal information without incurring significant risk. Stealing from employers also does not require one to disguise an IP address, redirect e-mail, recruit and trust an unscrupulous Internet Service Provider, or slink around in an electronic underworld. In many instances, the thief needs only access to the data and a means to remove it.

Once removed, the data is then repackaged or parsed. It ultimately finds its way to the criminals that misuse it. To the surprise of many, criminal networks exist that broker and distribute such information at the wholesale level. Eventually, the personal data is "retailed" to someone capable of using it to commit criminal mischief.

Identity Theft Terminology

Flagging. Identity thieves look for the raised flags on mailboxes. They take letters addressed to creditors that may contain checks and personal information. The thieves then "wash" checks and write their own name into the "Pay to the order of" line, and cash the check. It may take months to discover this form of identity theft.

Skimming. Skimming involves the use of a small electronic device to capture personal account information from debit or credit cards. Skimmers can be hand-held or affixed to ATM machines.

Dumpster Diving. Identity thieves search discarded trash for pre-approved credit card applications or other personal financial documents, and then use the information therein to make purchases.

Phishing. These attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, Social Security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers, and credit card companies, phishers are able to convince up to 5 percent of recipients to respond to them. The responding party is then asked to provide passwords and/or personal information which are then later used to commit crimes.

Prevention

While it appears clear that ID theft is pervasive and costly, it seems unclear what to do about it. While lawmakers hastily write new laws restricting access to public records, security professionals suggest that the key to preventing ID theft is already in the hand of the many potential victims.

Here is what the leading security experts recommend:

1. Keep credit cards, personal identification, and passwords in a safe place.
2. Never carry more credit cards or cash with you than you need at any particular time.
3. Report the theft of credit cards or personal identification immediately.
4. Carefully examine your credit card bills and look for charges that may not be yours.
5. If you must give your credit number over the telephone, ensure no one is eavesdropping.
6. Secure your mail. Obtain a mailbox which locks and is tamper-proof.
7. Destroy or safely store all credit card offers, receipts, and bills when finished with them. Shred documents containing sensitive information.

Although the public's concern about ID theft and the information they share while online is well placed, security experts say consumers should also be concerned about what they put in the mail. Here's what to do to protect yourself and your checks:

1. Never make checks payable to *Cash*.
2. Protect deposit slips. A common scam is to deposit worthless checks into your account and get some of the deposit back as cash.
3. Order your checks from your bank. Mail-order checks are often less expensive but typically are easier to alter than bank checks.

4. Pay all bills electronically. Most major banks offer electronic payment services. The convenience is safe and saves time and money.
5. Take your mail containing checks directly to the Post Office. Do not leave them in your mailbox for pickup.
6. Sign checks with indelible black ink. Do not use felt-tip pens or pencil.
7. Keep unused checks in a safe place. Destroy all unused checks from closed accounts.
8. Review your bank statements carefully. Notify your bank immediately if you suspect someone has altered or forged one of your checks.
9. Protect your signature. Use your real signature for checks and important documents; use another for forms, questionnaires, and other routine documents.
10. Report suspicious transactions to your bank immediately. The sooner the bank is aware of problem, the sooner it can investigate it and take corrective action.

Protecting Computers

Combine a readily available cracking application with a simple dictionary file and chances are any hacker could crack most of the passwords protecting your computer. As simple as it sounds, this type of "brute force" attack is one of the most common among hackers.

Password cracking doesn't always have to take a high-tech approach to be successful. Finding a sticky note on a computer or under a keyboard is fairly simple. Because most passwords are so simplistic, crackers often use tools that literally try every word in the dictionary. Add a hybrid module and this same program starts adding numbers and symbols to these words. According to security experts at Carnegie Mellon University, well over a million passwords have been stolen on the Internet.

Ineffective passwords include common words, the same words spelled backwards, or words with numbers added at the end. Users who are comfortable with a password will often start off with the word, and when prompted monthly to change their password, will simply add a digit. So what starts in January as "Snoopy" ends up in December as "Snoopy 12." Avoid family members' names, pets' names, and Social Security numbers.

An effective strategy is to use a combination of upper and lower case letters in conjunction with symbols and numbers. Some examples might be:

Time + effort = $

IThinKThere4Im!

$howMeThe$

Protecting E-mail

Most cyber-users know e-mail messages are neither secure nor private. But privacy advocates have recently issued a new warning that e-mail may be less confidential than people thought. A recent First Circuit Court of Appeals decision suggests that e-mail's mode of transmission—hopping from computer to computer—does not fit the definition of "electronic communications" in federal wiretap laws. If so, the privacy protections that were once thought to exist when using e-mail may not exist at all. In response, security and legal experts have issued their own warnings:

1. Do not send messages that, if compromised, would embarrass you or your organization.
2. Read your e-mail service provider's privacy statement. Ensure it promises that your messages will not be read by the provider or shared with others without your permission.
3. Consider using encryption software. A Google search while writing this paper for the term, *encryption software* yielded approximately 3,030,000 results.
4. Do not use instant messaging (IM) for confidential communications.
5. Before giving away an old computer, remove the hard drive and destroy it.

Summary

Identity theft is less likely to occur from online activities than by traditional means, such as

losing or having your wallet stolen, stolen mail, or dumpster diving. Researchers report that computer crime accounts for only 11.6 percent of all identity theft in 2004, while 68 percent occurs from paper sources. And while employers are not expected to provide an impenetrable island of safety for their employees or those with whom they do business, they should take reasonable and appropriate steps to protect personal information.

Organizations should create policies and practices that protect sensitive information. Supervisors and managers should enforce those policies consistently and investigate all credible allegations of theft or other misconduct. Employers should use training and education to inform employees of their responsibilities and obligations. Individuals should also take more responsibility for protecting their personal information.

Eugene F. Ferraro

INTERVIEWING WITNESSES

A witness is any person, other than a suspect, who has information concerning an incident. Victims, complainants, accusers, laboratory experts, and informants are simply types of witnesses.

The Victim

In some instances the nature of an incident or the victim's condition as a consequence of the incident can prevent an interview, at least a timely interview. When a business is the victim, an interview is made of a person representing the business. In almost every case, the person interviewed will be the person in charge of the department affected by the incident such as the custodian of a stockroom from which valuable computer equipment disappeared.

Although we can normally expect a victim to be cooperative, we cannot expect the information to be highly reliable. A victim may be overly eager to please, or may inflate the severity of the incident as a means to obtain sympathy or a larger insurance payoff. The investigator also has to guard against the possibility that a victim may be the guilty party.

When a victim is not cooperative, it may be due to fear of retaliation by the offender. Uncooperativeness can also stem from fear of publicity, or a belief that the amount of personal effort in cooperating exceeds the value of bringing an offender to justice.

Direct and Indirect Witnesses

A direct witness is an eye-witness, i.e., a person who saw the incident under investigation. Eye-witnesses are not always known or easily available. It may be necessary to learn the person's name, find him, and then hope he will cooperate. The investigator's task is made more difficult when an eye-witness actively seeks to avoid identification or contact.

An indirect witness is a person who did not see the incident but has valuable information such as the whereabouts of a suspect before and after a violation was committed, or heard the suspect make certain remarks, or knows the location of physical evidence.

Forensic specialists are indirect witnesses. These are persons that evaluate physical evidence and are qualified to give expert and impartial testimony in court. As a general rule, forensic specialists prepare their own statements, which are in the form of laboratory reports. These reports become addenda to the investigator's final report of investigation. When a laboratory report is unclear, the investigator should interview the specialist that made the examination.

A special kind of witness is the informant. Informants are persons who, for pay or other consideration, furnish information. The identity of the informant is usually protected. Interviewing an informant is done much differently than with other witnesses. The place of the interview is likely to be clandestine and the details are taken down in notes as opposed to a formal written statement.

The Complainant

The person who makes the initial report is called a complainant. A complainant can be the victim or a person close to the victim. The motivation of a complainant may not always be honorable. A person may make a report for revenge, to divert suspicion, or self-glorification.

Conducting the Interview

The rule rather than the exception is that an investigator will have very little time to prepare for interviews of non-suspect persons. Persons who are not immediately contacted after the occurrence of an incident may become entirely unavailable at a later time, and when the interval is long, details begin to slip from memory.

The investigator should fix in mind all that is currently known, pay particular attention to specific details, especially those that have not become public knowledge and may therefore be known only to the offender.

Background knowledge of the person to be interviewed will enable the investigator to select a suitable questioning technique. An understanding of the interviewee's connection to the incident helps the investigator evaluate the accuracy and truthfulness of information offered. Knowing something about the interviewee also helps the investigator establish rapport. Examples of background facts include age, place of birth, nationality, address, educational level, habits, companions, prior arrests and convictions, and hobbies.

If the incident is a criminal violation, an investigator who knows the elements of proof for the crime is better prepared to ask questions that bring out the relevant facts. For example, if the law requires that proof be shown of the suspect's use of a dangerous weapon, the investigator is alerted to the need to obtain a detailed description of the weapon in order to establish that a weapon was used and that it was capable of causing serious injury. In complex cases, the investigator can prepare a set of questions to consult during the interview. The questions should be formulated to reveal critical points but still allow the interviewee to freely talk.

Care should be taken not to overestimate or underestimate the interviewee as a potential source of information. Preparation in the context used here is essentially self-preparation, especially of the mind. The investigator readies himself for an encounter with an individual who may be friendly or hostile, communicative or reticent, full of facts or devoid of facts, truthful or lying. The best start that an investigator can make is to have a thorough grasp of case facts, know something about the person, and know what information is necessary to bring the case to a successful conclusion.

Although it is always useful to talk to a witness as soon as possible after an incident, it is sometimes more valuable to postpone an interview until other facts have been determined. Interviews that are scheduled in a logical sequence will permit the investigator to build upon information obtained previously and to avoid re-interviewing persons in order to fill missing gaps or remove contradictions.

Generally, cooperative witnesses can be interviewed first with uncooperative witnesses put on hold until a fuller understanding of the case has been obtained. Also, it might be desirable to delay an interview until physical evidence has been examined or records checked.

It is appropriate to interview witnesses at times and places of their convenience, except when there's a chance the witness may be a suspect or accomplice. The relaxed, psychologically comfortable atmosphere of the witness's office may help the investigator obtain valuable information in a paced, unrushed interview. There is, of course, no objection to conducting a non-suspect interview at the investigator's office if that is the desire of the witness.

The situation is different with hostile and reluctant witnesses. If resistance is anticipated, it is to the investigator's advantage to conduct the interview in an environment psychologically comfortable to him. When an uncooperative witness objects to being interviewed at the investigator's office, a neutral meeting place might be in order.

At the start of an interview, the investigator should make a courteous introduction using his/her correct name and title. The interviewee should be asked to do the same. If there's any doubt about identity, picture identification should be requested.

A quick introduction gives an appearance of haste. A few minutes spent in a proper introduction can pay off. Of even greater importance is the fact that an introduction provides an ideal opportunity for the investigator to assess the interviewee and select an appropriate interviewing technique. A good introduction also affords the interviewee time to overcome nervousness and relate to the investigator as a person.

The closing moments of the introduction should be used to make a general statement about the case without disclosing any of the specific facts. This not only sets the stage for discussions which follow, but also removes the possibility that the interviewee will later claim to be uninformed as to the nature of the inquiry.

What is meant by rapport? In the context used here, rapport is the condition of harmony or agreement that allows a free flow of communication.

The attitude and actions of the investigator during the initial moments of an interview will determine success or failure. The first few minutes almost certainly determine the tenor of the session. The investigator should be friendly, but professional. The objective is to get the interviewee into a talkative mood, and to guide the conversation toward the interviewee's knowledge of the case. Where possible, the interviewee is encouraged to tell the complete story without interruption.

There is usually no requirement to have an observer present during a non-suspect interview. When an investigator feels, however, that the person to be interviewed may have some guilt, it is appropriate to have another person present. When a woman is interviewed, either as a suspect or non-suspect, it is good practice to have another person present (preferably a female) or hold the interview in an open room or semi-public area. This affords some protection from a later accusation of sexual impropriety.

An interview observer should remain neutral, unless planned otherwise. Too many persons present during an interview, or even a single antagonistic person, can cause a statement to be later challenged on the grounds it was obtained under duress.

Conclusion

In the business environment, interviewing is the rule where interrogating is the exception. The term "interrogation" can conjure up visions of coercion and intimidation, and is largely unacceptable for that reason alone. Experienced corporate investigators typically care less; for them, a well conducted interview can be just as productive as an interrogation.

John J. Fay

KINESICS

Kinesics is the study of body language and is based on the behavioral patterns of nonverbal communication. Body language can include any non-reflexive or reflexive movement of a part or all of the body. Body language can be particularly revealing when a person communicates an emotional message to the outside world. It is said that actions speak louder than words, and it's not what you say, but how you say it that counts.

To understand this unspoken body language, kinesics experts often have to take into consideration cultural and environmental differences. The average man, unschooled in cultural nuances of body language, often misinterprets what he sees.

Some have called body language an unconscious signal, such as widening of the pupil when the eye sees something pleasant. Often the swiftest and most obvious type of body language is touch. The touch of the hand, or an arm around someone's shoulder, can spell a more vivid and direct message than dozens of words, but such a touch must come at the right moment in the right context.

We act out our state of being with nonverbal body language. We lift one eyebrow for disbelief. We rub our noses for puzzlement. We clasp our arms to isolate or protect ourselves. We shrug our shoulders for indifference, wink one eye for intimacy, tap our fingers for impatience, slap our forehead for forgetfulness. The gestures are numerous. While some are deliberate and others almost deliberate, there are some, such as rubbing under our noses for puzzlement or clasping our arms to protect ourselves, that are mostly unconscious.

No matter how crowded the area in which we humans live, each of us maintains a zone or territory around us, an inviolate area we try to keep for our own. How we defend this area and how we react to invasion of it, as well as how we encroach into other territories, can all be observed and charted, and in many cases used constructively. These are all elements of non-verbal communication. This guarding of zones is one of the first basic principles. How we guard our zones and how we intrude into other zones is an integral part of how we relate to other people.

When you are at close intimate distance you are overwhelmingly aware of your partner.

For this reason, if such contact takes place between two men, it can lead to awkwardness or uneasiness. It is most natural between a man and a woman on intimate terms. When a man and a woman are not on intimate terms, the close intimate situation can be embarrassing.

We use body language to communicate approval of someone's closeness. Aside from the actual physical retreat of going somewhere else, there will be a series of preliminary signals such as rocking, leg swinging, or tapping. These are the first signs of tension, which are saying, "You are too near, your presence makes me uneasy."

The next series of body language signals are closed eyes, withdrawal of the chin into the chest, and hunching of the shoulders. They say, "Leave me alone. You are in my space." When these signals are ignored, the person will usually move to another location.

Many people who act violently have said that their victims "messed around with them," although the victims had done nothing but come close to them. The victim had intruded on the assailant's personal space.

Defending personal space involves using the proper body language signals or gestures and postures, as well as a choice of a location. Body language and spoken language are dependent on each other. Spoken language alone will not give the full meaning of what a person is saying, nor for that matter will body language alone give the full meaning. If we listen only to the words when someone is talking, we may get as much of a distortion as if we listened only to the body language.

An awareness of someone else's body language and the ability to interpret it create an awareness of one's own body language. As we begin to receive and interpret the signals others are sending, we begin to monitor our own signals and achieve greater control over ourselves, and in turn function more effectively. Research suggests there are no more than about 30 traditional American gestures. There are even fewer body postures that carry any significance in communication and each of these occurs in a limited number of situations.

Of all parts of the human body that are used to transmit information, the eyes are the most important and can transmit the most subtle nuances. While the eyeball itself shows nothing, the emotional impact of the eyes occurs because of their use and the use of the face around them. The reason they have so confounded observers is because by length of glance, by opening of eyelids, by squinting, and by a dozen little manipulations of the skin and eyes, almost any meaning can be sent out.

The most important technique of eye management is the look, or the stare. With it we can often make or break another person, for example, by giving him or her human or non-human status. Simply, eye management boils down to two facts. One, we do not stare at another human being. Two, staring is reserved for a non-person. We stare at art, at sculpture, at scenery. We go to the zoo and stare at the animals. We stare at them for as long as we please, as intimately as we please, but we do not stare at humans if we want to accord them human treatment.

With unfamiliar human beings, when we acknowledge their humanness, we must avoid staring at them, and yet we must also avoid ignoring them. To make them into people rather than objects, we use a deliberate and polite inattention. We look at them long enough to make it quite clear that we see them, and then we immediately look away. We are saying, in body language, "I acknowledge you," and a moment later we add, "But I won't violate your privacy." A look in itself does not give the entire story, even though it has a meaning. A word in a sentence has a meaning too, but only in the context of the sentence can we learn the complete meaning of the words.

If we are to attempt to interpret body language, then we must assume that all movements of the body have meaning. None are accidental. Extreme caution must be used to avoid misinterpretation of behavior. We cannot rely on any one instance to make a valid inference. All the body signals must be added up to a correct total if we are to use body language effectively.

Perhaps scratching the nose is an indication of disagreement, but it may also be an indication of an itchy nose. This is where the real trouble in kinesics lies, in separating the significant from the insignificant gestures, the meaningful from the purely random, or from the carefully learned.

We must approach kinesics with caution and study a motion or a gesture only in terms of the total pattern of movement, and we must understand the pattern of movement in terms of the spoken language too. The two, while sometimes contradictory, are also inseparable.

There is a surprising lack of uniformity in body movement. Working class people will give certain interpretations to movements, and these interpretations will not apply in middle class circles.

A body movement may mean nothing at all in one context, and yet be extremely significant in another context. For example, the frown we make by creasing the skin between our eyebrows may simply mark a point in a sentence or in another context it may be a sign of annoyance or, in still another context, of deep concentration. Examining the face alone will not tell us the exact meaning of the frown. We must know what the frowner is doing. No single motion ever stands alone; it is always part of a pattern. We must examine other cues accompanying a particular movement to accurately assess its meaning. Body language can serve as a means of communications if we have the ability to understand it.

Kinesics and Interrogation

With respect to interrogation, the psychological assumptions underlying the kinesics technique are:

- The deceptive person who experiences physiological changes resulting from his fear of detection will regard the interrogation as a threat, i.e., an intensification of fear.
- The deceptive person's fears intensity during interrogation at moments when questioning focuses on investigative details having the greatest immediate threat to the person's self-preservation.
- The deceptive person is aware of physiological changes occurring in the body and may do or say things as a means to disguise the changes.
- The deceptive person who does not experience fear during an interrogation will not exhibit any of the body movements that can be associated with deception.

The guilty subject has a general fear of an investigation. When the investigation calls for an interrogation of the guilty subject, the fear intensifies. During the interrogation, the guilty subject's immediate anxieties and apprehensions are directed toward those questions that present the greatest threat to exposure. In other words, a guilty person's fear of detection increases as the investigation proceeds from the general to the specific.

The deceptive person will tune in on questions that indicate trouble or danger. His mental attention and sensory organs are anticipating particular questions. There is a tendency to tune out questions that are of a lesser threat and to concentrate on questions that lead to exposure.

The interrogator cannot always know what questions will produce fear in the guilty subject. As the line of questioning moves closer to the issues having the greatest psychological threat to the subject, there is likely to be an increase in the number and intensity of deceptive behaviors.

Following are tips for spotting deceptive behaviors:

- Determine the demeanor or combination of demeanors that represent a "normal" pattern for the individual being interrogated. Look for changes in the pattern.
- Look for consistency of behavioral signals. One quick change in behavior is not conclusive. Repeated changes from the "normal" pattern may be indicative of deception.
- Look for timing of behavioral signals. Look for deceptive signals or changes from the "normal" pattern when a fear-provoking question (stimulus) is asked. Anticipate a body language response, keeping in mind that it might be a delayed response.
- Interpret deceptive signals in clusters rather than as single observations.
- Look, listen, and follow intuition. Concentrate on watching and listening, and don't be afraid to follow your "sixth sense" in evaluating your observations.
- Compare the suspect's behavior in relation to case details and evidence. Ask yourself, "Is the outward personality of the suspect consistent with the nature of the offense, the manner in which the offense was committed, and the motive?"
- Do not challenge the suspect by telling him the specific indicators of deception you have observed. Although it may be a good practice to point out the forms of personal behavior that contradict a suspect's denial, this should be done in a general way without getting into specific detail. This tends to sidetrack the interrogation and give the suspect an opportunity to explain the symptoms as innocent phenomena.

- Prepare a checklist for recording deceptive signals. As soon as possible following or during a break in the interrogation, the checklist can be used to record the deceptive signals. The checklist can help the interrogator remember behavioral signals which otherwise would have gone unremembered and can serve as a guide in conducting further interrogation.

The interrogation must be planned, and modified during execution, so as to move the line of questioning toward issues that have the greatest threat. A successful interrogation is dependent to a very large degree upon the ability of the interrogator to force the guilty subject to focus upon specific, self-threatening issues.

Not all persons who react deceptively are in fact deceptive or guilty. Some people will respond with deceptive behavior signals when subjected to accusatory questions regardless of guilt. A person of this type is sometimes referred to as a guilt complex reactor. The guilt complex reactor is extremely rare. The basic emotionality of the subject being interrogated must be taken into consideration in determining his or her potential for reaction. Generally speaking, the severity of the offense is proportional to the reaction potential of the guilty subject.

At the beginning of an interrogation the subject will undergo a temporary heightening of the emotional state. This is true whether the subject is guilty or not guilty. As the interrogation proceeds, the heightened emotional state of the innocent subject will decrease.

The reaction potential of a deceptive subject is conditioned by the number and intensity of previous interrogations; and the reaction potential of the deceptive subject may be low or beyond observation if emotional fatigue is present. The innocent apprehensive subject (not necessarily the guilt complex reactor) may give random erratic reactions.

Physiological Roots of the Kinesics Technique

The human body is composed of cells. The cells are organized into tissues, organs, and systems.

The general composition of the human body is specialized both structurally and functionally to accomplish the basic life processes. These processes are: ingestion, digestion, absorption, respiration, excretion, growth, and reproduction.

There are nine major systems of the body. You can be assisted in remembering the nine major systems by the acronym MCRENDERS. The letters of this acronym are the first letters of the major systems of the body, i.e., muscular, circulatory, respiratory, endocrine, nervous, digestive, excretory, reproductive, skeletal.

The nervous system consists of conscious functions and unconscious or autonomic functions. The autonomic functions are actions that occur without our conscious knowledge. They control the actions of the intestine and other digestive organs, the heart and blood vessels, the adrenal glands and the sweat glands. The autonomic functions are performed by motor fibers only. There are no sensory nerve fibers involved.

The autonomic functions are of two types, sympathetic and parasympathetic, which are carried out through nerve fibers in certain body organs. If an organ has sympathetic nerve fibers, it also has parasympathetic fibers. The effects of the two types of fibers operate in exact opposition. For instance, the operation of the heart is accelerated by sympathetic nerves and slowed by parasympathetic nerves. The principal purposes of the autonomic subsystem are to direct the ordinary housekeeping of the body (parasympathetic) and to prepare the body for stress (sympathetic).

The sympathetic function strengthens the defenses of the body against various dangers such as lack of water, temperature extremes, and enemy attacks. By preparing the body to fight or run, the sympathetic function produces certain

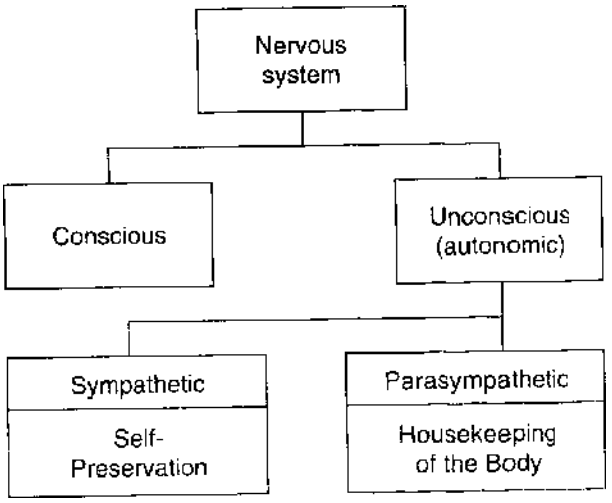


Figure 15. The nervous system responds to various stimuli.

physiological reactions over which the individual has little control.

The parasympathetic function causes the body to slow down, and in general manages body organs that permit the body to operate under normal, non-stressful conditions. With respect to interrogation, the significance of the parasympathetic function is that a person under stress (for example, a guilty subject) will very likely exhibit deceptive signals that are identifiable.

Deceptive Signals

What is meant by the term deceptive signal? It may be helpful to think of a deceptive signal in terms of the stimulus/response or action/reaction concept. The interrogator provides a stimulus or action that produces a response or reaction from the person being interrogated. The stimulus might be a verbal statement, a remark, a question, or the showing of a photograph or piece of evidence, or even a nonverbal message sent by the interrogator in the form of a gesture or facial expression. For every stimulus or action, one should expect a response or reaction. Sometimes the response is barely perceptible or entirely concealed. Even when the response is small or hidden, the interrogator can draw from this observation some indication of deception. The capacity for deceptive signals is present in every deceptive subject; it is up to the interrogator to provoke the signals through skillful interrogation and then to interpret the signals as he or she sees them.

Now that we know the origin of deceptive signals, what are they and what do they look like? Deceptive signals are varied and numerous. A few examples are: finger tapping; licking the lips; movement of the Adam's apple; rapid speech, stammering; eye movement; changes in pitch, tone, and volume of the voice, etc. You should note that the foregoing examples include signals that are delivered in two modes: a visual mode and an audio mode. It is not correct to think of deceptive signals as being in the visual mode only. Many strong signals are sent through speech and it is not the content of speech that is always significant, but the manner of speech. Deception may be indicated not in terms of what is said, but in the way it is said.

General Demeanor. This term has meaning with respect to the person being interrogated. A general demeanor is the outward manner, attitude, or bearing of a person in relation to other persons. For our purposes, we can regard a general demeanor as the attitudinal framework within which deceptive signals are manifested. For example, a nervous demeanor is manifested by such deceptive signals as wringing of the hands, slurred and rapid speech, knee jerking, fidgeting, and nail biting. In other words, it is the totality of behaviors (deceptive signals) that convey a general demeanor. Finally, it is possible for one or more demeanors to be exhibited simultaneously or in transition. It is possible for a person to be nervous, fearful, and angry simultaneously, or be in the process of making a transition from these attitudes to demeanors that are defensive, evasive, and complaining. These demeanors are consistent with each other and reflect a discernible pattern. Some demeanors, however, are not consistent. Demeanors that are apologetic and overly polite are inherently contradictory to demeanors that exhibit fear and anger. A shift of this type would represent a radical change in behavior worthy of notice by the interrogator.

Major Body Movements. Many of the gestures and mannerisms of the deceptive subject are somewhat difficult to detect because they are of short duration and hard to catch. This is not the case with gross body movements in which the subject may shift his entire body, move within the interrogation room, or even attempt to leave the room.

TABLE 2. Body Movements Are Easy to Spot but Not Always Easy to Interpret

When a Suspect Displays	
These facial expressions...	These may be the meanings...
Fear	Deception. May be difficult to question
Anger	Truthful person wrongly accused
Defiance	Deception. Difficult to interrogate
Acceptance	Progress is being made
Pleasure	Nervousness or flippant defiance
Blank	Deception. Suspect is careful and wary

Smaller gestures or mannerisms, such as facial expressions, occur at the same time a major body movement is occurring. In fact, the subject may undertake a major body movement at the moment he is aware of a revealing facial expression; the body movement is meant to mask an expression he wishes to hide. Sometimes a body movement will be used to thwart a growing physiological change which, of course, is the product of a threat posed by the interrogator and the line of questioning.

A deceptive subject is likely to want to place his chair as far as possible from the interrogator without giving the impression that he fears the interrogator. The deceptive subject will also want to place some substantial object between him and the interrogator; for example, position his chair so that a desk or table separates the interrogator from the suspect. The intervening object becomes something of a psychological barrier behind which the suspect finds some degree of protection.

Preparation of the interrogation room in advance will help the interrogator maintain control over major body movements of the suspect. These arrangements can include:

- Seat the suspect between the interrogator and the interrogator's partner, and away from the exit door.
- Place the suspect's chair close to the interrogator's chair.
- Select for the suspect a chair that is not too high, too wide, nor too comfortable.

The timing of a major body movement is important. What was asked or what was said immediately prior to the major body movement may have significance with respect to fears of the suspect. Keep in mind that sitting postures are preceded and followed by major body movements. The major body movements may also be revealing, especially when interpreted in conjunction with a sitting posture.

TABLE 3. All Facial Expressions Have Meaning

When the Deceptive Subject Performs	
These major body movements...	These may be the meanings...
Shift of the torso and gross movement of head and limbs	Internal conflict or fear of the subject being discussed
Stand up	Desire to change the subject
Attempt to leave	A bluff tactic
Move chair away	Retreat from fear

Gestures. A gesture is an activity created by the suspect to reduce tension. Most gestures are unconsciously performed. A deceptive person is likely to perform gestures without realizing it.

Some gestures are consciously initiated and deliberate. A conscious gesture may be an attempt by the deceptive subject to mislead the interrogator; it may be a gesture meant to mask an emotion the suspect wishes to conceal. Consciously controlled gestures should be viewed with suspicion. They are also indicative of a clever, willful, and self-controlled person who is determined to prevail over the interrogator.

Gestures are numerous and varied. As a group, they outnumber other forms of nonverbal communication. Gestures can be a rich source of information concerning the true feelings of a person, and can be placed into four categories: those that symbolize, those that relieve tension, those that mask inner tension, and those that protect.

Facial Expressions. A single facial expression by itself should not be interpreted to conclusively indicate deception. More meaning can be derived by observing the variety of facial expressions displayed by a person being interrogated, especially as the expressions relate to particular questions.

The main value of facial expressions is the help they give in identifying the emotional state of the person being interrogated. They can be likened to road signs that guide the traveler to the desired destination. The interrogator watches for them and alters the route to the final destination.

A problem with interpreting facial expressions is the difficulty of differentiating between genuine and false expressions. Also, a person has greater conscious control over the face than any other part of body. The interrogator should ask himself if a particular facial expression is appropriate to the question posed, or if the expression is consistent with similar questions posed previously.

Of the several features constituting the face, the eyes are most important simply because of the large number and variety of eye expressions. Some researchers suggest that about 90 percent of all facial expressions come from the eyes.

When two people are engaged in a normal conversation, between 30 and 60 percent of the time is maintained in eye contact. The implication of this fact is that abnormal or unusual eye contact occurs below or above the 30 to 60 percent range. For the professional investigator, interrogation is a normal, sometimes routine function. For the deceptive subject, interrogation may be a first-time or occasional experience. The deceptive subject therefore finds himself in an abnormal situation. Excessive eye shifting and looking away from the interrogator indicate deception. Prolonged eye contact may suggest that the suspect is aware of eye signals as body language and is over-compensating.

Also, a deceptive subject who is uncooperative and arrogant may stare at the interrogator to show his defiance and throw the interrogator off balance.

Eye contact is related to unwritten social rules. The character of eye contact will vary among persons of varying cultural and ethnic backgrounds. What could be regarded as deceptive eye contact by a person during questioning may in fact be perfectly normal within the person's cultural and ethnic environment.

The best way for an investigator to develop expertise in recognizing nonverbal language by cultural and social type is to study the many varieties of people engaged in routine daily activities. Although different cultures have different rules that govern eye contact, studies indicate that most cultures have these points in common:

- An extended gaze between two persons is normally a challenge and an invasion of privacy.
- Emotionally disturbed persons have abnormal eye contact.
- Strangers will look at each other longer in conversations than persons who know each other.
- The speaker in a conversation is regarded as having dominance and has greater freedom in keeping or breaking eye contact with listeners.

A study of body language is a study of the mixture of all body movements from the very deliberate to the completely unconscious, from those that apply only in one culture to those that cut across all cultural barriers. We are born with the elements of a nonverbal communication. We can make hate, fear, amusement, sadness, and other basic feelings known to other human beings without ever learning how to do it. Nonverbal language is partly instinctive, partly taught, and partly imitative.

Leon C. Mathieu

Sources

Archer, D. and Akut, R.M. "How Well Do You Read Body Language?" (*Psychology Today*, October, 1977).

Goleman, D. People Who Read People. (*Psychology Today*, July, 1979).

Goleman, D. The 7,000 Faces of Dr. Ekman. (*Psychology Today*, February, 1981).

Inbau, F.E. and Reid, J.E. 1967. *Criminal Interrogation and Confessions*. Baltimore: Williams and Wilkins Company.

O'Hara, C.E. 1970. *Fundamentals of Criminal Investigation*. Springfield, IL: Charles C. Thomas.

Plutchik, R. A Language for the Emotions. (*Psychology Today*, February, 1980).

Schurenberg, E. Sheepish Smiles Don't Hide Embarrassment. (*Psychology Today*, November, 1981).

Specter, A. and Ketz, M. 1967. *Police Guide to Search and Seizure, Interrogation and Confession*. Philadelphia: Chilton Books.

Swanson, C.R., Chamelin, N.C., and Territo, L. 1977. *Criminal Investigation*. Santa Monica, CA: Goodyear Publishing Company.

Tobias, M.W., and Peterson, R.D. 1972. *Pretrial Criminal Procedure*. Springfield, IL: Charles C. Thomas.

PHOTOGRAPHY IN INVESTIGATIONS

Photography is an essential tool for the investigator. As a tool it enables the investigator to record the evidence of a crime. Photographs made of a crime can be stored indefinitely and retrieved when needed. There is no other process that can record, retain, and recall criminal evidence as effectively as photography.

Photographs are also a means of communication. They tell something about the objects photographed or the scene of a crime that is helpful in clarifying the issues when testimony is given in court. Because photographs are meant to communicate information honestly, the investigator-photographer has a great responsibility. His photographs must portray a situation as it would be observed by anyone who stood in the same position as the camera and viewed the scene from where the photograph was made.

Photographs by themselves are not substantive evidence. Photographs accepted in court must be attested to by a person who saw the scene and can truthfully state under oath that the photographs accurately represent what the person saw at the scene. In the ordinary, nonlegal field of photography, only the finished photographic print is of interest, but in criminal investigative work, all photographic procedures are subject to review and inspection by the court. Obviously, this rigid requirement makes it imperative that investigative photography conform to high standards of quality and ethics.

Photographic Techniques

The most frequent factor contributing to inferior photographic results is over exposure of the negative. This produces soft, grainy images of low contrast and brightness. Exposure recommendations for any given film are based upon the requirement for a so-called average subject. This is a photographic subject that contains light, medium, and dark tones. If a photographic subject consists of all light tones, the subject would be very low in contrast and high in brightness. If the recommended speed for a given film for use with a so-called average subject were ASA 80, the fact that the photographic subject contained all light tones means that less exposure is required. If, on the other hand, the subject consisted of all dark tones, the subject is low in contrast and is therefore reflecting very little light. In this case the investigator-photographer adjusts his equipment to provide more exposure. For example, less exposure would be called for when the photographic subject is a nude body of a white bleached blonde lying on white sand; or at the other extreme, highly blackened wood at the scene of arson will require greater exposure than an average subject in order to obtain shadow detail. In short, the investigator must learn to evaluate his photographic subject by contrast and brightness, and to make appropriate adjustments.

Another common difficulty is a dirty lens. Dirt and oxidation may form on the back surface of the lens, as well on the front. Both the outer and inner surfaces of the camera lens should be checked frequently and cleaned when necessary.

Loss of detail in photographic prints is a common problem. This is usually caused by movement of the camera at the time the shutter is released. This problem can be reduced through the use of a rigid tripod and a fast shutter speed.

Sharpness, or image definition, suffers when the diaphragm of a lens is stopped down, i.e., adjusted from its largest opening to its smallest opening. When a lens is stopped down, three things happen:

- The aperture is reduced and less light passes through during a given period of time.
- The depth of field increases.
- The image definition improves to a point (although in a few special cases the definition softens at the smallest apertures).

To obtain good definition the following general rules apply:

- Use a tripod whenever possible.
- For outdoor photography with a hand-held camera, set the aperture as required by film and light conditions, and use a faster shutter speed.
- For flash pictures use an electronic flash.

Photography plays a vital part in establishing points of proof for certain types of crime, particularly crimes involving physical violence. The characteristics and location of relevant objects need to be captured in accurate detail and permanently recorded until presented at trial. If a crime scene is altered through carelessness or haste, it can never be restored to its exact original condition, and as a consequence, vital elements of proof may be lost forever. In addition, the significance of certain aspects of a crime scene may not be apparent, although later they may powerfully affect a guilty or innocent conclusion. The first step in the investigation of any crime

is to photograph completely and accurately all aspects of the scene before any of the objects of evidence are removed or otherwise disturbed. Photographs should also be made after victims have been removed. It is much better to take too many photographs rather than not enough.

When taking photographs at a scene, the objective should be to record the maximum of usable information in a series of photographs that will enable the viewer to understand where and how the crime was committed. The term *crime scene* refers not just to the immediate locality in which the offense occurred, but relates also to adjacent areas where important acts took place immediately before or after the commission of the offense. The number and types of photographs will be determined by the total circumstances of the crime.

Photographs of the broad area of the locale of the crime scene should be supplemented by closer shots of portions of the crime scene so that important details are made apparent. Each object within an area should be photographed so that it can be located readily in the overall pictures, thus enabling the viewer to gain a clear picture of its position in relation to other objects at the scene and to the overall scene.

Procedures. At an indoor crime scene location at least four photographs will be required to show the room adequately. Moving in a clockwise direction, each photograph will overlap a portion of the preceding photograph so that 360 degree coverage is made of the area. Obviously, when an area is large or contains many pieces of evidence, the number of photographs will be far in excess of the minimum four. Medium-distant, as well as close-up, photographs should be made of important objects. Two lenses are usually sufficient for crime scene photography. A wide-angle lens is useful for interior photographs and a normal angle lens for outdoor photographs.

Lighting. Indoor lighting is rarely satisfactory for photographic purposes. The investigator must take into account the need for additional illumination. Depending upon the size, shape, and location of a crime scene, the investigator may elect to provide additional illumination through photoflood, photoflash, or electronic flash equipment.

Markings in the Field of View. Because a court may object to the presence of rulers or similar measuring devices in a crime scene photograph, it is recommended that the photographs be taken first without the marker and then with the marker. Measuring devices that are used to show the relative size of and distances between objects should be placed in such a manner that they will not obscure any important part of the evidence.

The final determination of the admissibility of photographs is made in court and often depends upon legal points that have little to do with the investigator-photographer. The investigator's contribution to the admissibility of photographs relates mainly to their accuracy and to the custody of them prior to trial.

All evidence must be protected and ac counted for from the time it is found until it is offered in evidence. The law requires that the person presenting physical evidence in court be prepared to prove such evidence could not have been altered or replaced. This means that an investigator must be able to account for negatives and prints at all times. This does not present any great problem when photographs taken by the investigator are developed, printed, and secured within in-house resources. Problems can arise, however, when film is processed or placed into the custody of an outside agency. When this occurs, chain of custody procedures must be followed.

To be admissible, a photograph must be verified by a person who viewed the scene, object, or person represented in the photograph, and is able to state that it is an accurate and truthful representation. In other words, the photograph must be a fair and accurate representation of the scene of the crime. Depending on the desires of the court, this issue can be addressed through testimony given by the investigator who took the photographs or by some other competent witness present at the time the photograph was taken.

An investigator who is required to give testimony regarding photographs he or she took at a scene should be prepared to testify regarding safekeeping of negatives and prints, and to explain the details of the photographic procedures followed. An understanding of the rules of evidence and an application of common sense is usually sufficient to ensure that photographs taken in connection with a crime will be admissible in court.

John J. Fay

POLYGRAPH TESTING

The term "polygraph" literally means "many writings." The name refers to the manner in which selected physiological activities are simultaneously recorded. Polygraph examiners may use conventional instruments, sometimes referred to as analog instruments, or computerized polygraph instruments.

A polygraph instrument collects physiological data from at least three systems in the human body. Convoluted rubber tubes that are placed over the examinee's chest and abdominal area record respiratory activity. Two small metal plates, attached to the fingers, record sweat gland activity, and a blood pressure cuff, or similar device records cardiovascular activity.

A typical polygraph examination will include a period referred to as a pre-test, a chart collection phase, and a test data analysis phase. In the pre-test, the polygraph examiner completes required paperwork and talks with the examinee about the test. During this period, the examiner discusses the questions to be asked and familiarizes the examinee with the testing procedure. During the chart collection phase, the examiner administers and collects a number of polygraph charts. Following this, the examiner analyzes the charts and renders an opinion as to the truthfulness of the person taking the test. The examiner, when appropriate, will offer the examinee an opportunity to explain physiological responses in relation to one or more questions asked during the test. It is important to note that a polygraph does not include the analysis of physiology associated with the voice. Instruments that claim to record voice stress are not polygraphs and have not been shown to have scientific support.

Users of the Polygraph

The three segments of society that use the polygraph include law enforcement agencies, the legal community, and the private sector.

Law Enforcement Agencies

- Federal law enforcement agencies
- State law enforcement agencies
- Local law enforcement agencies, such as police and sheriff's departments

Legal Community

- U.S. attorney offices
- District attorney offices
- Public defender offices
- Defense attorneys
- Parole and probation departments

Private Sector

- Companies and corporations that fall under the restrictions and limitations of the Employee Polygraph Protection Act of 1988 (EPPA)
- Private citizens in matters not involving the legal or criminal justice system
- Attorneys in civil litigation

Critics of Polygraph

One of the problems in discussing accuracy figures and the differences between the statistics quoted by proponents and opponents of the polygraph technique is the way that the figures are calculated. At the risk of over simplification, critics, who often don't understand polygraph testing, classify inconclusive test results as errors. In the real life setting an inconclusive result simply means that the examiner is unable to render a definite diagnosis. In such cases a second examination is usually conducted at a later date.

To illustrate how the inclusion of inconclusive test results can distort accuracy figures, consider the following example: If 10 polygraph examinations are administered and the examiner is correct in 7 decisions, wrong in 1 and has 2 inconclusive test results, we calculate the accuracy rate as 87.5 percent (8 definitive results, 7 of which were correct). Critics of the polygraph technique would calculate the accuracy rate in this example as 70 percent (10 examinations with 7 correct decisions). Since those who use polygraph testing do not consider inconclusive test results as negative, and do not hold them against the examinee, to consider them as errors is clearly misleading and certainly skews the figures.

Pre-Employment Test Accuracy

To date, there has been only a limited number of research projects conducted on the accuracy of polygraph testing in the pre-employment context,

primarily because of the difficulty in establishing ground truth. However, since the same physiological measures are recorded and the same basic psychological principles may apply in both the specific issue and pre-employment examinations, there is no reason to believe that there is a substantial decrease in the accuracy rate for the pre-employment circumstance. The few studies that have been conducted on pre-employment testing support this contention.

While the polygraph technique is not infallible, research clearly indicates that when administered by a competent examiner, the polygraph test is one of the most accurate means available to determine truth and deception.

Polygraph Screening in Police Agencies

The Employee Polygraph Protection Act of 1988 (EPPA) prohibits most private employers from using polygraph testing to screen applicants for employment. It does not affect public employers such as police agencies or other governmental institutions.

False Positive and False Negative Errors

While the polygraph technique is highly accurate, it is not infallible and errors do occur. Polygraph errors may be caused by the examiner's failure to properly prepare the examinee for the examination, or by a misreading of the physiological data on the polygraph charts. Errors are usually referred to as either false positives or false negatives. A false positive will occur when a truthful examinee is reported as being deceptive; a false negative when a deceptive examinee is reported as truthful. Some research indicates that false negatives occur more frequently than do false positives; other research studies show the opposite conclusion. Since it is recognized that any error is damaging, examiners utilize a variety of procedures to identify the presence of factors which may cause false responses, and to insure an unbiased review of the polygraph records; these include:

Protection Procedures

- Assessment of the examinee's emotional state
- Medical information about the examinee's physical condition
- Specialized tests to identify the overly responsive examinee and to calm the overly nervous
- Control questions to evaluate the examinee's response capabilities
- Actual analysis of the case information
- Pre-test interview and detailed review of the questions
- Quality control reviews

Remedies

If a polygraph examinee believes that an error has been made, several remedies are available:

- Request a second examination
- Retain an independent examiner for a second opinion
- File a complaint with a state licensing board
- File a complaint with the Department of Labor under EPPA
- File a request for the assistance of the American Polygraph Association

Prohibited Inquiries

Personal and intrusive questions have no place in a properly conducted polygraph examination. Many state licensing laws, the Employee Polygraph Protection Act, as well as the American Polygraph Association, have stated that an examiner may not inquire into any of the following areas during pre-employment or periodic employment examinations:

- Religious beliefs or affiliations
- Beliefs or opinions regarding racial matters
- Political beliefs or affiliations
- Beliefs, affiliations or lawful activities regarding unions or labor organizations
- Sexual preferences or activities

In a law enforcement pre-employment polygraph examination, questions can only focus on job related inquiries, such as the theft of money or merchandise from previous employers, falsification of information on job applications, use of illegal drugs during working hours, and

criminal activities. The test questions are limited in the time span they cover, and all are reviewed and discussed with the examinee during a pre-test interview. There can be no surprise or trick questions.

In a specific issue polygraph examination, the relevant questions focus on the particular act under investigation.

Use of Results

According to the various state licensing laws and the American Polygraph Association's Standards and Principles of Practice, polygraph results can be released only to authorized persons. Generally those individuals who can receive test results are the examinee, and anyone specifically designated in writing by the examinee, the person, firm, corporation, or governmental agency that requested the examination, and others as may be required by law.

Employee Polygraph Protection Act

On December 27, 1988, the Employee Polygraph Protection Act (EPPA) became law. This federal law established guidelines for polygraph testing and imposed restrictions on most private employers. This legislation only affects commercial businesses. Local, state and federal governmental agencies (such as police departments) are not affected by the law, nor are public agencies, such as a school system or correctional institution. In addition, there are exemptions in EPPA for some commercial businesses. These are:

- Businesses under contract with the federal government involving specified activities (e.g., counterintelligence work).
- Businesses whose primary purpose consists of providing armored car personnel, personnel involved in the design, or security personnel in facilities which have a significant impact on the health or safety of any state. Examples of these facilities would be a nuclear or electric power plant, public water works, or toxic waste disposal.
- Companies that manufacture, distribute, or dispense controlled substances.

In general, businesses cannot request, suggest, or require a job applicant to take a pre-employment polygraph examination. A business can request a current employee to take a polygraph examination or suggest to such a person that a polygraph examination be taken but only when specific conditions have been satisfied. However, the employer cannot require a current employee to take an examination, and if the employee refuses, the employer cannot discipline or discharge the employee based on the refusal alone.

Guidance for the Employer

The American Polygraph Association conforms to U.S. Department of Labor guidance relating to polygraph tests for employees. This information is intended to assist in complying with the EPPA. Employers are encouraged to develop their own forms, use forms that bear their company name, and have the forms approved by legal counsel. When the polygraphist is a private sector person, the employer should demonstrate that the investigation is specific to the loss. In addition, the employer should:

- Show that the investigation is currently in progress.
- Show there is an identifiable economic loss to the employer.
- Abide by the EPPA.
- Provide the employee with a written statement that includes an identification of the company and the working location of the employee.
- Describe to the employee the incident under investigation.
- Name the location of the loss.
- Name the specific amount of the loss.
- Name the type of loss.
- Determine that the employee had access to the loss. (Access alone is not sufficient grounds for polygraph testing.)
- Have a valid reason to suspect the employee.
- Give to the employee a written statement signed by a person authorized to legally bind the employee. The binding statement must be retained by the employer for at least 3 years following the investigation. Read the statement to the employee. Have the employee acknowledge understanding

of the statement. If the employee agrees, the employee should then sign a timed and dated statement in the presence of a witness.

- Notify the employee in writing not less than 48 hours in advance (exclusive of weekends or holidays) as to the time and date of the scheduled polygraph test. If the test is to be conducted at a location other than the place of employment, directions to the location should be provided in writing.
- Conduct a follow-up interview of the employee before an adverse action is taken, during which the employee is told why the adverse action is to be taken.
- Keep all records for at least 3 years.
- Do nothing to require or otherwise coerce the employee to waive his or her right to refuse taking the polygraph test.

When the investigation is loss-related and conducted by a public sector employee, such as a law enforcement or government agent, all of the above apply before conducting a polygraph test. Test results cannot be released to the employer when the test is conducted by a public sector agency.

A $10,000 penalty can be applied for each violation of the EPPA. For this reason alone, the employer should verify that the polygraphist is licensed (if applicable) and possesses professional and experiential competence.

Guidance for the Polygraph Examiner

- Give to the employer a copy of EPPA guidelines and explain it in a face-to-face conference.
- Do not participate with the employer in determining if there is reasonable cause to believe a loss has occurred and who should or should not be tested.
- Prior to interviewing or conducting a polygraph exam, obtain from the employer copies of the relevant documents such as the advance notice and explanation of rights. Also obtain photo identification of the person to be tested.
- At the time and place of a polygraph test, give to the examinee a verbal and written explanation of polygraph test procedures. Obtain from the examinee a written acknowledgment of same.
- Read and explain the examinee's right to refuse taking the test. Obtain from the examinee a written acknowledgment of same.
- If the test is to be taped or viewed, such as through a one-way mirror, advised the examinee of these conditions.
- When one or more tests are conducted in the context of the EPPA, conduct not more than 5 polygraph tests in one day.
- When one or more tests are conducted in the context of the EPPA, keep a log of the company name, examinee names, and times of polygraph tests conducted in the course of one day.
- Administer a single test for not longer than 90 minutes.
- Give to the examinee a form that identifies the questions to be asked during the test. Ask the examinee to answer the questions in writing and sign the form. Retain the original of the form.
- If so required, possess a license issued for use in the state where the test is to be conducted.
- Inform the examinee of test results and allow the examinee to give reasons for the results.
- Inform the examinee in writing of your opinion as to deception or non-deception.
- Base your opinion on test results, and not behavior.

Inform the employer of your opinion but only in the context of the matter under investigation. Do not include extraneous information.

- Keep all documentation for at least 3 years.
- Provide a copy of charts and questions, and an original report to the employee upon request.
- Provide a copy of charts and questions, and an original report to the employer when test results indicate deception.
- Provide the U.S. Department of Labor and other authorized agencies with a copy of charts and questions, and an original report within 72 hours upon request.
- Carry a minimum of $50,000 or equivalent professional liability coverage.

Even when an employer holds an exemption to the EPPA, the EPPA guidelines should be followed.

REQUIREMENTS IMPOSED ON THE PRIVATE SECTOR EMPLOYER

1. The polygraph test must be relevant to an ongoing specific investigation involving an economic loss to the employer.

2. The employee must have had access to the property, money, or area central to the investigation. Access can mean physical presence or special knowledge, such as the combination to a safe.

3. The employer must have a reasonable suspicion that the employee was involved in the incident under investigation. Reasonable suspicion goes beyond having access, and incorporates such factors as a witness's statement, suspicious behavior on the part of the employee, or contradictions between the employee's statements and documented records.

4. At least 48 hours prior to the examination the employer must give to the employee a written statement which describes the nature of the loss and the investigation, as well as the basis for the employer's "reasonable suspicion."

5. The Employee Polygraph Protection Act (EPPA) requires that the polygraph examiner follow certain procedures in the administration of the examination. Examples of these include a minimum duration of 90 minutes for the examination, and reading a statement to the employee that enunciates certain rights under the Act.

6. The employee to be tested cannot be required to take the test.

Qualifications of a Polygraph Examiner

A person is qualified to receive a license as a polygraph examiner when he or she:

- Presents evidence of good moral character.
- Has passed an examination to determine competency.
- Holds an academic degree at the baccalaureate level from an accredited educational institution.
- Has satisfactorily completed 6 months of study in the detection of deception, as prescribed by applicable rule.

Sources

American Polygraph Association. 2006. <http://www.polygraph.org/faq.htm>

Employee Protection Act. 2006. http://www.admpoly.com/eppahome.htm

U.S. Department of Labor. 2006. http://www.dol.gov/esa/regs/compliance/posters/eppa.htm

QUESTIONED DOCUMENTS

A set of absolute rules cannot be applied to the conduct of any investigation, and no two cases involving questioned documents will be exactly alike. The implication? Use the information in this section as a guide and be prepared to season it with liberal amounts of common sense.

An exemplar is a collected writing obtained from an individual at the request of another, usually an investigator. It is a sample of an individual's handwriting or hand printing, and relates to a case under investigation in which the individual is somehow involved. A standard is a known writing made during the normal course of an individual's activity, usually prior to the incident under investigation. Hand-printed entries on an employment application form and signatures on canceled checks are examples of standards.

Standards are particularly valuable to the document examiner because they allow comparison with characteristics that appear in exemplars. If a disguise is attempted by the

writer of exemplars, the examiner may be able to detect the attempt in the examination of standards. Exemplars and standards are often called known writings because authorship is known.

In addition to linking a suspect to the questioned text or signature, exemplars and standards are often used to eliminate the victim from consideration as the author. They are also valuable in determining attempts to simulate or trace the writing of the victim. Exemplars and standards should be collected from the victim in every case, even when the indications of guilt point strongly elsewhere.

Obtaining Known Writings

Exemplars are made from dictation without allowing the writer to view the questioned document. No assistance should be given to the writer as to spelling and punctuation. An error in spelling or punctuation that appears in both the questioned document and an exemplar would be noteworthy. As each exemplar is completed, the investigator removes it from the writer's sight. The objective is to not make it easy for the writer to create a consistent disguise among all the exemplars by copying one after the other.

Each exemplar is placed on a separate piece of paper. The shape and size of the paper corresponds to the shape and size of the questioned document. The writer is directed by the investigator to place the exemplar in the same area or space as it appears on the questioned document. If the questioned writing is on a form, such as a credit application, the investigator would want to obtain a quantity of the same credit application stock. Blank forms would be handed one at a time to the writer. An absolutely incorrect procedure would be for the writer to put all of the exemplars on one piece of paper, one immediately below the other.

Exemplars need to be made of all writings that appear on the questioned document. For example, if a check is the questioned document, the writer should be asked to write not only the maker's signature, but the "Pay to the Order of" entry, the date, and the check amount in words and numbers. A point to keep in mind is that a document may bear writings made by more than one person. Because a person did not write a questioned signature does not mean he or she did not write some other portion of the document. In check cases, it is not unusual for one person to fill out the check and get an accomplice to sign it.

How Much Is Enough?

This question is answered with the observation that the chances for obtaining a definitive opinion increase relative to the number of exemplars provided to the questioned document examiner. Case circumstances will sometimes dictate a need for collecting a large number of exemplars and standards. Consultation with a document examiner is recommended before making the collections. As a general rule, a greater number of known writings is required for analysis when the questioned writing is meager, and vice versa. Also as a general rule, the collected standards should reflect a mix of writings that were made just prior to and shortly after the time frame of the document in question. A signature made 10 years before or after a signature in doubt will not be very meaningful to the examiner.

Typically, a questioned signature will require the investigator to obtain 12 to 15 signature exemplars, plus 12 to 15 known signature standards. A note or letter to be examined will require two to three repetitions, depending on length, and an address on an envelope or package will require about 25 exemplars. If the questioned document is typewritten and lengthy, such as a letter, two to three repetitions of the exact text should suffice, but if the typewritten text is short, such as a signature block, at least 25 exemplars will be needed.

Because some people can write equally or nearly as well with either hand, the investigator should ask the writer at the beginning of an exemplar collecting session to provide one or two samples from each hand. If the investigator is satisfied that the writer is proficient with only one hand, further exemplars by the weak or "unaccustomed writing hand" will not be necessary. If the investigator is not satisfied on this point, exemplars from both hands should be collected. When the questioned writing appears to have been made by the weak hand, the investigator will want to obtain a sufficient number of samples made with that hand.

A questioned writing that is illegible or unreadable is called an abbreviated writing. Generally, an abbreviated writing occurs when

the author writes with speed so as to save time. A person with a long name who writes the name many times a day is likely to develop an abbreviated signature. When an abbreviated signature is questioned, the investigator should attempt to acquire standard signatures that would have been made under conditions that called for speedy writing, and also obtain exemplars under similar conditions. An investigator wanting to introduce speed into the exemplar-taking process can dictate rapidly or require so many exemplars that the writer may resort to abbreviation.

Original Documents Are Critical

A properly conducted analysis requires the examiner to work with the original document. Although remarkable advances have been made in the technology of document reproduction, the examiner cannot make definitive judgments based on a copy. Particular characteristics present on the original are simply not transferred to a copy. Indications of pressure of the writing instrument on the paper and constituents of ink are examples of characteristics that lie outside the examiner's analysis when working from a copy. A good examiner will not render unqualified opinions in such cases, and many examiners will refuse to accept work or give opinions involving reproductions.

It will happen, however, that the original of a questioned document has been lost or destroyed, leaving only a reproduction. The examiner may be asked to make an analysis with the understanding that the finding could be inconclusive, qualified, or limited.

An original is sometimes not readily available for analysis because it is an official record entrusted to a custodian whose authority does not extend to allowing replacement of an original with a certified true copy. The investigator will need to direct his request for the original to a higher level in the custodian's organization or petition a court. An alternative solution, although decidedly less desirable, would be for the examiner to conduct the analysis at the place of custody. Because the examiner utilizes equipment that is not easily transported, this approach is like bringing the hospital to the patient.

In addition to giving the examiner materials to evaluate, the investigator needs to provide certain details such as the writer's date of birth and date of death, if applicable; whether the writer was left-handed or right-handed; the duration of formal schooling of the writer; the profession of the writer; the country where the writer learned to write; the state of the writer's health on the date the questioned document was executed; the dates of execution for standards; and the date exemplars were obtained.

Selecting a Document Examiner

A Chief Security Officer or investigator in need of forensic document examination services has to differentiate between examiners who apply scientific-based techniques in the analysis of questioned writings and people who assess personalities based on handwriting. So-called graphologists and graphoanalysts will sometimes claim, often in public advertisements, the ability to judge questioned documents. More art than science, their techniques focus on writing characteristics that purport to reveal the writer's personal traits such as deceit and dishonesty.

A competent document examiner will hold diplomate status conferred by the American Board of Forensic Document Examiners (ABFDE), which is the only recognized national certifying board in this discipline. Recognition of the ABFDE is derived from the field, principally two professional organizations: the American Academy of Forensic Sciences and the American Society of Questioned Document Examiners. The ABFDE diplomate will:

- Possess a baccalaureate degree.
- Have completed a 2-year, full-time training program at a recognized document laboratory.
- Have completed an additional 2 years of full-time independent document work.
- Practice forensic document examination on a full-time basis.
- Have passed a comprehensive written and/or oral examination.

A professionally concerned examiner will attend seminars, workshop, and training courses to maintain or enhance competency. Some of the better specialized courses are offered by the U.S. Secret Service and the Federal Bureau of Investigation (FBI). Participation in professional

associations is an indicator of professional commitment. National associations of interest include the Questioned Document Section of the American Academy of Forensic Sciences, the American Society of Questioned Document Examiners, and the International Association for Identification.

A qualified examiner will own or have access to a professional library of forensic document literature and an assemblage of technical equipment such as a stereoscopic binocular microscope and hand magnifiers, an electrostatic detection apparatus for detecting and visualizing indentations on paper, a video spectral comparator for detecting differences in inks, test grids for detecting alterations to typewritten documents, and a variety of special cameras and films for documenting the examiner's findings. Finally, a very important qualification is the recognition extended to a forensic document examiner by civil and criminal courts and administrative bodies for the provision of expert witness testimony.

Checking out the credentials of prospective examiners and making a careful selection before authorizing the work may very well be the most critical activity in a case. It could mean the difference between establishing the truth of the situation in doubt, and if taken to court could mean the difference between winning and losing. At stake may be large sums in litigation costs, awards, and punitive fees. The best advice to the Chief Security Officer or investigator charged with making an inquiry is to do the homework necessary to choose a competent examiner.

Hans M. Gidion

QUESTIONING SUSPECTS

Questioning suspects requires careful planning and skillful execution. Although questioning should not follow an inflexible, predetermined script, a general "game plan" can be very helpful. Knowledge of the case enables the investigator to determine what information needs to be obtained and how much the suspect can be expected to possess. The investigator may want to prepare a list of questions and to arrange topics of discussion in a logical sequence so that the questioning session will progress smoothly and important points will not be overlooked.

Statements of witnesses and facts derived from physical evidence are carefully examined for the purpose of re-constructing the offense mentally and anticipating the suspect's admissions and denials.

The general rule is that witnesses and suspects should be interviewed as soon as possible after commission of the offense. With respect to witnesses, the value of timely interviews lies in the freshness of details and the opportunity for the investigator to obtain productive leads. Early questioning of a suspect reduces the chances for fabricating an alibi and for keeping accomplices from synchronizing their separate stories.

While speed may be helpful, hasty preparation can be counterproductive. The timing of a questioning session cannot be fixed by some absolute rule that applies in all situations. Rather, it is conducted at a time of maximum advantage to the investigator.

The session is scheduled so that other activities do not interfere. Questioning is paced and unhurried. A session can be long but not so long that duress is suggested. Duress includes conditions also such as the need for food, water, personal hygiene, and sleep.

Ideally, questioning is conducted at a place where:

- Facilities are available for recording the session.
- Secretarial assistance is available if needed.
- Observers are available if needed.
- Control of the physical environment is ensured.
- Interruptions are minimal.
- Privacy is guaranteed.

A room specifically designed for questioning is typically plain but comfortably furnished, devoid of pictures or items that can distract attention. It will have recording devices and a two-way mirror. The room will be neither so hot nor so cold as to raise contentions that information was extracted through physical discomfort. Furniture will consist of three chairs and a small table large enough to write on, but not large enough for the suspect to hide behind. Pens, pencils, forms, wastebaskets, and like items should be in place prior to beginning. If the room is equipped with a telephone, it should be disconnected or removed for the purpose of

reducing possible interruptions. Most important, any article or item in the room that might serve as a weapon should be removed.

The suspect should be seated at the side of the table. This removes a physical barrier and enables the investigator to fully observe the suspect's body language. If there is a window in the room, chairs should be arranged so that window light falls on the face of the suspect rather than the investigator. Chair arrangement should also preclude the suspect from being able to gaze out of a window.

Establishing Control and Rapport

At the beginning of the session, it must be made very clear that the investigator is in charge. This can be done in a variety of ways, for example: demonstrating an air of confidence, authority and professionalism; telling the suspect where to sit; calling the suspect by his/her last name; telling the suspect that smoking and tobacco or gum chewing is not permitted.

Establishing control and establishing rapport are two different techniques, yet they complement one another. Control, of course, is established first. After the ground rules have been laid, the process of establishing rapport can begin. Study of case materials prior to the questioning session usually reveals at least some personal aspects of the suspect such as place of residence, places frequented, marital status, job held, and perhaps an avocation or hobby. Any of these can provide opportunities to open the suspect to two-way communication. "I understand you like fishing," could be a starting point, assuming the investigator knows something about fishing.

Assessing the Suspect

With rapport comes the opportunity to assess the suspect. Productive questioning depends in large measure upon the investigator's ability to size up the suspect and choose a general approach for getting the suspect to cooperate and dealing with resistance should it arise. If the first approach does not succeed, an alternate approach should be tried. All of this is in the nature of sparring; two contestants testing and appraising each other. The investigator has the advantage for two reasons: control and familiarity with the process.

The ability to assess others is largely a matter of practical experience, even though a lack of experience can be compensated for by pure native ability and keen psychological insight. While the "sizing-up" of a suspect is essentially a subjective process, there are usually a sufficient number of facts known to the investigator that can help in judging probable guilt prior to questioning. A person can fall under suspicion through the examination of physical evidence and statements of witnesses. On the other hand, a lack of essential facts will cause some doubt or uncertainty as to probable guilt.

The Questioning Session

Once the questioning begins, the investigator and suspect are locked into a contest. The investigator will use his/her knowledge of human behavior to find a chink in the armor of the suspect. The suspect will resist and try to avoid traps set by the investigator.

At the outset, the investigator will use everything known about the suspect to form a preliminary judgment as to involvement. The tradition of questioning provides two convenient categories: the apparently guilty person and the person whose guilt is uncertain.

The Apparently Guilty Person. A direct approach is normally used to question a suspect in this category. The investigator assumes an air of complete confidence with regard to evidence or witness statements that point to the suspect; incontrovertible proof implicates the suspect beyond any doubt. The investigator assumes a brisk, accusatory manner, displays a complete belief in the suspect's guilt, and acts as if a statement is not really important because the quantity and quality of evidence already on hand is more than enough to bring the investigation to a conclusion—a conclusion that places the suspect in a difficult position. The purpose of the interview, according to the investigator, is not to establish that the suspect committed the offense—because that has already been determined—but to learn why. The meeting is nothing more than an opportunity for the suspect to tell his/her "side of the story."

The Person Whose Guilt is Uncertain. A person in this category is best questioned using an indirect approach. Questioning is designed to establish a detailed account of the suspect's activities before, during, and after the time of the offense. Facts that are definitely known can be used to test the suspect's reactions. Guilt is indicated when the suspect lies regarding a known fact. If, as the questioning progresses, the investigator becomes increasingly convinced of the suspect's guilt, the direct approach is merited.

Tactics and Techniques

The number and kinds of possible tactics and techniques are limited only by the investigator's imagination, within reason however. There are limitations to what an investigator can do or say. Constitutional safeguards, case law, appellate decisions, and a variety of other rules or procedures apply to suspect rights. A good rule of thumb to follow when deciding to employ a particular questioning tactic is to internalize this question: "Does a possibility exist that the action I take could result in an admission of guilt by an innocent person?" If the answer to the question is "yes," the tactic is out of bounds. To illustrate, assume that questioning is about to take place of a suspect whose guilt is uncertain and the offense involves a degrading act. It would be wrong for the investigator to imply that a failure of the suspect to confess would require interviewing the suspect's family and friends. If such a tactic were employed, a possibility exists for the truly innocent person to confess out of concern for family and friends.

Following are descriptions of the more common questioning tactics. In them the reader will see their applicability to different kinds of suspects in different kinds of situations.

Sympathy. A person who has committed an offense in the heat of passion is normally responsive to a sympathetic and understanding attitude. Violent offenses have emotional overtones; they are generally committed by people acting from the heat of passion, anger, revenge, or mental aberration. In the mildest of such instances, the investigator can treat offenders as rational people who, under the pressure of circumstance or extreme provocation, committed acts that are out of keeping with their true personalities. The investigator should present a rationalization of the crime by pointing out that "it could happen to anyone" and minimize the moral seriousness of the act by alluding to the frequency by which such crimes occur. The investigator can attempt to gain the confidence of the suspect, for example, by referring to similarities of good citizenship that appear to exist between them.

Sympathy can be mixed with confidence by pointing out the evidence linking the suspect to the incident. Signs of stress and nervous tension can be pointed out to the suspect as indicators of guilt.

Repugnant acts and low motives can be treated as "out of character" for the suspect. The idea is to help the suspect "save face" by putting forth an excuse. Euphemisms should be used in place of emotion-laden words like "stab" and "steal."

The sympathetic technique is also particularly useful in dealing with the first offender. A person who has not been in trouble previously is likely to respond to an understanding attitude. It is natural for a first offender to experience feelings of regret and penitence. A skilled investigator will play upon these feelings by acting considerate and helpful. In fact, a showing of warm feelings is not always false. There have been many cases where investigators, through compassion and understanding, have turned first offenders away from disrespect for laws.

Reasoning. In this technique the suspect is told that guilt is already established, or that it will be established soon, and that there is nothing else to do but make an admission. The investigator points out the futility of denying guilt. Every denial is met with logic and facts that refute the suspect's assertions. Laboratory reports, photographs, fingerprint lifts, and similar items can be very useful in convincing a suspect that lying is useless. The thrust of this technique is to appeal to the suspect's common sense.

Point Out the Symptoms of Guilt. Demeanor and verbal expressions can place a suspect in a vulnerable situation. A person who knows that the signs of guilt are apparent may be moved one step closer to an admission.

Nonverbal symptoms of guilt can be very revealing. Kinesics, the study of nonverbal communications, teaches us that the body can

communicate what we are not saying. Body positions, motions, gestures, and facial expressions are forms of silent language that convey inner thoughts. Some people find it easy to use words to mask their true feelings, but no one can completely control the body's natural reaction to intense inner feelings. While the brain can learn to lie, the body cannot.

Documenting the Session

Documenting a questioning session consists of three main phases: note taking, electronic recording, and obtaining a written statement.

Note Taking. The traditional method for documenting a questioning session is note taking. Notes do more than just create a record, they help the investigator keep track of what has been asked and answered, what remains to be asked, and what needs to be asked again. Electronic devices are far superior to note taking for recording a session but have no value in the give and take of questioning.

Handwritten notes are subject to examination by opposing counsel at a legal proceeding, and for that reason must be understandable to others. Notes that are confusing to understand or appear to be out of character for a professional, can discredit an otherwise excellent investigation.

Because suspects are inclined to conceal the truth, it bothers them to observe note taking. This can be overcome by using a third party to take notes out of the suspect's sight.

The suspect should be permitted to tell the story at least once before the investigator lifts pencil to paper. Notes are seldom taken in a fully narrative form. They tend to consist of key words that denote salient points, common abbreviations, and words compressed with the use of apostrophes. Points notated while the suspect talks usually become points for later questions that can amplify guilt or clarify facts.

Electronic Recording. The preferred recording device is the video/recorder. Video leaves little doubt as to the identification of persons present, objects examined or handled, the environment, the activities of persons present, and words said.

Video allows parties of interest to see the offender nod, shrug, and make other telling movements that convey guilt. Video can be used to capture images of the suspect re-constructing the offense through physical actions such as the way in which a security container was pried open.

The video recording should be preceded and concluded with acknowledgments by the suspect that he/she understands the purpose of the questioning and is free to leave at any time. The recorder should have a time and date generator.

Video recordings should be carefully kept in their entirety, along with a chain of custody form. Except for chain of custody, the same is true for notes and any other recordings such as stenographic transcripts.

Written Statements. The most convincing type of statement is the one in which a suspect personally writes the confession and signs it. Statements exclusively prepared by suspects are relatively uncommon because of the difficulty in persuading suspects to write them.

On the other hand, the investigator may not wish a suspect to write the statement because in so doing critical points can be omitted. The investigator may prefer instead to prepare a typed statement and have the suspect sign it.

When preparing a typed statement, common sense is called for. The text of the statement should reflect the general vocabulary of the suspect. A confession obtained from a suspect having a sixth grade education deserves skepticism when it includes large words and highly complex sentences. If a suspect speaks with profanity, the typed statement should contain profanity. As much as possible, the actual sentences spoken are included, although they may not necessarily appear in the same order given by the suspect.

It sometimes happens that a suspect will refuse to sign a statement of any type, even though an understanding may have been reached prior. If the suspect declines to sign, the investigator should try to obtain a verbal acknowledgment in the presence of an observer. If the suspect refuses to do even this, the investigator should prepare a personal statement that describes the entire session in detail. For this task, notes are essential.

Conclusion

Questioning skill is acquired through training, practice, and experience. For some, the skill comes

with difficulty and for others it comes easily. The important point is that it can be acquired.

Skill is not simply verbal. It requires study prior to the questioning session, making good choices as to when and where to hold the session, assuring that the questioning environment is arranged to personal advantage, "reading" the suspect, concentrating on what is important, taking notes, closing the session with a signature or acknowledgment, and assuring that recordings are marked for identification at a later time.

John J. Fay

Sources

Bennett, W. and Hess, M. 1998. *Criminal Investigation, 5th Edition*. New York: West/Wadsworth.

Berg, B. 1999. *Policing in Modern Society*. Boston: Butterworth-Heinemann.

Inbau, F. and Reid, J. 1967. *Criminal Interrogation and Confessions*. Baltimore: Williams and Wilkins.

Montgomery, R. and Majeski, W. 2002. *Corporate Investigations*. Tucson: Lawyers and Judges Publishing.

O'Hara, C. 1970. *Fundamentals of Criminal Investigation*. Springfield: Charles C. Thomas.

Sennewald, C. and Tsukayama, J. 2001. *The Process of Investigation, 2nd Edition*. Boston: Butterworth-Heinemann.

Specter, A. and Katz, M. 1967. *Police Guide to Search and Seizure, Interrogation and Confession*. Philadelphia: Chilton Books.

Stuckey, G. 1968. *Evidence for the Law Enforcement Officer*. New York: McGraw-Hill.

Swanson, C., Chamelin, N., and Territo, L. 1997. *Criminal Investigation*. Santa Monica: Goodyear Publishing.

Tobias, M. and Peterson, R. 1972. *Pre-Trial Criminal Procedure*. Springfield: Charles C. Thomas.

QUESTIONING TECHNIQUES

Security professionals like to make a distinction between "interview" and "interrogation" and, of course, there are differences. For example:

- An interview is non-accusatory; the interrogation is.
- An interview has a free-flowing dialogue; the interrogation does not.
- An interview can be held at many places; the interrogation is done in an environment controlled by the questioner.
- An interview does not have to be perfectly private; the interrogation does.
- Interviewing is the mode for questioning cooperative non-suspects; interrogating is the mode for questioning suspects and hostile witnesses.
- An interview is not lengthy; an interrogation can be.
- An interview is characterized by friendliness; an interrogation is often hostile.
- An interview is unstructured; an interrogation is highly structured.
- An interview requires some planning; an interrogation requires extensive planning.
- In an interview, note taking is okay; in an interrogation it may not be.

An interview is the questioning of a person who has or is believed to have facts of official interest. The person questioned usually gives an account of the incident under investigation or offers information concerning a suspect. The person being interviewed is usually a witness, victim, or complainant. An interrogation, on the other hand, is the questioning of a person suspected of having committed an offense, or of a person who is reluctant to make a full disclosure. The person being interrogated is a suspect, or may be a reluctant witness.

Both definitions have one thing in common; each seeks to obtain information through questioning. The differences arise in the manner of questioning and the type of person being questioned. It is not unusual for an information-gathering session to switch back and forth between interview and interrogation, depending on the degree of cooperation or hostility encountered.

The most consistently available and most valuable sources of information in the majority of inquiries are the people involved. The inquiry obtains information from people for a variety of reasons; initially to establish the facts of an incident, including determination of whether or not an incident actually occurred. During initial phases it is important to verify information given by other persons connected with the case, or tie in facts gleaned from an examination of physical evidence. Information collected from the victim, complainant, or witnesses may lead to identification of offenders and accomplices.

Prompt and properly conducted interviews can produce investigative leads, additional physical evidence, and develop background information regarding motives, habits of the offender and other details that contribute to a fuller understanding of the incident. Interviews can also lead to a discovery of unreported offenses, or connect other persons to other incidents. The function of interviewing has many important uses.

An investigator charged with conducting an investigation of a criminal act must become thoroughly familiar with the elements of proof pertaining to the crime committed. A working knowledge of criminal law helps the investigator formulate questions, the answers to which will satisfy the elements of proof. In the questioning of a suspect, for example, knowledge of what is required to establish criminal intent will assist the investigator to steer questioning toward motivation and premeditation.

The Questioning Session

After rapport has been established and the interviewee is communicating, the investigator must guide the conversation in productive directions. For those interviewees who require no stimulation to continue talking, the investigator can wait until the story has been told, review it out loud, and ask clarification of confusing points. Matters that were not touched upon can be covered at the end. For some persons, occasional prodding is necessary to keep a conversation moving. A common mistake of the fledgling interviewer is the tendency to interrupt or dominate a conversation to such a degree that the interviewee is not permitted to tell the story. Knowing when to ask a question is every bit as important as knowing what to ask and how to ask. Following are some questioning techniques for non-suspects.

Ask One Question at a Time. Too many questions at one time can be confusing for any person. Questions should be segregated one from each other, and the investigator should not proceed to the next question until the fullest answer possible has been obtained. It is important also to pose questions intermittently. A constant series of questions is less desirable than a conversation punctuated by occasional questions inserted to clarify or stimulate.

Use Simple Questions. Long and complex questions lead to confusion and irritation. Legal terms and security jargon are unfamiliar to many people. If the person being interviewed does not understand the question, the answer cannot be accurate. Also, some people when confronted with a misunderstood question will become defensive and difficult to deal with.

Avoid Implied Answers. There is not much point in asking a question that provides its own answer. Suggesting answers defeats the whole purpose of the interview. An example of a question with an implied answer is "Was the weapon a caliber 0.38 revolver?" A better question might be "What kind of a weapon was it?"

Avoid "Yes" and "No" Questions. The idea in interviewing is to encourage elaboration. Short answers can omit valuable facts. While a "yes" or "no" reply is very specific, they are not always absolutely accurate and can be misleading in the absence of details.

Avoid Embarrassment to the Interviewee. Remarks, gestures, or facial expressions that can be interpreted as ridiculing should be avoided. When dealing with the non-suspect interviewee, it is usually not difficult to separate deliberate misrepresentation from unintentional mistakes. If honest errors are made, they should be resolved with tact and courtesy.

Control Digressions. While it is extremely important to get an interviewee to talk, it is equally important to confine talking to the issues at hand. Long, rambling discourses are time consuming and unproductive. The investigator must keep the discussion from drifting into irrelevant matters and excessive detail. The use of precise questions is effective in limiting the range of information being offered. Questions that are highly specific require answers that are not easily shifted to side issues. A technique called shunting can also be useful in controlling digression. A shunting maneuver allows the investigator to bring the interviewee back to the original line of discussion. A shunt might occur by saying, "Let's return to that point where you said the suspect was wearing a baseball cap." The shunt is an inoffensive interruption because it appears to rise out of an interest in what the person has said.

Radiate Confidence. How many times have we been infected by the enthusiasm of others? People who think and act in positive ways influence those around them. The investigator who looks and acts in a confident manner projects an image of competence. The comments and questions of the investigator are expressed in positive terms and avoid negative comments like, "I don't know if there is much we can do in this case, but I need to talk with you anyway." Comments of that type practically guarantee failure. It would be far better to say, "I intend to get to the bottom of this matter, and I am sure you will be able to help."

Concluding the Session

When the investigator terminates the interview of a non-suspect person, it is appropriate to display appreciation for cooperation received. This applies not only to interviewees who have been completely cooperative from the very start, but also to those who initially or occasionally had to be motivated to furnish information. It is not unusual during the closing phase of an interview for the individual to request confidentiality of information provided. Although it is never a good practice for an investigator to release official information, absolute assurances can never be given concerning releases of information.

The closing of an interview is not necessarily the termination of communications between the investigator and the interviewee. On the contrary, an effective closing can result in the acquisition of valuable information. A person who may not have been fully cooperative during the body of the interview may feel safe in saying something after questioning has apparently ceased. Pertinent facts that may have been suppressed during the interview might be disclosed as the interview is being ended. Details that escaped the investigator earlier can be brought to the surface even while making a farewell hand-shake.

John J. Fay

RAPE

The security professional holds a special responsibility for helping employees prevent being assaulted. Rape is a particularly odious form of assault. Fortunately, it is a crime susceptible to prevention, largely through engaging in avoidance tactics and knowing what to do if attacked.

Although the legal definition of rape will vary from state to state, it is generally accepted that rape is first and foremost a crime of force. The rapist uses or threatens to use violence in what is essentially an exercise of power. The primary motive of the rapist is not to attain sexual pleasure, but to feel a sense of superiority by dominating the victim.

Rape has no boundaries. Males have been victims as well as females. Anyone, regardless of age, race, economic status, and physical appearance can be victimized. Victims have included infants, mentally retarded persons, and the elderly.

Rape is also unlimited as to time and place of occurrence. It is not something that happens mainly at night or in ghetto areas. Rapes occur at all times of the day in the poorest and wealthiest sections of cities, suburbs, and rural areas all across America.

Many rapes take place in the victim's home and frequently the rapist is there by invitation. This is so because the rapist is likely to be a friend, relative, or work associate. In some cases, he is an estranged husband or lover, and in about 9 of every 10 reported cases, is of the same race as the victim.

Violence is an element of the act and only about 3 of 10 incidents will involve the use of a weapon. Only very infrequently will a rape end in murder. This is not to suggest that the crime is any less serious, but it does point to the high probability that the victim will survive.

There has never been any truth to the notion that rape is an invited crime, meaning that the victim invited rape because of the way she dressed or behaved. The idea that the rapist was provoked by the victim's sexual advances reflects a dishonored and mistaken view that rape is motivated by sexual desire.

There is also little evidence to support the proposition that women use accusations of rape as a means of obtaining revenge. On the contrary, there is evidence to show that women accusers often suffer further harm by being stigmatized in their communities and abandoned by friends and loved ones.

Another disturbing reality is that a rapist will usually continue to rape until caught and

removed from society. The only effective remedy is for the victim to report the crime and assist in the investigation and prosecution. This can be difficult and unpleasant for the victim, but is essential in preventing repeat occurrences of the crime.

Setting Up Personal Defenses

The rapist, like most criminals, will prefer the "easy target," that is to say, a woman who has the appearance of vulnerability. If the rapist can be made to believe that a particular woman would be difficult to overcome, he will look elsewhere for easier prey. A good defense, then, is to display strength—not in the physical sense, but in character and personality. How is that done? It is done through expressions of self-confidence, capability, and control of events. Strength can be shown by actions and appearance. It is also manifested in what is said and how it is said.

Assertiveness is one of the most powerful indicators of strength. It is largely verbal in nature and is an excellent weapon to use when confronted with a threatening situation. A verbal response that says "no" without any doubt or hesitation could be all that's required to defuse a potentially dangerous encounter.

If a simple refusal is not sufficient, a woman should not be afraid to make a scene. Embarrassment is an acceptable alternative to the risk of the possible consequences of giving in. A woman can use her voice to attract attention, to make people nearby aware of her need for help, and to tell them how they can help, such as by staying close or calling the police.

From childhood, people are taught to be courteous and friendly. These are valuable teachings, but they should not have priority in situations that pose danger. Traits that are trusting and passive give encouragement to the rapist.

John J. Fay

REID'S NINE STEPS OF INTERROGATION

An interview is a non-accusatory information gathering conversation during which the investigator develops investigative and behavioral information that will help to assess the veracity of the statements made by a suspect, victim, or witness. When the results of the interview and subsequent investigation indicate that the subject is withholding information, then an interrogation may be appropriate. However, it is very important to conduct a non-accusatory interview before any interrogation takes place for a number of reasons. During this interview process the investigator gains important insight with respect to the subject's psychological characteristics; possible reasons or motives for committing the act in question; fears or concerns regarding the discovery of their participation; and, the process allows the investigator to establish an image of professionalism and competency by giving the subject the opportunity to tell their story to an objective listener. An interrogation should only be conducted when the investigator is reasonably certain that the subject has not told the truth during the interview.

In contrast to the interview process, interrogation is an accusatory procedure designed to persuade the subject to tell the truth about information that they are believed to be withholding. While interrogation is most often used with an individual suspected of committing a crime, a victim who is believed to be fabricating a crime or a witness who is believed to be withholding relevant information may also be the subject of an interrogation. The process seeks to obtain an acknowledgment that the person did not tell the truth in an earlier statement to conceal guilt or to protect the guilty party.

Privacy is one of the principal psychological factors contributing to the successful outcome of an interview or interrogation. Typically, the investigator and the subject sit in similar chairs, directly facing each other approximately 5 feet apart and without any physical barrier (such as a desk) between them. The investigator should minimize distractions, such as phones ringing, the disturbance of others interrupting the session, open views out of windows, etc.

The Accusatory Interrogation

As a result of many years experience, primarily on the part of the staff of John E. Reid and Associates under the guidance of the late John E. Reid, the interrogation process has been formulated into nine structural components—the nine steps of criminal interrogation. These nine steps are presented in the context of the interrogation of suspects whose guilt seems definite or

reasonably certain. It must be remembered that none of the steps is apt to make an innocent person confess and that all of the steps are legally as well as morally justifiable.

The Positive Confrontation. Following the non-accusatory interview, the investigator leaves the room. After several minutes, the investigator returns carrying an investigative file, opens it, and confronts the subject with facts that clearly point to the subject's deception. ("Jim, the results of our investigation clearly indicate that you did [issue]."). This type of accusation is made only when the subject's guilt is very apparent. Otherwise, the statement should be less direct. ("Jim, the results of our Investigation indicates that you have not told me the complete truth about [issue]."). Following the confrontation, the questioner pauses to evaluate the subject's reaction to the statement, then repeats the statement. Following this, the questioner places the investigative file aside, sits down directly opposite the subject, and makes a transition from being an accuser to a sympathetic and understanding person.

Theme Development. The next step is to present themes that are "moral justifications" for the subject's criminal behavior. One way of doing this is to place moral blame for an illegal activity on another person or an outside set of circumstances. This appeals to a basic aspect of human nature. Most people tend to minimize responsibility for their actions by placing blame on someone or something else. In a credit card fraud case, for example, the questioner might suggest that the subject was not paid enough by the employer or that someone left the card out where it was an open invitation to use. Other moral justifications include unusual family expenses, desperate financial circumstances, a friend came up with the idea, retribution for an argument, and drug or alcohol dependence.

The questioner presents the moral justification in a sympathetic and understanding way. An interest in working with the subject to resolve the problem breaks the ice. The justification is presented in an unbroken monologue that minimizes the subject's opportunity to voice denials.

Handling Denials. In fact, the more often the subject denies guilt, the more difficult it becomes for the subject to admit guilt later. Therefore, during theme development the questioner interjects a blocking statement whenever the subject attempts to verbalize an "I didn't do it" plea. Denials from the guilty subject are often preceded by permission phrases such as, "Can I say one thing?" or "If I could only explain" or "But sir, if you'll just let me talk." Each of these permission phrases will be followed by the denial, "I didn't do it." When the investigator hears these permission phrases he should interject a comment, such as, "Jim, hold on for one second" or "Sue, wait just a minute" and then return to the development of the theme.

Innocent subjects rarely use permission phrases before denying guilt. Instead, the innocent subject will, with any display of etiquette, promptly and unequivocally maintain innocence. An innocent subject remains steadfast in the assertion of innocence and never moves past the denial stage. On the other hand, many guilty subjects will abandon the strategy of denial, which is a defensive tactic, and move to an offensive strategy that offers objections.

Overcoming Objections. An objection is a stated reason why a subject would not or could not have committed the crime under investigation. Most guilty subjects will make objections that fall into general categories. The first of these are trait objections such as, "I wasn't brought up that way" or "I'd be too scared to do something like that." The other category of objections includes factual objections that allege lack of opportunity or access to commit the crime. Examples of factual objections are, "I don't even have the combination to the safe," "I don't own a handgun," and "I was with my girl friend that night."

While both types of objections offer feeble reasons supporting a claim of innocence, most objections will have some basis in fact. For example, the subject in fact was probably not brought up to rob gas stations and in fact was probably with his girl friend at some point in time on the night of the robbery. Because of the factual basis for most objections, the questioner generally does not refute them. To do so would only encourage an argument or discussion that would break the flow of theme development. Rather, when the subject offers an objection the questioner first rewards it, perhaps with a statement such as "I'm glad you said that" or "You're absolutely right, I was aware of that before I talked with you about

this." The objection is then incorporated into the theme. For example, a subject who states, "I'd be too scared to do something like this" could be told, "I'm glad you said that because it tells me that this crime was out of character for you and that you probably had never done anything like this before in your life." By handling objections in this manner the subject is made to realize that this offensive tactic will be ineffective in convincing the questioner of innocence. At this stage most subjects psychologically withdraw and begin to focus mentally on the prospects of impending punishment.

Keeping a Subject's Attention. Following the objection stage, the guilty subject often becomes pensive, apathetic, and quiet. It is most important during this stage that the questioner procure and focus the subject's attention on the theme (i.e., the psychological justification for the subject's behavior). Through this process the subject's thoughts will be diverted away from the impending punishment (which only serves to reinforce the resolve to deny guilt). To procure the subject's attention, the questioner draws nearer to the subject. A closer physical proximity helps direct the subject's thoughts to what the questioner is doing and saying. The questioner now begins to channel the theme down to the probable alternative components.

Handling a Subject's Passive Mood. At this stage, the subject may cry, which is often an expression of remorse. Many other subjects do not cry, but express their emotional state by assuming a defeatist posture—slumped head and shoulders, relaxed legs, and a vacant stare. In order to facilitate the impending admission of guilt, the questioner intensifies the theme presentation and concentrates on the psychological justification for the unlawful act.

Presenting an Alternative Question. The alternative question is one in which the questioner presents two incriminatory choices concerning some aspect of the crime. Elements of the alternative are developed as logical extensions of the theme. If the theme focuses on contrasting behavior that is impulsive or spur-of-the-moment versus planned or premeditated acts, the alternative question is, "Did you plan this thing out or did it just happen on the spur of the moment?" Either choice is an admission of guilt. The alternative question should be followed by a statement in which the investigator indicates he believes the good side of the alternative: "I'm sure it was just on the spur of the moment, wasn't it?" The alternative question should be based on an assumption of guilt, not on a yes or no proposition, such as, "Did you do this or didn't you?" A misphrased question invites denial. The first admission of guilt is established when the subject accepts either of the offered alternatives. The way now stands clear to develop the admission into a corroborated confession.

Having the Subject Relate Details. Once the alternative question is answered, the investigator responds with a statement of reinforcement such as, "Good, that's what I thought all along." Essentially, this is a statement that acknowledges the subject's admission of guilt. Following this, the objective is to obtain a brief oral review of the basic sequence of events, while obtaining sufficient detail to corroborate the subject's guilt.

Questions asked at this time should be brief, concise, and clear, calling only for limited verbal responses from the subject. It is premature to ask all-encompassing questions like, "Well, just tell me everything that happened." Furthermore, questions should be open-ended and devoid of emotionally charged terminology. Once the subject has offered a brief verbal statement about the crime sequence, the questioner should ask detailed questions to obtain information that can be corroborated by subsequent investigation. After this full verbal statement is complete, it may be necessary to return to the subject's choice of alternatives or to some other statement previously made. Discussions along these lines tend to shed light on the subject's motive, purpose, and intent at the time of the crime.

Converting an Oral Confession. In this step, the investigator tells the subject he has to leave for a few moments to check on something. The investigator leaves the interrogation room and then returns with a partner who the investigator introduces as someone who has been working on the investigation. The actual function of the partner is to be a witness to the subject's confession. The investigator then goes over the essential details in a manner that would allow the witness to testify to the correctness and voluntariness of the confession. The questioner is

now ready to convert the oral confession into a written or recorded confession. One of four formats can be used:

- A statement handwritten by the subject
- A statement written by the questioner, and read and signed by the subject
- A statement taken down by a secretary or stenographer and transcribed into a typed document for the subject to read and sign
- A tape-recorded or video-recorded statement

Fundamental guidelines should be followed. In a custodial setting, even though Miranda warnings may have been given and the appropriate waiver obtained, it is advisable to repeat the warning at the beginning of the confession, referring to the fact that the subject had received them earlier.

The statement of guilt must be readable and understandable by someone who is not familiar with what the subject has done. Leading questions should be avoided, the confessor's own language should be used, and full corroboration should be established. Any errors, changes, or crossed-out words should be initialed with an "OK" written in the margin by the subject. The statement should reflect that the subject was treated properly, that no threats or promises were made, and that the statement was freely given by the subject. When the subject has completed reading the written statement, the questioner says, "Write your name here" while pointing to the place of signature. The questioner avoids saying "Sign here" because "sign" connotes a degree of legalism that may cause the subject to back out of making a written confession. The subject signs each page of the statement in front of the questioner and the witness, who also add their signatures.

Obtaining the written confession at the end of the interrogation is, of course, not the capstone. Every effort should be made to verify the statement and obtain the support evidence necessary for trial.

Joseph P. Buckley, III

Source Inbau, F., Reid, J., Buckley, J., and Jayne, B., ed. 2001. *Criminal Interrogation and Confessions, 4th Edition*. Gaithersburg: Aspen.

ROBBERY

The crime of robbery is a serious offense capable of being carried out by a variety of means. Crime statistics show that robbers are not always men and come from a wide range of age, racial, social, economic, and occupational groups. The robber's principal motive is usually to obtain money, or property that is easily converted to cash. Robbery is also a crime that is sometimes committed in conjunction with another crime, such as murder or rape, and because robbery is a form of larceny that uses violence as its means, the investigative techniques used in larceny and assault cases have application to robbery cases.

Types of Robberies

Mugging. Mugging is a type of robbery committed by the muffling of the victim's mouth (or by choking) while forcibly taking property from the victim's possession. The amateur or inexperienced mugger will usually act on the earliest opportunity to victimize a lone person. He will act on the spur of the moment, usually with little or no preparation, and is acting in response to some urgent need for money, as for example the drug addict in early withdrawal who needs money to buy his next fix. At the other extreme is the experienced mugger who usually selects his target carefully and formulates a plan that includes a concealed location and an unobstructed escape route. His victims are chosen on the basis of the valuables they are expected to be carrying. The experienced mugger looks for high return at low risk. When a particular mugging method proves successful over a period of time, the experienced mugger will establish a modus operandi or pattern of activity.

A common example of a mugger's operandi is the yoking technique. The largest of a group of two or three muggers subdues the victim from behind by a strangle-hold on the neck. If there are three or more muggers the victim's arms are pinned while the last mugger, usually the smallest, searches the victim's pockets and removes valuables. Other similarities in the mugger's method of operation might include use of the same or similar locations such as parking lots or stairwells; weapons used, if any; the manner of approach; opening statement to the victim or other conversation

leading up to the incident; and the use of violence inflicted in certain ways upon the victim. A particularly dangerous type of mugger is the sadist-flagellant robber whose primary motive is sexual gratification through inflicting injury on his victim. The theft aspect of the crime is a secondary consideration.

Robberies of Places. Banks, stores, and residences are common robbery targets. As is the case with mugging, this type of robbery can be committed by amateurs or professionals. The amateur robber is capable of traveling to and from the place of robbery in his own car or with a leased car, sometimes leased in his own name, or may travel on foot or even by bicycle. Because the inexperienced robber is certain to be nervous during the commission of the crime, he is apt to use violence unnecessarily. The experienced robber is likely to retain his composure and is comforted by the preparation and planning that has preceded the act. He knows what he is doing, is operating on a schedule, and realizes the risk of causing injury. He will usually use a stolen car, which he later abandons, or he might rent a car in a false name and use stolen plates.

Vehicle Robberies. The target of the crime is frequently a commercial-type vehicle carrying cash or high-value cargo. Vehicle robberies are more likely to be committed by experienced, professional robbers because of the requirements to obtain "inside" information concerning the valuables being transported, the schedule of the vehicle, and its defense capability. A vehicle robber needs also to stop his target, extricate the valuables, and safely get away.

Investigative Techniques

Robberies that are committed on the spur of the moment by amateurs or robberies that are committed by professionals only after long and intricate planning have at least one thing in common: they are both difficult to solve. Many robberies are committed during hours of darkness or under conditions that make it difficult for the robber's features to be seen by the victim. Adding to this is the fact that the attention of the victim is frequently focused on the weapon, thereby making it difficult for the victim to provide a good description of the suspect.

A robbery is usually reported fairly soon after it has happened. The investigator who is called to the scene of the robbery should follow the basic steps of crime scene processing. The crime scene is usually larger than the normal crime scene because it covers that territory where a robber may have lain in wait for his victim, the approach routes of the suspect and victim, the place of the robbery, and the escape route of the suspect. Persons who were present immediately before, during, and after the incident are potential witnesses. The investigator should question witnesses, as well as the victim, to determine the following:

- A description of the robber to include words used, voice peculiarities, gestures, mannerisms, and clothing
- The direction and type of approach used by the suspect
- A description of valuables taken
- The victim's action prior to the robbery
- The direction traveled by the robber when he left the scene and the method of travel

After the victim has had time to recover and the investigator has had time to make a careful examination of the crime scene, a second interview should be conducted. The victim may remember details after he has settled himself emotionally and the investigator may have to ask specific questions to clarify details or develop leads on the basis of evidence discovered. The second interview can also be used as an opportunity to prepare a composite likeness of the suspect.

If an automobile is involved in the robbery, the investigator should obtain a detailed description of it from as many persons as possible. In addition to making a routine stolen vehicle check, the investigator should contact car rental agencies. When a rental automobile is used in the commission of a robbery, it is possible that a description will be obtained from the clerk who handled the rental transaction. If and when an abandoned vehicle used in a robbery is located, latent fingerprints and items recovered from it will provide valuable leads. Items of clothing found in the car or close to it should be checked for laundry marks or other peculiarities that may provide leads to the identity of the suspect. Footprints at the scene of an abandoned stolen vehicle should not be ignored. Valuable leads can also be developed from discarded items

such as newspapers, matchbooks, and cigarette butts that are inside or around the vehicle.

When a robbery has occurred indoors, there should be an intensive search for latent fingerprints. Furniture, counter tops, and anything else that could have been touched by the robber should be processed for latent prints. Notes handed to a teller, discarded deposit slips, or counter checks not only provide opportunities to obtain fingerprints, but can also link the robber to the crime through handwriting analysis.

Some robbers feel a need to restrain their victims using such items as rope or adhesive tape. When rope has been used and to the extent that it is possible to do so, the investigator should obtain the rope with any knots still intact. The type of knot used by the robber may provide a link to him and to other crimes he may have committed. It may also be possible to trace the type of rope to a particular dealer. Adhesive tape has an especially high potential as evidence because it may be possible to obtain fingerprints from either side of it. It may also be possible to match the torn edge of the tape to the end of a roll of tape found in the possession of the suspect.

When interviewing witnesses or victims, the investigator should concentrate on determining the exact words used by the robber. The use of particular words or groups of words is valuable in matching the crime against previous robberies. The speech, gestures, and mannerisms of the robber are sometimes the only leads an investigator may be able to develop.

Any discussion of robbery is not complete without mention of the critical importance that informants can play in the identification and arrest of robbery suspects. While there is no replacement for hard work in developing physical evidence and testimony from people having knowledge of a robbery, there is tremendous value in obtaining the right piece of information from a confidential source that is in a position to know or acquire information beyond the influence of the investigator.

John J. Fay

UNDERCOVER INVESTIGATIONS IN THE WORKPLACE

While undercover is one of the most powerful forms of workplace investigation, it is also the most complicated. Successful undercover investigations require the investment of time, patience, and resources. An employer that is unwilling to make the required investment should not contemplate this form of investigation. The chief distinction between undercover and other forms of investigation is that the undercover investigator does not conceal his or her presence or attempt to pass unnoticed. What is concealed is the investigator's true identity or purpose. Other than interviewing, undercover investigation is the only form of interactive investigation. This unique quality allows the skilled undercover investigator (properly identified as the operative) to not only gather information concerning a workplace problem, but to learn the "how" and "why" behind the actions of those under investigation.

When Should Undercover Be Used?

Undercover enables the collection of information and ultimately the solving of problems not possible by other means. The shape and form of the investigation, and the way it unfolds will be dictated by the nature of the information sought. Consequently, it is widely held that undercover operations are not a panacea and should only be used in the most aggravated circumstances. Undercover investigation should be the exception, not the rule. Undercover should only be contemplated when no other options are available.

The following are situations which typically lend themselves to the use of undercover:

1. When there is consistent, reliable information suggesting employee misconduct or criminal activity but insufficient detail to permit prevention or the identification of those involved
2. When losses are known to occur in a specific area, but there is no information as to how they occur or who is responsible
3. When there is a strong suspicion or actual indicators of on-the-job alcohol or drug abuse and/or drug dealing in the workplace
4. When there is a strong suspicion or actual indicators of on-the-job impairment due to alcohol or drug abuse, yet

supervision is non-responsive or incapable of intervening
5. When it is necessary to compare actual practices with required or stated practices and routine auditing is not possible
6. When there is a high probability the use of undercover will produce significant results and all other reasonable options have been ruled out

Undercover operations are not appropriate for:

1. The investigation of protected union activities.
2. The investigation of any activity permitted or protected by any governmental statute, rule, or regulation, or otherwise protected by a union agreement or contract.
3. Fact-finding that will likely produce the same results while consuming less time and resources.

It should be noted that simply because a workforce is unionized, the use of undercover should not automatically be ruled out. It is permissible for an employer to use undercover and even place undercover investigators into a unionized workforce as long as the investigation does not impinge upon the lawful and protected activities of the union or its membership.

Clearly, undercover should not be used to gather or collect information of a personal or confidential nature or offensively intrude into private lives where a reasonable expectation of privacy exists. Such efforts are actionable and may give rise to legal claims against the employer and its investigators.

The Undercover Investigative Process

Workplace undercover investigations have potentially several distinct outcomes. Categorically, when employee misconduct is uncovered these outcomes include: employee discipline; employee prosecution; and restitution. The organization must select the desired outcome(s) and then engineer the investigation to achieve it. To do so, the organization must contemplate past practices, precedent, organizational policies, labor contracts (should they exist), the criminality of the suspected activity, employee relations, potential public opinion, the organization's culture and its reputation, and the potential return on investment. Sometimes competing, these considerations must be thoroughly analyzed and weighed before realistic objectives can be decided.

Next, the organization must select the investigative team. At a minimum the team should include a corporate decision maker, a representative from human resources, a corporate security professional, and an attorney familiar with state and local employment law. Once constituted, the team should then seek a vendor that can provide the undercover investigator and conduct the investigation. Because undercover is so complex and fraught with such enormous liability, it is best to hire only experts.

Although law enforcement can conduct workplace undercover investigations, most often law enforcement has neither the time or resources to conduct an investigation properly or for any useful duration. As such, most employers turn to private agencies that specialize in undercover. Consider the following when selecting an undercover agency:

- Licensing: In all but several states, private investigators and their agencies must be licensed.
- Training: The agency selected should provide professional training and rigorously screen its investigators.
- Experience: Ensure the agency as well as the employees they assign to the investigation have the experience necessary to do the job properly.
- Reputation: Reputations vary widely in the industry. The best agencies are well known in the business community and are active in their trade associations. Find out about the firm's litigation and claims experience. A reputation of sloppy work, high profile lawsuits, and big settlements could spell trouble.
- Willingness to Testify: All undercover investigators must be willing to testify and see their cases through to their fullest completion. Sometimes that means testifying in court or before an arbitrator.
- Reports: Reports are an important part of every investigation, not just undercover. As such, detailed reports should follow

all investigative efforts. The information provided in a report should be complete, concise, and correct.

- Insurance: All quality agencies carry general liability insurance. In fact most states that license investigators require insurance. Bonding is not enough protection. In order to be safe, require the agency under consideration to provide a Certificate of Insurance naming your organization as an additional insured. Also ensure the coverage is occurrence not claims-made.
- Willingness to Involve the Police: Employee prosecution is not always necessary. It is complicated and often expensive. As such, the decision to prosecute should be made for business reasons only. However, a good agency knows its limitations and when to involve the authorities. Investigations involving illegal drugs for example can not be done without the assistance of the police. Also ask the vendor about their success with prosecution. The answer will provide some idea as to how many cases the agency has run, and how complicated they were. A low prosecution ratio should not patently disqualify an agency. Instead examine the organization in its totality before making your selection.
- Attorney Involvement: All experienced undercover agencies insist on the involvement of their client's attorneys. The attorney's role is an important one and the attorney should be an active participant during most of the investigation. Sophisticated undercover firms know the attorney will contribute to the smooth running of the investigation and coincidentally protect its interests as well as the interests of the client.

Once an agency is selected, the next step is to select the investigator. Undercover investigators come in all shapes, sizes, and colors. They also vary in experience and ability. Some of the best positions for the undercover are in:

- Materiel handling and expediting.
- Shipping and receiving.
- Mailrooms.
- Customer service.
- Uniformed security.
- Some on-site contractor capacity.

The professional operative must also have strong communication skills. Not only must he make daily written reports detailing his day's activities, he must be able to effectively communicate verbally with his supervisor and occasionally with the employer-client. The successful operative will also eventually have to testify. His cases may eventually yield criminal prosecutions, terminations, and other employment actions. Compelling testimony is essential for successful prosecution and winning civil actions, and is a skill that must usually be taught. In order for the investigation to be successful, the operative must be able and willing to testify effectively and professionally.

Once selected, the undercover investigator should not be placed in a position for which he does not have the requisite credentials, prior experience, or documentation. The operative should also have the skills required for the job he will be performing. If he lacks the necessary skills, sometimes remedial training can be provided before he is inserted into the job. In some instances, it is easier and more cost-effective to simply select another investigator.

Consequently, for these and other reasons a position should not be created for the investigator if possible. To do so might bring unnecessary suspicion upon him and will likely lengthen the duration and expense of the investigation. Regardless of the circumstances, the undercover investigator should be treated like any other employee and not receive any preferential treatment or special considerations.

The Cover Story

The operative should also have a plausible cover story. The cover story is the explanation of the investigator's identity and how he or she came to obtain the job. In some situations, the level of detail may be quite superficial and in other cases, the history may be quite involved. Generally, the more intimate the personal association between the investigator and members of the target group, the greater depth of the cover story.

The cover must not only explain the investigator's qualifications for the particular job, but must also offer a convincing account of how the job was obtained and something about the investigator's past. Routine documents

supporting the cover story should be carried if possible. However, no documentation indicating the investigator's actual identity should ever be carried while on the assignment.

Once the investigator has been successfully placed into the target workforce, he or she will first engage in what is commonly called the relationship-building phase. During this phase the operative will learn the job, become familiar with the surroundings, and make acquaintances. The investigator should resist the temptation to press for information or appear too inquisitive. To do so will create suspicion and will hamper the collection of useful information later.

Law enforcement plays an important role in most workplace undercover investigations. In cases involving illegal drugs, no drug purchases should take place without the approval of law enforcement. In other types of cases law enforcement may provide resources, manpower, and intelligence, and in some instances actively participate in the supervision of the operative.

However, law enforcement's role should be limited. As the line between private corporate investigation and public law enforcement begins to blur, legal responsibilities and liability begin to shift. The more law enforcement becomes involved in the undercover investigation the more "police-agent-like" the operative becomes. If agent status is bestowed upon the investigator, the rights of the investigated persons are expanded. Significant among those rights is that of due process and Miranda. Furthermore, if agent status is achieved the criminal defendant may be able to escape prosecution using the entrapment defense.

Aside from the telephone, written reports are the most fundamental form of communication used in undercover. Even before the operative is placed, generation of reports should begin. Although practices vary from agency to agency, most firms require their operatives to make daily reports. These daily reports in their most basic form detail the who, what, when, where, how, and why of the investigator's daily observations and experiences. Generated by the operative at the end of his workday, the reports are then transmitted to his case manager for review and dissemination. The formats for these reports are as varied as the agencies that generate them. However, most are chronological and begin with the operative's arrival at work and conclude with his return home at the end of the work day. Whatever the format selected, reports must be easy to read and use, and above all accurately describe the observations and experiences of the operative.

Employee Prosecution

It is logical that those who are caught violating the law be punished. In fact it is the mission of law enforcement to enforce public law and bring to justice those who violate it. For example, if the objective of the investigation is elimination of workplace substance abuse the investigative team must then articulate how prosecution will help achieve that objective. In most places, only dealers can be prosecuted. The criminal justice system generally does not have the capacity to prosecute every user. In workplace drug investigations, the users are almost never prosecuted. Prosecution is expensive and problematic. Although counterintuitive, prosecuting employees may not be the best action to take. Prosecution is expensive, time consuming, and often exasperating. Even before a trial date is set, documents, photographs, notes, sketches, and physical evidence may have to be produced, pre-trial conferences may be necessary, and witnesses may have to be interviewed. Then, after lengthy and costly preparation, the defendant's attorney negotiates a settlement with the prosecuting attorney that very frequently amounts to nothing more than a slap on the wrist.

Buy-Busts and Sting Operations

The buy-bust is nothing more than arranging the arrest of the perpetrator at the moment he is committing the crime. Usually the other party to the transaction is a member of law enforcement or a designated agent. Upon some prearranged signal, the suspect is confronted and arrested on the spot. In theft cases, the technique works best toward the end of the investigation. By necessity or design, the true identities of the undercover operative and law enforcement agents can be revealed at the time of the bust because the bust culminates the investigation. By arresting the offender(s) at this point reduces the chance that valuable evidence will disappear or that accomplices will escape. Chasing down a fleeing felon can be dangerous.

A sting operation is similar to a bust but is typically longer, more complicated, and more expensive. A sting usually involves an elaborate setup such as an apparently legitimate store where thieves can sell or trade stolen goods. A sting requires considerable planning, preparation, coordination, and skillful operative performance.

Recoveries

Recoveries can be a big part of theft investigations. Because undercover investigations permit a high degree of interactivity with the offenders, they permit the gathering of information not generally otherwise obtainable. Of obvious value is the determination of who is stealing and what it is they are taking. But of equal value is why are they stealing and how the property is stolen and disposed of. If other parties are receiving the property, civil recovery may be possible. A properly conducted investigation should reveal the identities of third parties and to what degree they are involved. Once identified, the investigation can be engineered to allow recovery from them as well as the principal perpetrators. Not only can property or consideration for the property be recovered, but also so can some of the costs of the investigation. A recovery of costs will significantly increase the return on investment of any investigation, not just undercover.

Case Closure

Every undercover investigation eventually evolves to where the production of useful information reaches the point of diminishing return. In some instances, the investigative effort has met every objective and the undercover investigator identified every perpetrator. More common, however, is something short of this idealistic outcome. Typically, the investigation simply reaches the point where it has yielded enough information to permit the removal of the operative and allow the rest of the investigative team to take over. Generally, the properly engineered investigation has anticipated this eventuality and has designated and allocated the sources necessary to properly close the investigation. The next phase of the investigation is called Verification and Analysis and it usually involves interviewing the offenders.

Interviews

Interviews of the guilty are key to any successful workplace investigation. In fact, the undercover portion of the investigation could be considered only a vehicle by which the investigative team reaches the point where interviews are likely to be successful. In other words, the information developed by the operative serves as the seed information, which enables the proper selection of candidates for interview. However, unlike most general investigations where the interview process over time closes in on the perpetrators, these interviews begin with those most involved and work toward those less involved. Interviews are the most critical component of the entire undercover investigation. To not conduct employee interviews following the efforts of a productive undercover is the equivalent of professional negligence. For those who use this powerful tool will attest, most of the information gleaned during the investigative process comes from interviews. When it is all said and done, only a fraction of the useable information is actually developed by the undercover. Investigative agencies that don't effectively interview are not properly serving their clients.

Investigatory interviews are interviews in which the subject is either known to have committed the offense in question or the interviewer has very good reason to believe that he has. Investigatory interviews are complex and can be fraught with liability even when properly conducted. For tactical reasons, the most serious offenders should be interviewed first. These individuals are usually the easiest to obtain admissions from and very often the most cooperative. Thus the skilled interviewer (or team in some cases) will start at the top and work down the list of interviewees, such that each subsequent interviewee is less involved than the one prior. This procedure also allows the interviews to be concluded at any time without the concern of someone claiming discrimination, bias, or disparate treatment. Theoretically, by this process the initially interviewed persons were believed to have committed more serious offenses than persons that were interviewed later.

Operative Extraction

The timing of the removal of the operative is one of the most frequently debated subjects among

undercover supervisors. However, the answer is a simple one: the operative should be kept in as long as possible. In instances where interviews follow the undercover effort, the operative should stay in place until he is named as a co-offender by enough actual offenders that they would expect the operative to be interviewed. To remove the operative sooner will only bring suspicion upon him. If he is removed before the interviews begin, it will appear clear to everyone that he was an informant.

If the undercover investigator is not compromised or otherwise exposed he can be very valuable if left in place. Often after the disciplinary and corrective action is taken, offenders who have not been caught will sometimes become complacent. Some offenders will even brag of their cunningness and of having slipped through management's grasp. These individuals are easy targets for the operative.

The Administration of Disciplinary and Corrective Action

Following the interviews the investigative team should compile all of the information gleaned during the investigation and separate it by individual. The team can then guide the employer's decision makers through the information, examining each offender and the totality of information regarding them. Clearly, if an employee made an admission against interest, it would serve as the best evidence against him. If the admission was properly obtained, no other evidence is needed to take disciplinary action such as termination. Unlike the criminal justice system, which requires substantial evidence and a long waiting time for trial, an admission is all that is needed to make the case. In some instances, it is wise for the employer to disregard all of the other evidence in favor of an admission. In doing so, the disciplined employee can only challenge his admission. Because nothing else from the actual investigation (including the information developed by the undercover) has been used, he cannot challenge any of it. In other words, he cannot challenge the undercover operative and those who provided incriminating information about him. If the employer exclusively relied upon the subject's admission and nothing else, the subject will have difficulty challenging the employer's disciplinary decision.

Once all of the discipline and corrective actions have been taken, the entire case file must be provided to the custodian of record for storage and safe-keeping.

Eugene F. Ferraro

Source Ferraro, E. 2000. *Undercover Investigations in the Workplace*. Boston: Butterworth-Heinemann.

WHITE-COLLAR CRIME

The term "white-collar crime" is a general descriptor that relates broadly to a wide variety of specific crimes. It may take the form of consumer fraud, illegal competition, deceptive practices, check and credit card fraud, tax evasion, bankruptcy fraud, bribes, kickbacks, pay-offs, computer-related crime, pilferage, insurance fraud, fencing stolen property, securities fraud, and similar offenses.

The white-collar criminal can be a bank executive who embezzles or a shipping clerk who pilfers. The essential characteristic of white-collar crime, however, has more to do with the nature of the offense rather than the status of the offender. White-collar crime is a non-violent crime; it involves deceit, corruption, or breach of trust. The offense frequently involves lying, cheating, or stealing through misrepresentation. It can be committed against private individuals, business corporations, non-profit organizations, and government units.

A problem in addressing white-collar crime is the absence of valid measures for determining if criminal activity is present and to what extent. A difficulty in detecting its presence is the fact that a victim is not aware that he is being victimized, and when discovery is made, it may be too late to take effective action against the offender. In a sense, white-collar crime is an invisible crime.

The invisibility of the crime is complicated by two other factors: an unwillingness of the public to vigorously prosecute white-collar criminals and the failure of investigators to keep pace with increasingly complex schemes.

The Nature of White-Collar Crime

In most crimes there is a "crime scene," but with white-collar crime the offense is not readily

apparent and is usually in progress. The investigator needs to detect the crime and work backwards to identify the principals. Following are general characteristics of white-collar offenses:

- Detection is frequently accidental.
- Offenses are frequently reported anonymously.
- There is usually no complainant.
- The scheme has been in existence over a long period of time.
- The crime tends to cover a large geographical area, often spanning several prosecutorial jurisdictions.
- The scheme tends to involve several specific violations of law.
- The principals are usually well known, respected, intelligent and, in some cases, influential.
- The scheme is sometimes difficult to decipher.
- Evidence tends to get "lost or destroyed" when the principal learns that an investigation is in progress.

Types of White-Collar Crime

Following are brief discussions of the more common types of white-collar crime.

Advanced Fee Schemes. These are designed to obtain fees in advance for services the promoter has no intention of providing. They usually occur when the offender claims to have means of obtaining buyers for one's business, property, securities, or other assets, or to have access to sources of loan financing. These usually occur when property is hard to obtain.

Pyramid Schemes. These are investment frauds by which an individual is offered a distributorship or franchise to market a particular product. The contract also authorizes the investor to sell additional franchises. Promoters represent that the marketing of the product will result in profits, but that the selling of franchises will result in quicker return on investment. Therefore, investors expend greater energies on selling franchises than on sale of products. Finally, a point is reached where the supply of investors is exhausted, leading to the collapse of the pyramid. Often, too, the product itself is overpriced, and no real effort is made by promoters to sell the product.

Chain Referral Schemes. These involve sales of grossly overpriced products through false representation that the cost will be recovered by commissions the promoter will pay on sales to the purchaser's friends, if only the purchaser will permit them to be contacted with the same proposition.

Ponzi Schemes. These are basically investment frauds. Operators solicit investors in a business venture, promising extremely high financial returns or dividends in a very short time. The operator never invests the money in anything, but does pay "dividends" to the investor by giving him back some of his original investment. This is done as an inducement to investors to put up additional funds, or to solicit others to do so. During the early stages, the investor may even be able to liquidate his investment if he wishes, plus interest. This makes the operation more credible to others. When the operator has accumulated sufficient funds for his purposes, he flees the area.

Business Opportunity Schemes. These are a number of schemes and deceptions concocted to attract victims into participating in an allegedly lucrative business venture. They may appear in almost any type of financial dealing, e.g., vending machines, product dispensing, distributorships in limited areas, multi-level sales organizations, etc. The schemes may differ in form, but may have basic identifiable similarities, such as:

- Financial investment by the victim in advance.
- The victim's investment is "covered" by company inventory, buy-back agreements, or escrow accounts.
- The promoter convinces the victim that the company will work closely with him to ensure success. This usually includes management and marketing aids, training, and saturation advertising.

The best way to identify potentially fraudulent business opportunity schemes is to attempt to identify the misrepresentation. Some of the common indicators of misrepresentation are:

- Claiming affiliation or association with a larger or well-known company.
- Presenting a misleading credit rating, such as a false Dunn & Bradstreet report.
- Citing false business and personal references (e.g., Better Business Bureau, Chamber of Commerce, and well-known individuals).
- Inflating marketing experience and national sales.
- Misreporting the size of the firm.
- Promoting a unique product or service that has a high public demand and need.
- Projecting unrealistic sales and profits.
- Presenting doctored marketing surveys.
- Claiming easy selling, working during spare time and/or at home, such as filling orders for retail stores and selling via direct mail.
- Offering exclusive territory with leads and potential customers furnished.
- Offering a re-purchase or buy-back option.
- Providing free training, free servicing, and repair of the product to be marketed.
- Representing that the manufacturer or sponsor will provide saturated advertising.
- Advising that the offer to "get on board" will soon expire.
- Changing the contract or deleting clauses before signing.

Planned Bankruptcy Schemes. This is a merchandising swindle based on the abuse of credit that has been established, either legitimately or fraudulently. The scheme usually consists of:

- Overpurchasing of inventory on credit
- Selling or other disposing of the merchandise obtained
- Concealing the proceeds
- Not paying the creditors
- Filing a bankruptcy petition, either voluntarily or involuntarily

The new company is organized, a bank account opened, and operating space is leased. The company begins making purchases from a number of suppliers and making payment promptly to establish credit. The operators then use this credit to find other suppliers and order more merchandise, while slowing payments to the original suppliers.

The orders for goods from all suppliers are increased while the goods are sold to fences below cost. The operators now either abscond or gut the business and file bankruptcy. This can also be accomplished in one step by buying a business with a good credit rating. Organized crime has been particularly active in this type of scheme.

Merchandising Schemes. Many times these schemes are visible, blatant, and occur in the retail marketplace. All are frauds based on a twisting of the truth for increased profits. Some include:

- Bait and Switch. A product or service is promoted with no intent to sell it as advertised. The customer is lured to the seller by an extraordinarily good buy and upon arrival the salesperson tries to induce the customer to buy a higher-priced product or service. Hence the name, "bait and switch."
- Phony Sales. The unscrupulous businessperson relies on the customer's desire for a bargain. These may take the form of fire, liquidation, or going out of business sales. The advertising must be shown to be fraudulent.
- Deceptive Sales Contest. Through a variety of means, the deceptive businessperson promotes a contest in which the victim is led to believe that the chance of winning is much greater than it really is.
- Short Weighing. This practice involves substantially more than simply cheating a customer in the weighing of produce in a grocery store. Producers at the packaging stages of production can fill containers of their product 9/10 the capacity and charge retailers for the entire amount. Investigative efforts directed at a package-by-package basis seems a waste, but considering mass marketing practices, this can be extremely lucrative for the dishonest firm.

Service and Repair Schemes. Since in the affluent society many of our appliances, automobiles, or other mechanical devices need repair from time to time, this can be a very lucrative scheme. Repair schemes, regardless of the product involved, give dishonest repairpersons the

chance to "lowball" the customer. Lowballing occurs when a customer takes a product in for repair, and is quoted a ridiculously low bid for the repairs. The operator has no intention of fixing the product at this price, but the lowball price will induce the customer to authorize the repairs.

Once the repairperson has the product in his possession, he tends to discover other malfunctions or worn parts, and the repair price is adjusted upward.

The most difficult element to prove is that from the beginning the repairperson intended the original estimate only as an enticement to obtain the repair job under false pretenses.

Land Schemes. Increasing in frequency, land schemes are marked by high-pressure sales tactics in which many misrepresentations are made, such as the location of the land, value, utilities available, title validity, prospect for future profitable sale, the installation of roads, or other improvements. The land is often sold sight unseen with the use of deceptive photographs, appraisal reports, and false promotions as to free bonuses, refunds, and closing costs. Targets are usually retirees, middle-income families seeking vacation resort property, and investors lured by promises of lucrative returns.

Home Improvement, Debt Consolidation, and Mortgage Loans. In recent years, all of these have been combined into one overall scheme. Homeowners already heavily burdened with debt have been the victims. The homeowner is offered a loan sufficient to pay off all other debts, as well as finance a home improvement, and is promised that the one monthly payment is less, or at least no larger, than the combined payment now being made. The large amount of the loan offered may stem from the criminal's intention to quickly sell the note at a discount to a finance company. To do so profitably he knows the amount borrowed must sufficiently exceed the cost of the home improvement work so as to offset the discount. The finance company, a third party, assumes legal possession of the promissory note, collects the monthly payments as a holder in due course, and disowns all responsibility for any misrepresentations that may have been made in its creation. In this type of scheme, promoters rely on the bewildering terms of the signed documents and numerous put-off tactics to forestall serious consequences when the home improvement falls in arrears, is poorly done, or is not done at all.

Home Solicitation Schemes. In this type of scheme, the operator represents that an individual may receive a product at no cost because the operators wish to showcase the product in the neighborhood. He will often say that the person was selected because of his reputation in the community. The victim is then asked to sign a contract that supposedly reflects the terms of the oral agreement. It is, in fact, a long-term sales contract that requires the consumer to make additional purchases for as long as 10 years.

Personal Improvement Schemes. Promoters prey on the victim's need to improve himself. These may come in the form of joining a health spa, attending a trade school, computer dating service, losing weight, learning to dance, becoming more attractive, etc.

Medical Frauds. In these illegal activities are found a number of schemes that involve defrauding of government-sponsored medical programs:

- *Double Billing.* Others billed include the patient, Medicare, Blue Cross, Medicaid of another county or state, or state insurance (Workers' Compensation).
- *Over-Billing and Billing for Services Not Performed*
- *Billing for Services Provided by Another.* This is done by gaining access to another provider's records and billing for the other's as yet unbilled services. This frequently occurs where many doctors work at the same location and records are centrally maintained.
- *Ping-Ponging.* The victim is given unnecessary treatment at the same time needed services are performed.

Welfare Frauds. These involve the acquisition of public assistance funds by those not entitled to such funds, for example:

- Receiving payments while employed.
- Receiving payments with an undisclosed source of support that would otherwise disqualify the person from receiving funds.

- Receiving funds for individuals no longer residing in the household.

Food Stamp Frauds. The individual may improperly receive food stamps in much the same way that welfare frauds are committed. The following are examples:

- Misrepresenting current income or property
- Receiving support from an undisclosed source
- Trafficking in the sale of stamps for cash

Official Corruption. Many times the investigation of other white-collar type crimes, such as bid-rigging or fraud in government programs, have corrupt public officials at the core. Often the only way to identify these frauds is when they are brought to the attention of the investigator by informants. To succeed, these investigations must be discreetly conducted.

Bid-Rigging. Generally, large public contracts are awarded by means of competitive bidding. Sometimes providers of the bids will agree on which one will submit the lowest bid, and although it is the lowest bid received, it is usually inflated because of the rigging. Oftentimes, this is very difficult to prove because the rigging is the result of a tacit understanding rather than a provable conspiracy. Sometimes the bidders may have divided the public market among themselves, or the competitors may rotate the lowest bids. Either way, the competitive bidding process is no more than a sham.

Commercial Bribery. This includes payments, kickbacks, and rebates. Through the offer of a bribe, a responsible corporate official may be persuaded to purchase inferior supplies from one firm, or to overlook deficiencies or irregularities by a contractor and thus certify payment for unsatisfactory work. The cost of the corruption is ultimately passed on to the consumer.

Insurance Fraud. This type of fraud basically occurs in four ways:

- Fraud Committed by Insurance Agents. Agents who become involved in this type of fraud usually practice a form of the Ponzi scheme. They are normally independent, travel large territories, and sell a variety of types of insurance. They purport to represent legitimate insurance companies, and often use forms and promotional materials of the major companies. Since all premium payments, policy changes, and claims are processed through the agent, the agent simply fails to forward the payment to the company. Barring a rash of claims at once, the agent can operate successfully over a number of years by simply paying the claims out of the premiums. State insurance agent licensing laws makes this type of fraud fairly easy to detect, but this has not seemed to decrease the incidence of this fraud.
- Fraud Committed by Claim Adjusters. An adjuster's investigation is the basis for insurance settlements. The most common fraud is when the adjuster conspires with claimants or repairpersons. Exclusive dealing arrangements and falsely inflated bills are the hallmark of this type. They also often substitute claimants.
- Fraud Committed by Individual Policy Holders. False customer claims are the largest source of insurance fraud. Sometimes this involves the "staging" of accidents.
- Fraud Committed by Organized Rings of Phony Claimants. Although many times an individual will commit frauds involving "staged" accidents, an increasing number of false claims are the result of organized rings of economic criminals who work together. The annual loss suffered by legitimate insurance companies is enormous in terms of fraudulent accident and health claims—losses that impact increasingly on the rising cost of insurance to the general public.

Computer-Related Frauds. Most computer crime is not detected and most of what is detected is not reported. This type of fraud is very difficult for the investigator because of lack of expertise and because the computer can be programmed to wipe out the evidence of a crime. Many schemes involve fraudulent conversion of confidential information stored within the memory banks. For this type of criminal, data is money and power.

Credit Card Frauds. Several distinct crimes are included in this classification.

- Falsely acquired credit cards by misrepresentation, including identity, age, employment, etc.
- Use of the card to defraud merchants or other providers
- Professional credit card rings who deal in counterfeit, lost, stolen, or misdelivered credit cards

These losses are in the millions annually. As always, the economic consequences are borne by the honest consumer in terms of increased prices.

Charity Frauds. The most common form of this type of fraud involves solicitation of money for an ostensibly worthwhile cause by an individual who has no intention of turning the money over to the organization if, in fact, one does exist. Also, professional fund raisers solicit donations for legitimate charities but fail to disclose that because they are professional they take for themselves a large percentage of the funds.

Check Kiting. This is the practice of drawing checks on accounts whose balances consist substantially of uncollected funds (checks that have not cleared). Using two different banks, the kiter can cover checks drawn on one bank by checks drawn on the other. The key to the scheme is the time required for the bank to actually collect deposited funds (checks).

John J. Fay

WORKPLACE INVESTIGATIONS

Workplace investigations are complex affairs, each one unique to another. A workplace investigator must have a comprehensive understanding of criminal, civil, and employment law. Workplace investigations also require a considerable investment of time, money, and patience by the employer. And finally, to ensure success, the process must be highly structured and flawlessly executed. Even the most sophisticated organization or experienced investigator can find the task consistently challenging.

Every organization at any level inevitably finds itself in need of an internal investigation. Workplace misconduct occurs in every type of organization, and at every level. Every organization is eventually confronted with the need to gather evidence, interview suspects, and uncover the truth. With the ability to muster the necessary resources, deploy skilled fact-finders, and adhere to a disciplined process, an organization can conduct a successful investigation. The investigator that is able to assist the employer in conducting a successful investigation is an invaluable asset to that organization.

Predictably, workplace investigations are fraught with liability. These considerations significantly add to the complexity of the fact-finding process and the manner in which the subject may respond to the investigation's findings and management's corrective actions. For the unsophisticated and hapless employer, a workplace investigation is a virtual legal minefield. An investigator familiar with the legal issues can be of vital assistance.

Necessary Elements of Investigative Success

A successful workplace investigation provides many dividends for the employer. In addition to uncovering facts and essential information needed to solve problems, a successful investigation helps restore order. It provides the employer the opportunity to analyze process and system failures and re-engineer them to prevent future problems. For an investigation to be successful, it must have:

- Management commitment.
- Meaningful objectives.
- A well-conceived strategy.
- Properly pooled resources and expertise.
- Lawful execution.

An investigation will undoubtedly fail when the investigator is confronted with a management that is dysfunctional or cannot make decisions. Failure in this case has nothing to do with the actual workplace problem, but with the resolve and commitment of the employer.

An investigation without meaningful, practical objectives cannot succeed. Success will be denied also when objectives constantly change and when efforts to achieve the objectives are allowed to wane and shift.

A well-conceived strategy is essential. A strategy explicates how the investigation will proceed; the objectives are the intended

outcomes of the strategy. The employer's role is to define the objectives, such as to identify guilty parties and recover stolen property; it is the investigator's role to determine how the objectives are to be met.

Knowing what needs to be done and how it is to be done is one thing; having the expertise and tools is another. Before taking a first step, the investigator must possess the requisite talent and have access to resources, which can include human, logistical, and financial resources.

One of the dangers in conducting a workplace investigation is the natural urge to cut corners, an urge that is often encouraged by an employer that wants to cut costs. The risk is defeat in the courtroom. A single unlawful act, particularly one that violates a constitutional right, can cause havoc. From it can come judicial problems, negative publicity for the employer, and damage to the investigator's professional reputation.

The Investigative Framework

In order to be successful, any workplace investigation should be conducted within a logical framework that provides process to the investigator and attainable goals to the organization. This framework specifies the objectives of most any workplace investigation:

- Seek out and identify the true nature and scope of the problem
- Identify who is involved and why
- Gather any and all information in such a fashion as to allow the proper distribution of appropriate disciplinary and/or corrective action
- Orchestrate the process in such a fashion that is least disruptive to the organization and its operations
- Achieve the best possible return on investment

An investigator who does not understand the true nature and scope of the problem may focus on one area or one individual related to misconduct, while failing to notice other critical elements of misconduct. Identifying who is involved is key to any investigation, and a seasoned investigator can often learn through skillful interviewing the identities of other employees previously unknown. Gathering information in an investigation is very important, but being able to properly present it to the client is of paramount importance. A skilled investigator may uncover mountains of actionable information, but it must be presented coherently and in such a way that the client can exact appropriate disciplinary and/or corrective action. An organization can be adversely affected by employee misconduct, but a careless investigator can also be worse than the disease and inflict damage to the organization.

Process of Investigation

Most workplace investigations unfold incrementally. That incremental, yet dynamic process is called *The Process of Investigation*. It includes five distinct phases. They are:

- Planning and Preparation
- Information Gathering and Fact-Finding
- Verification and Analysis
- Determination and Disbursement of Disciplinary and/or Corrective Action
- Prevention and Education

Every proper workplace investigation requires the investigator to structure his or her investigation such that it systematically contemplates each phase. To do otherwise is insufficient, unprofessional, and possibly even negligent. The investigator who imposes process and structure on his investigation obtains better results and does so with more efficiency. What's more, it differentiates him as a professional. It affords him and his employer or client the benefit of ease in assessing and analyzing the result. As in the scientific community, process also permits peer review. In the community of employer-employee relations, others may review the investigator's efforts and are able to easily and accurately reconstruct that which the investigator found and how he found it. The ability to reconstruct the process and demonstrate its integrity and propriety lends it credibility. That credibility is the foundation on which all facts rest. An investigative process without credibility is fatally defective. That defect potentially imposes a bar to the admission and ultimate use of otherwise admissible and actionable evidence. It is the implementation and ultimate integrity of this process that is the hallmark of the professional investigator.

Methods of Investigation

Fundamentally, there are six basic methods of investigation available to those who conduct workplace investigations:

- Physical surveillance
- Electronic surveillance
- Research and internal audit
- Forensic analysis
- Undercover
- Interviewing and interrogation

Physical surveillance is likely the oldest investigative technique and is nothing more than observing people, places, or things. Electronic surveillance is the use of electronic technology to enhance the investigator's observations and overcome limitations of physical surveillance. Research and audit is the review and examination of documents and records, both of public record and internal to the organization. Forensic analysis is the application of modern science and scientific technology in the gathering of information. Undercover investigation is the surreptitious placement of an operative into the workplace to gather information. Interviewing and interrogation is an interactive investigative technique that requires little more than an interviewer and an interviewee. An effective interview should always contain some semblance of methodology and offer the interviewee the element of due process.

Every workplace investigation uses one or more of these methods. The challenge then for the professional investigator is to select the method(s) most suitable for his particular circumstances and deploy them properly and efficiently. In many instances, the investigator will find that he must combine the methods in some fashion or mix and match them. It is only with knowledge and experience can the investigator know which methods to use and when. It is this unique ability to combine these methods properly and efficiently that separates exceptional investigators from good investigators.

Due Process

As with many other facets of workplace investigations, oftentimes the investigator should engage in practices that not only produce the desired results in terms of the goals of the investigation, but that are defensible to legal challenge. Among these considerations is that of due process. Among other things, due process includes: the right to know the offense(s) and crime(s) of which one is accused; the right to view and examine the government's evidence; the right to face one's accusers and examine them as well as any and all witnesses; the right to competent representation; and protection against self incrimination.

Employers must be careful. Although they have no legal duty to provide the subjects of internal investigations any due process, some triers of fact and jury sometimes think otherwise. The appearance of treating the subject unfairly and the failure to comply with the reasonable requests of the subject may expose the employer to considerable liability. Even absent the rights of due process, it is expected that all people be treated fairly and provided all reasonable accommodations while under suspicion or when accused of misconduct.

Burden of Proof

Ultimately, when one is conducting or supervising a workplace investigation, it is critical to understand the burden of proof that is applicable to the investigation and equally important for the investigator to be able to educate and communicate to management the differentiation between the perceived and actual burden of proof in a workplace investigation.

It is very common for members of management to assume that the standard of proof in building a case against an employee who is engaging in workplace misconduct is the same as it would be in a civil or criminal arena; most of the time, the burden of proof is actually lower and more attainable.

As most people know, the burden of proof in a criminal case is "beyond a reasonable doubt," which is the highest level of proof in any case. In mathematical terms, beyond a reasonable doubt equates to being approximately 99 percent sure of a decision. In most civil cases, the burden of proof is a "preponderance of the evidence." A preponderance of the evidence means that a trier of fact is swayed to one side more than the other given the facts of the case. One may see the "clear and convincing" burden of proof in certain types of

civil cases or matters involving civil fraud. Clear and convincing evidence falls between preponderance of the evidence and beyond a reasonable doubt, and contains evidence so clear and weighty in terms of quality, and convincing as to cause the trier of fact to come to a clear conviction of the truth of the precise facts in issue.

Employers, however, need only to meet the "good faith investigation/reasonable conclusion" burden of proof. As it states, management must only reasonably conclude that misconduct occurred after conducting a good faith investigation.

Reporting

Another important consideration, fraught with pitfalls, is the question of to whom the investigator reports during a workplace investigation. Ideally, in the planning stages of an investigation, a distinct and select group (or individual) is identified who is in the "need to know" group. This group should contain individuals who can be a point of contact for the investigator, a management representative for employees (and union stewards, if applicable), who can exact disciplinary or corrective action if necessary, and who can assist the investigator in coordinating certain logistics of the investigation and obtain critical records. Involving the appropriate legal counsel, whether internal, external, or both, can be helpful to management, especially when deciding what to do with the investigative results. Legal counsel should always be involved in undercover investigations without exception. Involving too many members of management or non-essential members can have a negative impact on the process of investigation and, ultimately, the entire investigation's outcome.

Litigation Avoidance

Workplace investigations have precedent in the arena of employment law to help guide the investigator and employer through litigation avoidance. *Noble v. Sears, Roebuck & Co.*, 33 Cal. App. 3d 654 (1973) held that an organization that hires an investigator can be held liable for violations of law made by the investigator which the employer authorized, either implicitly or expressly. Similarly, *Solis v. Southern Cal. Rapid Transit Dist.*, 105 Cal. App. 3d 382 (1980) held that employers may be held liable for the tortuous invasion of privacy when investigators conduct an "unreasonably intrusive investigation."

Organizations must also be sensitive to the federal requirements regarding discrimination. According to the Americans with Disabilities Act, employers may test for drug use but may not discriminate against a person who has successfully completed a drug rehabilitation program and who no longer uses illegal drugs. Title VII of the Civil Rights Act of 1964 states that employers must avoid disparate or different treatment and/or disparate impact in regards to an employee's race, gender, color, religion, or national origin. The Civil Rights Act of 1991 affects workplace investigations in that employers must be nondiscriminatory in investigating suspicious activity, be consistent applying discipline to all levels of the organization, and offer consistent rehabilitation opportunities. Furthermore, organizations must be diligent in ensuring that sexual harassment does not exist in the workplace and that claims of sexual harassment are dutifully investigated.

Labor Union Involvement

In a unionized workplace environment, considerations must be given to union employees when involving them in a workplace investigation. Failure for the employer (or investigator) to afford such consideration could result in heavy fines and sanctions to the offending employer, not to mention having to take back employees involved in misconduct. Under no circumstances may any employer (or its agents) conduct surveillance or monitor employees' union activities. In the *Weingarten* ruling [*NLRB v. Weingarten, Inc.*, 420 U.S. 241 (1975)], the Supreme Court ruled that an employee is entitled to ask for and receive union representation at an employer's interview if the employee reasonably believes that the interview might result in disciplinary action against them. An employer who disciplines or terminates an employee for refusing to participate in an interview without a union representative present is in violation of *Weingarten*.

Invasion of Privacy

While law enforcement enjoys the power to search people and seize property, the closest thing to it in the private sector is the ability of an employer to search its own property. Workplace searches of desks, computers, lockers, and other work areas are permissible only where an employee does not have a reasonable expectation of privacy. The employer can substantially reduce the expectation of privacy by: advising employees that such areas are subject to inspection, with or without notice; restricting private use of these areas by issuing its own locks and retaining duplicate keys; and by crafting policies that limit workers' expectation of privacy and permit searches under any circumstances. An organization can broaden its ability to search by creating company policy and advising employees that there is no privacy associated with specific aspects of work or workplace locations. It is important for the organization in this instance to document employee notification of those policies and to apply the policies without discrimination. For the investigator, considerations around invasion of privacy include limiting the use of the methods of investigation in those areas where an employee could conceivably have an expectation of privacy.

Entrapment

Employers shy away from undercover investigations for many reasons. But among the most common and unnecessary is the fear of entrapment. Employers and sometimes the lawyers that represent them fear entrapment because they don't understand it. Contrary to popular belief, entrapment is not a crime. It is not something bad employers do to innocent employees. Entrapment is not something for which one might be punished or even admonished. Entrapment is nothing more than a criminal defense. Because entrapment is a criminal defense, only the government can entrap. What's more, the defense of entrapment can only be used after a defendant admits to the commission of the crime.

Eugene F. Ferraro and Brad Mathers

WOUNDS: TRAUMA CAUSED BY SHOOTING AND CUTTING

In gunshot cases, a bullet entrance wound is usually a neat, round hole made by a bullet entering the body. The shape of an exit wound will vary according to where it exits (whether through a fleshy or bony structure), the shape of the bullet as it exits (whether pristine or flattened), and the motion of the bullet (whether spinning or tumbling). Exit wound shapes include marks that are stellate (star-like), slit-like, everted (inside-out), and irregular.

A bullet exit wound is typically a ragged or torn hole made by a bullet leaving the body and is usually much larger than the size of the bullet.

An abrasion collar is a narrow ring around the entry of a bullet hole in the skin. The skin, being resistant and elastic, will be stretched by the impacting bullet. A narrow ring around the bullet hole is formed by the abrasive action of the bullet. The ring may also contain residues from the surface of the bullet.

A contact or tattooed gunshot wound is a close-range wound characterized by gunpowder tattooing in and around the bullet hole. The tattooing consists of charring at the entry point, and powder grains and combustion products embedded in the skin. The wound results when the muzzle of the gun has been firmly applied to the skin at the instant of firing. When the muzzle is against a bony structure, such as the head, the blast causes a lacerated, charred wound that shows flame burns of the skin and hair from the rapidly expanding explosive gases. Smudges from carbon deposits appear within the subcutaneous tissue, muscle, and bone. A distinct abraded and contused imprint, with the laceration in the shape of a star, will very likely appear on the skin. When the muzzle is in contact with soft flesh, such as the abdomen, the star-shaped laceration and flame burns are not present because the exploding gases of the muzzle blast are dispersed without resistance into the abdominal cavity.

A near-contact gunshot wound results when the muzzle, at time of discharge, is approximately 2 inches or less from the victim but not in contact with the skin. The wound is rounded with inverted abraded edges, surrounded by a zone of scorching, soot deposits, and compact tattooing from powder grains embedded in the skin.

A close-range gunshot wound is a wound caused when the muzzle, at time of discharge, is 2–24 inches from the victim. As the distance between a gun and the skin is increased, the flame burns diminish and powder grains embedded in the skin (tattooing) are spread in a widening circle around the bullet entry hole. Eventually, the tattooing effect disappears. When a bullet fired at close range first passes through clothing or some other substance, the tattooing effect may not be visible at all, thereby giving the appearance of a distant shot.

A distant wound is a wound caused by a bullet that traveled in excess of at least 2 feet from muzzle to victim. A distant wound is apparent by the absence of flame, smoke, and tattooing marks characteristic of a shot made in contact or in close contact with the victim. When a bullet penetrates the body perpendicular to the skin, it produces a round wound with abraded margins, called a collar abrasion. When a bullet penetrates the skin at an angle, the direction from which it enters the skin is indicated by a triangular abrasion and undermining of the skin. A bullet that grazes but does not penetrate the skin will produce a rectangular abrasion of the skin, called a bullet rub.

A beveled wound or a tangential gunshot wound results when the skin is penetrated at an angle. One margin of the wound is beveled and the other margin overhangs it. A residue track may be visible.

Marks from shotgun wounds have similar characteristics and are potentially classifiable as to the distance separating the victim and the shotgun muzzle at time of discharge. Four classifications are generally recognized: (1) the direct contact wound, which shows an imprint of the muzzle on the skin or which indicates contact by massive destruction of bone and tissue; (2) the up-close or loose-contact wound, which shows a small diameter entry pattern having abraded edges surrounded by a zone of considerable scorching, soot, and powder residue; (3) the close-range or near-range wound, which has a larger diameter entry pattern consistent with a discharge at 4–6 feet and shows abraded, scalloped margins, wad-impact abrasion, and wide dispersal of powder residue, soot, and smoke stains; and (4) the distance wound, which has a very large-diameter entry pattern consistent with a discharge at greater than 6 feet and shows scattered, small, round pellet holes with abraded margins.

In cutting and stabbing cases, a cleavage line wound is a gaping wound produced by cutting or stabbing perpendicularly to a cleavage line. The wound will appear to have been caused by a large blade or a deep cutting action. The gaping aspect, however, results from a distortion of the muscle fibers that provide a normal tension to the skin. Defense wounds are often found on the victim's hands and arms. The wounds evidence the manner in which the victim maneuvered to fend off the attacker. Wounds made by cutting instruments are called incised wounds.

A wrinkle wound results from a cutting or stabbing action that produces multiple cuts or punctures along the line of the blade, with interspersed areas of uninvolved skin. Wrinkle wounds are usually associated with obese or elderly victims.

John J. Fay

Source Fay, J. 1987. *Butterworths Security Dictionary*. Boston: Butterworth–Heinemann.

V: Legal Aspects

ARREST LAW

Because our justice system places a high value on the rights of the individual citizen, private and public officers cannot simply arrest, search, question, and confine a person by whim. A consideration of individual rights is an important factor. The Bill of Rights of the U.S. Constitution affords citizens numerous protections. If we examine the Fourth and Fifth Amendments of the Bill of Rights, we can see how individual rights are safeguarded during criminal investigations.

Amendment IV: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation; and particularly describing the place to be searched, and the person or things to be seized."

The Fourth Amendment stipulates guidelines for the issuance of warrants. Public and private police obtain arrest and search warrants from an impartial judicial officer. Sometimes immediate action (e.g., chasing a bank robber) does not permit time to obtain warrants before arrest and search. In such a case, an arrest warrant is obtained as soon as possible. Private police should contact public police for assistance in securing warrants and in apprehending suspects.

Amendment V: "... nor shall [any person] be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law."

The Sixth, Eighth, and Fourteenth Amendments are other important amendments frequently associated with our criminal justice process. Briefly, the Sixth pertains to the right to trial by jury and assistance of counsel. The Eighth states that "excessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishments inflicted." The Fourteenth bars states from depriving any person of due process of law or equal protection of the laws.

Probable Cause

A key factor to support a legal arrest and search is "probable cause," which means that there are reasonable grounds to justify legal action. An eyewitness viewing of a crime would support probable cause in an arrest warrant.

Knowledge of arrest powers is essential for those likely to exercise this authority. These powers differ from state to state and depend on the statutory authority of the type of individual involved. Generally, public police officers have the greatest arrest powers. They are also protected from civil liability for false arrest, as long as they had probable cause that the crime was committed. Those in the private sector have arrest powers equal to citizen arrest powers which means that they are liable for false arrest if a crime was not, in fact, committed—regardless of the reasonableness of their belief. An exception is apparent if state statutes point out that these personnel have arrest powers equal to public police only on the protected property. If private sector personnel are deputized or given a special constabulary commission, their arrest powers are likely to equal those of public police.

Whoever makes an arrest must have the legal authority to do so. Furthermore, the distinction between felonies and misdemeanors, for those making arrests, is of tremendous importance. Felonies are considered more serious crimes and include burglary, armed robbery, murder, and arson. Misdemeanors are less serious crimes such as trespassing, disorderly conduct, and being drunk in public. Generally, public police can arrest someone for a felony or a misdemeanor committed in view. Arrest for a felony not seen by the public police is lawful with probable cause; arrest for a misdemeanor not seen by the public police is unlawful, and a warrant is needed based upon probable cause. On the other hand, private police have less arrest powers (equal to citizen arrest powers). Basically, citizen arrest powers permit felony arrests based upon probable cause, but prohibit misdemeanor arrests.

A serious situation evolves when, for example, a private officer mistakenly arrests a person for a misdemeanor thinking that the offense was a felony, or when the jurisdiction in which the arrest occurred does not grant such authority. Many employers in the private sector are so afraid of an illegal arrest, and subsequent legal action, that they prohibit their officers from making arrests without supervisory approval. It is imperative that private sector personnel know state arrest law.

An illegal arrest may lead to civil and/or criminal prosecution of the arrestor. False arrest may be grounds for a civil action for damages. If an illegal arrest has resulted in the death of the arrestee, an arrestor can be prosecuted for homicide.

Force

During the exercise of arrest powers, force may be necessary. The key criterion is "reasonableness." Force should be no more than what is reasonably necessary to carry out legitimate authority. If an arrestee struggles to escape and is subdued to the ground, it would be unreasonable for the arrestor to step on the arrestee's face. Although jurisdictions vary, "deadly force" is usually reserved for life-threatening situations. Unreasonable force can lead to difficulties in prosecuting a case, besides civil and criminal litigation.

Searches

A legal arrest is a prerequisite to a search. Ordinarily, a public police officer conducts a search of an arrestee right after arrest. This has been consistently upheld by courts for the protection of the officer who may be harmed by a concealed weapon. However, evidence obtained through an unreasonable search and seizure is not admissible in court; this is known as the "exclusionary rule." In reference to private sector officers, who generally have citizen arrest powers, the law is not clear and varies widely. Generally, a search is valid when consent is given and where, in a retail environment, a shoplifting statute permits the retrieval of merchandise. A search for weapons may be justified through common law, which states that citizens have the right of self-defense. The recovery of stolen goods as the basis for a search is typically forbidden, except in some state shoplifting statutes.

Though the law of searches by private police is not as well developed as for public police, court cases are evolving that are changing this situation. In the California Supreme Court decision *People v. Zelinsky*, 24 Ca. 3d.357, handed down in 1979, the court ruled, in essence, that the exclusionary rule applies to private security officers.

This decision involved a shoplifting case in which Virginia Zelinsky placed a blouse in her purse without paying for it. She was stopped outside the store and escorted to the security office. When the officers opened her purse and found the blouse, they also discovered a vial of heroin. She went to trial on a charge of possession of narcotics. Zelinsky requested the judge to suppress the heroin because it had been seized illegally. The judge denied her request stating that store detectives are not governed by the prohibition against unreasonable searches. On appeal, the California Supreme Court disagreed. What was also significant about this case was that the court had ruled that when private security officers investigate crimes, their acts are "government actions," so the full force of the Constitution governs those acts.

Questioning

An important clause of the Fifth Amendment states that a person cannot be compelled in any criminal case to be a witness against himself. What constitutional protections does a suspect have upon being approached by an investigator for questioning? Here again, the law differs with respect to public and private sector investigations.

Basic criminal law states that a person about to be questioned about a crime by public police must be advised of:

1. The right to remain silent.
2. The fact that statements can be used against the person in a court of law.
3. The right to have an attorney present, even if the suspect has no money.
4. The right to stop answering questions at any time.

These rights, known as "Miranda rights," evolved out of a 1966 Supreme Court case known as *Miranda v. Arizona*. If these rights are not read to a person (by public police) before questioning, the statements or a confession of the accused will not be admissible as evidence in court.

Are private police required to read a person the Miranda warnings prior to questioning? The courts have not yet required the reading.

However, any type of coercion or trick during questioning is prohibited for private as well as public police. A voluntary confession by the suspect is in the best interests of public and private investigators. Many private sector investigators choose to read suspects the Miranda warnings as a protection against legal challenge.

Philip P. Purpura

Source Purpura, P.P. 2002. *Security and Loss Prevention, 4th Edition*. Boston: Butterworth-Heinemann.

BUSINESS LAW

Business and law are inextricably linked; the law determines who may engage in business, how business is to be carried out, and the penalties that apply when the law is broken. An understanding of the law as it relates to business is indispensable to the security manager.

An understanding of business law means knowing the origins of law, how they have changed and are continuing to change, and how they are currently applied. The particular areas of interest to the security manager are constitutional law, statutory law, case law, administrative law, and the role of ethics in influencing business conduct.

Sources of Law

Law acts as an instrument of social control and of change. Many of the laws that regulate business, for example, have evolved in response to societal demands. In responding to the will of society, the law is in a constant state of flow, ebbing and rising in relation to pressures from many different sources. We see this, for example, in restrictions designed to protect ecological systems. Clearly, law has a profound impact on the decisions of managers in all disciplines and at all levels in a business organization.

The security manager's view of the law will necessarily be both broad and purposeful. It will be broad in the sense that the law expresses concepts that generally ascribe to the notion that for civilization to be functional there must be a body of rules enforced by the government for the good of the people. The security manager's view will be purposeful because it will focus on functional purposes, such as prevention of crime, maintenance of order, investigation of crime, and apprehension of violators. This view acknowledges that the law is not just a statement of rules of conduct, but also the mechanism for dealing with violations and affording remedies.

American law has four sources: (1) the U.S. and state constitutions, (2) legislation or statutory law, (3) judicial decisions or case law, and (4) the rules and regulations of governmental agencies or administrative law. The general priority among the various sources of law is that constitutions prevail over statutes, and statutes prevail over common-law principles established in court decisions. Courts will not turn to judicial decisions for law if a statute is directly applicable.

The rules and principles that are applied by the courts fall into three groups: (1) laws that have been passed by legislative bodies; (2) case law, derived from cases decided by the courts; and (3) procedural rules, which determine how lawsuits are handled in the courts and include matters such as the rules of evidence. The first two groups are used by the courts to decide controversies. They are often called substantive law. The third group, known as procedural law, provides the machinery whereby substantive law is given effect and applied to resolve controversies.

Substantive law defines rights, whereas procedural law establishes the procedures by which rights are enforced and protected. For example, Jones claims that Smith should reimburse him for losses sustained in a burglary at the apartment that Jones rented from Smith. The rules that provide for bringing Smith into court and for the conduct of the trial constitute procedural law. Whether Smith had a duty to protect Jones against burglary and whether Jones is entitled to damages are matters of substance that would be determined on the basis of the substantive law.

Private law pertains to the relationships between individuals. It encompasses the subjects of contracts, torts, and property. The law of torts is a chief source of litigation. A tort is a wrong committed by one person against another or against his property. The law of torts holds that people who injure others or their property should compensate them for their loss.

Constitutional Law

The Constitution of the United States and the constitutions of the various states form the foundation of our legal system. All other laws must be consistent with them. A federal law cannot violate the U.S. Constitution; all state laws must conform to the federal Constitution, as well as with the constitution of the appropriate state.

Statutory Law

Much of law is found in legislation. Legislation is the expression of society's judgment and the product of the political process. Legislative bodies exist at all levels of government. Legislation is created by Congress, state legislatures, and local government bodies. Legislation enacted by Congress or by a state legislature is usually referred to as a statute. Laws passed by local governments are frequently called ordinances. Compilations of legislation at all levels of government are called codes. For example, we have city fire codes that cover fire safety, state traffic codes that regulate the operation of motor vehicles, and, at the federal level, we have the U.S. Code consisting of statutes that regulate general conduct.

Substantial differences in the law exist among the various states simply because each state has its own constitution, statutes, and body of case law. Two methods of achieving uniformity in business law are possible: (1) having federal legislation govern business law, and (2) having uniform state laws for certain common business transactions. The latter method has produced more than 100 model uniform laws concerning such subjects as partnership, leases, arbitration, warehouse receipts, bills of lading, and stock transfers. The most important development for business in the field of uniform state legislation has been the Uniform Commercial Code (UCC).

Case Law

A very substantial part of law is found in cases decided by the courts. This concept of decided cases as a source of law is generally referred to as case law and has been a predominant influence in the evolution of the body of law in the United States. Case law is important because of the great difficulty in establishing law in advance of an issue being raised.

When a case is decided, the court writes an opinion. These written opinions, or precedents, make up the body of case law. The concept of precedent is linked to a doctrine called *stare decisis*, which means "to stand by decisions and not to disturb what is settled." *Stare decisis* holds that once a precedent has been set, it should be followed in later cases involving the same issue. In this way, the law takes on certainty and predictability. *Stare decisis* is also flexible. If a court, especially an appeals court, finds that the prior decision was wrong or that it is no longer sound under prevailing conditions, it may overrule and change the decision. Although *stare decisis* introduces some degree of consistency, the system is far from perfect. Precedents (and statutes) vary from state to state. In some states the plaintiff in a negligent security case must be completely free of fault in order to recover damages; in most other states the doctrine of comparative negligence is used, so that a plaintiff found to be 10 percent at fault can recover not more than 90 percent of his damages.

Administrative Law

Administrative law is concerned with the many administrative agencies of the government. This type of law is in the form of rules and regulations promulgated by an administrative agency created by a state legislature or by the Congress to carry out a specific statute. For example, in a variety of statutes the Congress gives authority to the U.S. Department of Transportation (DOT) to regulate the nation's transportation systems (air, maritime, highway, railroad, pipeline, and metropolitan transit). The rules put into effect by DOT are in the nature of law to the regulated parties, e.g., the air, sea, motor, and rail carriers engaged in interstate transportation.

The powers and procedures of the administrative agencies do not always correspond exactly to the general intent of the legislature. By its very nature, most legislation is general, and interpretation is necessary to carry out the intent of the legislative body when it passed an act. The rules that implement a legislative act are often the interpretation of a government administrator. Since it is not possible to precisely express

legislative intent in words that mean the same thing to everyone, the rules and regulations are often approximations that, when implemented, are quickly challenged by the affected parties.

Ethics

Ethics play a part in influencing conduct and regulating the behavior of individuals and businesses. Concern for the consequences of one's actions is clearly a powerful motivator. For example, as security professionals we are concerned about the damage to our reputations that would follow if we were found to have engaged in practices that were unethical or immoral, although not necessarily illegal. Business entities have similar fears based on economic consequences. Personal and institutional ethical standards are having an ever-increasing impact on decisions. Almost every publicly held business has adopted a code of ethical conduct for its employees; the federal government has one for its employees; and nearly all trade and professional associations, including the American Society for Industrial Security, adhere to ethical codes. While these codes are not laws, they are usually enforced and provide penalties for non-compliance.

Ethical conduct is based on a personal commitment to do what is correct and to not do what is wrong. Ethical standards articulate values that go beyond what the law specifically demands and proscribes. The law provides a floor above which ethical conduct rises. Although ethical standards are usually considered to be extensions beyond the law, they are sometimes enacted into law when legislatures bring the law into alignment with society's views of right and wrong.

In the business environment, ethical conduct normally exists at a level well above legal minimums. It often means doing more than the law requires or less than it allows. Codes of ethics adopted by businesses can be thought of as internal work rules for all persons subject to them. Typically, they are based on fairness and honesty, and most provisions only require disclosure of facts to superiors in particular situations, while a few may dictate certain decisions and conduct. Codes of ethics state a collective sense of right and wrong, usually in the broadest of terms.

John J. Fay

Source Corley, R. and Shedd, P. 1989. *Principles of Business Law, 14th Edition.* Englewood Cliffs: Prentice-Hall.

CONCEPTS IN NEGLIGENCE

Negligence is the doing of that thing which a reasonably prudent person would not have done, or the failure to do that thing which a reasonably prudent person would have done in like or similar circumstances. It is the failure to exercise that degree of care that reasonably prudent persons would have exercised in similar circumstances.

Tort law has attempted to refine the concept of negligence by subdividing it into narrower categories. Degrees of care and degrees of negligence are closely related but separate approaches in refining negligence. Degrees of care is the amount of care that is reasonable for a given situation. It depends on various factors, including the relationship between the parties and the nature and extent of the risk inherent in that situation. For example, transporting school children requires a higher degree of care than hauling watermelons.

Degrees of negligence embraces the idea that negligence may be classified as slight or gross. This has been a persistent theme in tort law and criminal law. There are statutes in which the term negligence is preceded by some adjective, such as "slight" or "gross." In most cases, the statute applies only to a particular situation or activity.

Slight negligence is the failure to exercise great care. It is not a slight departure from ordinary care. Technically, it is the failure to exercise greater care than the circumstances would ordinarily require. On the other hand, gross negligence is something more than ordinary negligence but only in degree. It is less than recklessness, which is a different kind of conduct showing a conscious disregard for the safety of others. The distinction is important since contributory negligence is not a defense to wanton misconduct but is to gross negligence. A finding of reckless misconduct will usually support an award of punitive damages whereas gross negligence will not.

Contributory negligence is an act or omission amounting to want of ordinary care on the part of a complaining party, which, concurring

with the defendant's negligence, is the proximate cause of injury. Contributory negligence generally applies to a condition of employment, either express or implied, with which an employee agrees that the dangers of injury ordinarily or obviously incident to the discharge of required duties will be at the employee's own risk.

Negligent conduct is an element of various tort causes of action. The components of the cause of action for negligence are: (1) a duty owed by the defendant to the plaintiff, (2) a violation of that duty by the defendant's failure to conform to the required standard of conduct, (3) sufficient causal connection between the negligent conduct and the resulting harm, and (4) actual loss or damage. The plaintiff's contributory negligence, if any, will reduce or defeat a claim. In many jurisdictions, contributory negligence is a defense to be pleaded and proved by the defendant, but in some jurisdictions the plaintiff must allege and prove his freedom from contributory negligence as a part of his case.

Negligent conduct can be alleged in an employer's hiring practices. The term *negligent hiring* refers to a concept that holds an employer directly liable for an employee's harmful conduct after the employer failed to exercise reasonable care in hiring the employee. Although similar to *respondeat superior*, this concept can extend to situations that occur outside of the workplace. For example, assume that during working hours a security officer makes a date with a female employee. During the date (off the employer's premises and during non-working hours) the officer rapes the other employee.

She learns that the employer was aware that this same officer had assaulted other women whom he had met at work, but had hired him anyway without warning her or other female employees. The employer can be charged with failure to exercise reasonable care in the hiring and retention of a dangerous employee.

The "reasonable person" concept applies objective standards of reasonableness when judging whether conduct is negligent. The law does not make special allowance for the particular weaknesses of a person acting negligently. Conduct that creates an unreasonable risk of harm is no less dangerous because the actor lacked the capacity to conform to an acceptable level of performance. While it may seem unfair to hold some people to standards they cannot always meet, it would be more unjust to require the innocent victims of substandard conduct to bear the consequences.

The standard is usually stated as reasonable care, ordinary care, or due care, and is measured against the hypothetical conduct of a hypothetical person, i.e., the reasonable human of ordinary prudence. Such a person is not the average or typical person, but an idealized image. He is a composite of the community's judgment as to how the typical citizen ought to behave in circumstances where there is a potential or actual risk of harm. The reasonable person is not perfect or infallible. He is allowed mistakes of judgment, of perception, and he may even be momentarily distracted. Above all, he is human and prone to errors, but such errors must have been reasonable or excusable under the circumstances.

The law of negligence distinguishes between liability for the consequences of affirmative acts (misfeasance) and liability for merely doing nothing (nonfeasance).

Almost any inaction can be characterized as misfeasance if the court is so disposed, and often inaction is substantially the equivalent of active misconduct. The failure to repair defective brakes may be seen as active negligence. A fundamental question is whether there is a sufficient relationship between the one who failed to act and the one injured as a result.

A common example is the absence of a duty to go to the aid of someone needing help (when such help is not required by some preexisting status or relationship). A person skilled in administering cardiopulmonary resuscitation is not required to aid a victim needing such assistance, unless the person happens to also be a paramedic hired for that purpose.

Duties of affirmative action that would not otherwise exist may be voluntarily assumed. It is commonly held that one who freely undertakes to render aid to another assumes a duty to act with reasonable care, and once the duty is assumed it may not be abandoned. This rule is thought by many to have the negative effect of discouraging rescuers.

John J. Fay

Source Fay, J. 1987. *Butterworths Security Dictionary: Terms and Concepts*. Boston: Butterworth-Heinemann.

COURTS: PROSECUTION IN STATE COURTS

A chief prosecutor is the attorney who advocates for the public in felony cases, as well as in a variety of other cases. A prosecutor's responsibilities are limited geographically. A prosecutorial district follows county lines and typically consists of a single county but may include two or more.

In the recent past half of these officials had the title of either district attorney or county attorney. A chief prosecutor may have a staff of "assistant prosecutors," attorneys who do much of the actual case work.

The prosecutor usually does not know of a felony matter until a law enforcement agency made an arrest. Because 95 percent of prosecutors receive felony cases from three or more arresting agencies, an opportunity exists for considerable variation in the time between arrest and notification of the prosecutor's office. About 73 percent of law enforcement agencies in the United States are state or local police departments and 18 percent are county sheriff's departments; the remainder are special agencies such as transit police or campus police.

Some prosecutors are notified only after the arresting agency has filed papers in a special or "lower" court. This court conducts necessary pre-trial events, such as informing the accused person of the charges, setting bail, and assigning defense counsel.

When a staff attorney handles all phases of a criminal case, the processing is known as "vertical" case assignment. A career-criminal unit is an example of a vertical case assignment in which certain assistant prosecutors handle repeat offenders from the targeting stage onward. "Horizontal" assignment means that different assistants specialize in different phases—drafting complaints, conducting trials, or doing appellate work.

Indigent Defendants

The U.S. Constitution guarantees rights to citizens as they relate to the federal government and federal criminal prosecutions. Such rights are not automatically applicable to state governments and state criminal prosecutions. In lawsuits concerning specific rights, the U.S. Supreme Court decides the applicability of such rights to the states.

The Sixth Amendment to the U.S. Constitution establishes the right of a criminal defendant to have assistance of counsel for his or her defense. The Supreme Court has ruled that counsel must be available to any defendant who is at risk of a federal or state sentence of incarceration. This right extends to indigent defendants unable to pay a lawyer. If an indigent defendant who faces a penalty of incarceration wants a lawyer, the state must either provide a lawyer or seek a lesser penalty.

Filing

After a document charging a person with a crime is submitted to the felony court, an event known as a case "filing," the court takes control of the case. Most felony cases begin with the filing of an indictment issued by a grand jury. In most other felony cases, the charging document is an "information" filed by the prosecutor. Either type of document states who the accused person is and what illegal acts were committed. To proceed on the basis of an information rather than an indictment, the prosecutor normally must present the case in a preliminary hearing, which in some places occurs in a lower court. In a preliminary hearing, the judge reviews the facts and circumstances of the case to determine whether there are reasonable grounds ("probable cause") to believe the accused person committed the crime for which he or she is being charged. The accused person may waive any right to have the matter reviewed by grand jury. Such waivers often occur, particularly when the accused decides to plead guilty early in the case.

The Fifth Amendment to the Constitution establishes that a citizen accused of a felony has the right to have a grand jury, rather than the prosecutor, decide whether he or she shall be prosecuted. Except in cases that could involve a death sentence, the accused may waive this right. The grand jury right does not apply to prosecutions in state courts. About half of the states, however, have laws allowing or requiring the use of grand juries in felony cases.

Where grand juries are used, an indictment takes precedence over the prosecutor's view of whether probable cause exists in a case. The court rather than the prosecutor convenes grand juries. In districts with grand juries, however, judges of a lower court or a felony court often screen cases for probable cause, providing for greater grand jury efficiency.

Criminal History Data

When a person is arrested or brought before a court on a criminal charge, usually a government agency keeps a permanent official record of the event. These records enable prosecutors to find out about a person's "criminal history." That knowledge can help prosecutors make proper decisions.

Plea Negotiation

In a vast majority of felony convictions, the defendant pleads guilty rather than requests a trial. The high percentage of guilty pleas is a key factor in minimizing case backlogs. Guilty pleas often result from negotiations: the defendant agrees to plead guilty to a lesser charge or to a charge for which the prosecutor recommends a reduced sentence. The court may impose deadlines on negotiations when responding to requests for extensions of time or continuances. Requests for more time to negotiate a plea agreement are sometimes made on the day of trial, even when witnesses, juries, and court personnel have already assembled.

Speedy Trial

The Sixth Amendment of the U.S. Constitution guarantees to the accused in a criminal trial, whether federal or state, the right to a speedy trial. In recent years legislatures and courts have established limits on the time following an arrest that a prosecutor has to bring the case to trial. Such speedy trial requirements often apply when a defendant is held in custody, but do not apply when the defendant has been granted pre-trial release.

Jury Trial

The Sixth Amendment to the U.S. Constitution gives state and federal felony defendants the right to trial by jury. This right may be vaived in favor of trial by judge. An estimated 4 percent of all felony convictions are the result of a judge trial.

In some jurisdictions the prosecutor also has the right to have a case tried by a jury. In such jurisdictions, the jury may be used even if the defendant prefers a judge trial, although how the proceedings are carried out is decided by the trial judge. The prosecutor may exercise this right to a jury trial for many reasons, including belief that

- A jury is more likely than a particular judge to convict.
- A jury is likely to impose or recommend a desired sentence.
- A jury trial will attract more public attention to a defendant's heinous conduct.

Policies and Practices after Trial

A convicted defendant remains under the court's jurisdiction until sentencing. Between conviction and sentencing, information is often gathered to enable the judge to impose an appropriate sentence. In most districts the judge requests a pre-sentence report containing information about the defendant, family and enployment circumstances, mental or physical health problems, and history of drug or alcohol abuse. This information may have an important bearing on the choice between a sentence of confinement and a sentence of probation.

A convicted defendant may appeal to a higher court, asking it to review any defect in the proceedings of the original trial. Only certain major issues, such as the sentence or what trial evidence was admitted or excluded, will serve as a basis for the appeals court accepting the appeal. Under some circumstances the prosecutor may also appeal. The special condtions for a prosecutorial appeal usually do not include the prosecutor's view of the determination of guilt in a particular case.

An appeal involves two main activities: preparing the written document (brief) that explains

both the case and the defects complained of, and presenting this material verbally to the appeals judges (oral argument).

Source "Special Report." *Bureau of Justice Statistics*. 1992.

CRIMINAL JUSTICE PROCEDURE

The criminal justice system operates as a process. Following is a brief and generalized description of the process.

1. The purpose of an arrest is to bring the person into the criminal justice system so that he/she may be held to answer the criminal charges.
2. A citation is frequently used by public police instead of a formal arrest for less serious crimes (e.g., traffic violation). If the conditions set forth in the citation are not followed, a magistrate of the appropriate court will issue a misdemeanor warrant.
3. All arrests must be based on probable cause which is stated in arrest warrants. Probable cause, which is more than mere suspicion, is reasonable grounds to justify legal action. A viewing of an assault would be good probable cause.
4. Booking takes place when an arrestee is taken to a police department or jail so that a record can be made of the arrested person's name, the date, time, location of offense, charge, and the arresting officer's name. Fingerprinting and photographing are part of the booking process.
5. Because our system of justice has a high regard for civil liberties as expressed in the Bill of Rights, the accused is informed, usually right after arrest, of the Miranda rights.
6. After booking, and without unnecessary delay, the accused is taken before a magistrate for the "initial appearance." At this appearance the magistrate has the responsibility of informing the accused of constitutional rights, stating the charge, and fixing bail (if necessary).
7. Also after booking, the arresting officer will meet with the prosecutor or prosecutor's representative to review evidence. A decision is made whether to continue legal action or to drop the case. A case may be dropped by the prosecutor for insufficient evidence or when the case can be better handled by another agency, such as a mental health agency.
8. The prosecutor prepares an "information" when prosecution is initiated. It cites the defendant's name, the charge, and is signed by the complainant (e.g., the person who witnessed the crime). An arrest warrant is prepared by the proper judicial officer. The defendant may already be in custody at this point.
9. At the initial appearance, the magistrate will inform the defendant about the right to have a preliminary hearing. The defendant and the defense attorney make this decision. The hearing is used to determine if probable cause exists for a trial. The courtroom participants in a preliminary hearing are a judge, defendant, defense attorney, and prosecutor. The prosecutor has the "burden of proof." Witnesses may be called by the prosecutor to testify.
10. Federal law and the laws of more than half the states require that probable cause to hold a person for trial must result from grand jury action. The Fifth Amendment of the Bill of Rights states such a requirement. When probable cause is established, the grand jury will return an "indictment" or "true bill" against the accused. A "presentment" results from an investigation initiated by a grand jury establishing probable cause. Based on indictment or presentment, an arrest warrant is issued.
11. At an "arraignment" the accused enters a plea to the charges. Four plea options are: guilty, not guilty, *nolo*

contendere (no contest), and not guilty by reason of insanity.

12. Few defendants reach the trial stage. Plea bargaining is an indispensable method to clear crowded court dockets. Essentially, it means that the prosecutor and defense attorney have worked out an agreement whereby the prosecutor reduces the charge in exchange for a guilty plea. Charges may also be dropped if the accused becomes a witness in another case.
13. Pre-trial motions can be entered by the defense attorney prior to entering a plea at arraignment. Examples: A motion to quash an indictment or information because the grand jury was improperly selected. The defense attorney may request a continuance because more time is needed to prepare the case. A change of venue is requested when pre-trial publicity is harmful to the defendant's case. The defense hopes to locate the trial in another jurisdiction so that an impartial jury is more likely to be selected.
14. The accused is tried by the court or a jury. The prosecutor and defense attorney make brief opening statements to the jury. The prosecutor presents evidence. Witnesses are called to the stand to testify; they go through direct examination by the prosecutor, followed by defense cross-examination. The prosecutor attempts to show the defendant's guilt "beyond a reasonable doubt." The defense attorney strives to discredit evidence. Redirect examination rebuilds evidence discredited by cross-examination. Recross-examination may follow. After the prosecutor presents all the evidence, the defense attorney may ask for acquittal. This motion is commonly overruled by the judge. The defense attorney then presents evidence. Defense evidence undergoes direct and redirect examination by the defense, and cross- and recross-examination by the prosecutor.

Next, the judge will "charge the jury," which means that the jury is briefed by the judge on the charge, and how a verdict is to be reached based on the evidence. In certain states, juries have responsibilities for recommending a sentence after a guilty verdict; the judge will brief the jury on this issue. Closing arguments are then presented by opposing attorneys.

The jury retires to the deliberation room, a verdict follows. A not guilty verdict signifies release for the defendant. A guilty verdict leads to sentencing. Motions and appeals may be initiated after the sentence.

Philip P. Purpura

Source Purpura, P. 2002. *Security and Loss Prevention, 4th Edition*. Boston: Butterworth-Heinemann.

DEFENSES TO CRIME

The law allows many defenses to charges of crime and it is the right of the accused to use any and all of them. The concept of defenses against prosecution may be viewed from two aspects: the basic capacity of the accused to commit the crime charged, and the applicability of certain specifically accepted defenses.

Capacity Defenses

The concept called "capacity to commit crime" demands that a person should not be held criminally punishable for his conduct unless he is actually responsible for it. Young persons and mentally afflicted persons, for example, may be recognized as not having the capacity to commit crimes, because they lack a sufficient degree of responsibility.

The infancy defense holds that children are incapable of committing any crime below a certain age, that at a higher age there is a presumption of incapacity to commit crime, and at an even higher age certain crimes are conclusively presumed to be beyond the capability of a child. For example, it may be presumed that a toddler is incapable of stealing and a 10 year old is incapable of committing the crime of rape.

The corporation defense holds that because a corporation is an artificial creation, it is

considered incapable of forming the requisite criminal intent. This defense has been largely overcome in recent years. Some crimes, such as rape, bigamy, and murder, cannot logically be imputed to a corporation.

The insanity defense holds that a person cannot be held liable for his criminal act if he was insane at the time of the act. The defense goes to the heart of the fundamental principle of intent, or guilty mind. If the accused did not understand what he was doing or understand that his actions were wrong, he cannot have criminal intent and, without intent, there is no crime.

The intoxication defense is similar to that of the insanity defense. It argues that the accused could not have a guilty mind due to intoxication. The fact of voluntary intoxication is generally not accepted as a defense. Involuntary intoxication produced by fraud or coercion of another may be a defense, and insanity produced by intoxicants may be acceptable.

Intoxication can also be offered as evidence that an accused was incapable of forming the intent to commit a crime, e.g., the accused was too drunk to entertain the idea of breaking and entering into a house at night for the purpose of committing an offense.

Specific Defenses

The alibi defense seeks to prove that because the defendant was elsewhere at the time the offense occurred, the defendant cannot be accused.

The compulsion or necessity defense argues that a person should not be charged with a crime when the act was committed in response to an imminent, impending, and overwhelmingly coercive influence. For example, a person who is ordered to drive a getaway car under the threat of immediate death would not be punishable as a principal to the crime.

The condonation defense is used in some rare cases where the law allows an accused not to be prosecuted if certain conditions are met. For example, a charge of seduction might be dropped if the parties involved subsequently marry.

The immunity defense grants protection from prosecution in exchange for cooperation by the accused. The required cooperation might be a full disclosure of all facts and testimony at trial.

The consent defense may be used when consent of the victim is involved. Where consent is offered as a defense, the consent must have been given by a person legally capable of giving it and it must be voluntary.

The entrapment defense argues that an accused should not be charged if he was induced to commit a crime for the mere purpose of instituting criminal prosecution against him. Generally, where the criminal intent originates in the mind of the accused and the criminal offense is completed by him, the fact that a law enforcement officer furnished the accused an opportunity for commission does not constitute entrapment. A key point is that where the criminal intent originates in the mind of the officer and the accused is lured into the commission, no conviction may be had.

The withdrawal defense may sometimes be used in a prosecution for conspiracy. A conspirator who withdraws from the conspiracy prior to commission of the requisite overt act may attempt a defense based on withdrawal.

The good character defense may seek to offer evidence that the accused is of such good character that it was unlikely he/she committed the act. This is not a defense as a matter of law, but an attempt to convince a jury it was improbable for the accused to have committed the crime.

The defense of ignorance or mistake of fact argues that the accused had no criminal intent. This defense seeks to excuse the accused because he was misled or was not in possession of all facts at the time of the crime. For example, this defense might be used in a case where a homeowner injured someone who he thought was a burglar in his home, but who in fact was the invited guest of another member of the family. This defense is based on the grounds that a defendant did not know certain essential facts, that he could not have been expected to know them, and that there could be no crime without such knowledge. Mistake of law is a rarely allowed defense offered by an accused that he did not know his act was criminal or did not comprehend the consequences of the act.

The statute of limitations defense seeks to prevent prosecution on the grounds that the government failed to bring charges within the period of time fixed by a particular enactment. Not all crimes have time limitations for seeking prosecution, and some crimes, such as murder and other major crimes, have no limits whatsoever.

Irresistible impulse is a legal defense by which an accused seeks to be fully or partially excused from responsibility on the grounds that although he knew the act was wrong, he was compelled to its execution by an impulse he was powerless to control.

Necessity is the defense of justification of an otherwise criminal act on the ground that the perpetrator was compelled to commit it because a greater evil would have ensued had he failed to do so. Thus, one could plead necessity if he committed arson to destroy official documents that would otherwise have fallen into the hands of a wartime enemy.

The self-defense or defense of life rule is derived from English common law, which authorizes the use of deadly force in self-defense and in order to apprehend persons committing or fleeing from felonies. In many jurisdictions, the rule has been narrowed by statute so that the use of weaponry is limited only to defense of life situations and to some specific violent felonies, for example, murder, rape, aggravated assault, arson, or burglary. This protection against prosecution relies on the premise that every person has a right to defend himself from harm. A person may use, in self-defense, that force which, under all the circumstances of the case, reasonably appears necessary to prevent impending injury.

Diminished capacity is the decreased or less-than-normal ability, temporary or permanent, to distinguish right from wrong or to fully appreciate the consequences of one's act. It is a plea used by the defendant for conviction of a lesser degree of a crime, for a lenient sentence, or for mercy or clemency.

Former jeopardy is a plea founded on the common law principle that a person cannot be brought into danger of his life or limb for the same offense more than once. The former jeopardy defense is founded on the principle that a case once terminated upon its merits should not be tried again.

Double jeopardy can only be claimed when the second prosecution is brought by the same government as the first. When the act is a violation of the law as to two or more governments, the accused is regarded as having committed separate offenses.

The "but for" rule or the sine qua non rule holds that a defendant's conduct is not the cause of an event if the event would have occurred without it.

Related to legal defenses is the bill of particulars. It is a statement by the prosecution filed by order of the court, at the court's own request or that of the defendant, of such particulars as may be necessary to give the defendant and the court reasonable knowledge of the nature and grounds of the crime charged, such as the time and place, means by which it was alleged to have been committed, or more specific information.

The concept can also apply to the defendant; for example, a defendant who intends to rely on an alibi defense may be required to furnish the prosecuting officer with a bill of particulars as to the alibi. This bill sets forth in detail the place or places the defendant claims to have been, together with the names and addresses of witnesses upon whom he intends to rely to establish his alibi. The purpose of this procedure is to prevent the sudden and unexpected appearance of alibi witnesses whose testimony in the latter stage of a trial could cast reasonable doubt on the state's case.

By compelling advance notice, the prosecutor is afforded time to investigate the alibi, as well as the credibility of the alibi witnesses, and, in so doing, establish a position for refuting the alibi defense.

John J. Fay

Source Fay, J. 1987. *Butterworths Security Dictionary: Terms and Concepts.* Boston: Butterworth-Heinemann

THE DEPOSITION

A deposition is a legal proceeding conducted for the purpose of preserving the testimony of a witness for use in court. In this case, we are talking about a witness who is an expert witness. The deposition is usually held in a reasonably comfortable and private setting, very often the conference room of an attorney's office. The persons present are the witness, a notary public to administer an oath, a court reporter (usually a notary), and lawyers for all parties. The parties themselves or their representatives have a right to attend but seldom choose to do so.

The deposition begins by administering an oath to the witness. The lawyers take turns in asking the witness questions. A lawyer may skip a turn or take more than one turn. The proceeding is relatively informal, although serious to the outcome of the lawsuit. The reporter takes

down everything said and the reporter's record will later be typed and bound in a document called a deposition or a transcript. The deposition is essentially a tool for opposing lawyers to discover what a witness' testimony will be at trial. For example, the plaintiff's lawyer in deposing an expert witness for the defense:

- Will want to discover what the expert knows concerning the facts involved in the matter being litigated. The search here is for evidence that the expert will present in support of the defendant.
- Will want to discover if the expert knows of any facts that may be damaging to the defense, e.g., that the defendant may have been careless or failed to do something.
- Will want to commit the expert to the statements made under oath so that at trial the expert's testimony cannot be changed (at least not without difficulty and damage to the defense).
- Will look for ways to discredit the expert's testimony or to use the expert's testimony to discredit the testimony of other defense witnesses. Minor contradictions among witnesses are inevitable, while major contradictions or the appearance of them can be damaging.
- Will attempt to learn the basic theory and strategy that the defense will rely on at trial. The plaintiff's attorney may decide that the defense will be formidable against the claim as stated and that the claim needs to be changed.

Although a deposition can embarrass or even damage the reputation of an expert witness, this is not a legitimate purpose of the proceeding. When it happens, it is often the result of inadequate preparation by both the expert witness and the attorney that engaged the witness.

The expert witness has three fundamental obligations. First, is to tell the truth, even if the truth will hurt. This is an obligation that sits above the outcome of the lawsuit. Second, is to be fair. This does not mean that the witness has to give equal favor to both sides, only that the witness not overstate or color the facts. Third, is to be accurate, and this is where the expert witness plays a critical part in helping the judge and jurors fulfill their responsibilities in seeing that justice is carried out.

John J. Fay

Source Baker, T. 1992. *Operator's Manual for a Witness Chair.* Kansas City: Baker and Sterchi.

DETENTION FOR SHOPLIFTING

In the fight against shoplifting, merchants and their employees are directly on the front line. The statistics can vary widely, but it's safe to say that hundreds of thousands of individuals are detained for shoplifting each year in the United States, and although anti-shoplifting technology continues to improve, there will always be a need to detain shoplifters. Shoplifting is usually thought of as the concealment and subsequent theft of merchandise from a merchant, but shoplifting language can also include price-switching of merchandise, refunding for unpaid merchandise, and "sweet-hearting" of merchandise at the point of sale. The majority of shoplifting offenses are misdemeanor crimes unless a specific dollar amount is reached. In most states, this dollar amount falls within the $300 to $500 range, but in some states the value can be in excess of $1,000 before shoplifting becomes a felony crime.

A shoplifting detention is multi-faceted and should only be attempted by trained personnel. The many factors that must be considered include knowledge of the criminal elements that constitute a crime, the merchant's policy on detaining shoplifters, and strategies on how to make a detention as safely as possible. Additional considerations include how to respond to a problematic or violent person and how best to communicate with the person in order to obtain cooperation. While recovering property is the primary goal of any detention, it is important for employees to remember that safety should never be compromised. In addition to their own safety, employees should also consider the safety of bystanders. Liability to the merchant is an additional factor that needs consideration.

Necessary Elements

Prior to making a detention, a set of proofs, or elements, must be established, If not done, the merchant faces potential liability. It is generally acceptable for employees to detain suspected shoplifters based on probable cause.

Care, however, should be taken to avoid behavior that could lead to civil action. Such behavior can include making accusations in the hearing of others, unnecessary touching, unnecessary use of force, detaining the individual for a lengthy period of time, intimidating or browbeating the individual, denying the individual water or the use of a restroom, not calling the police immediately when it appears that arrest is the proper course of action, and being untruthful when giving details to the police or writing an incident report. For these reasons, many merchants require that their employees use standards higher than probable cause before detaining a suspected shoplifter.

Since shoplifting is simply "theft" or "larceny," the elements required are the same as for any other theft crime. Those elements being that the item in question has a value; that a taking and carrying away of the merchandise has occurred (i.e., selection); that there was no permission granted to take the merchandise; that the merchandise belonged to the merchant and that the person had the intent to permanently deprive the merchant of the merchandise. It's this last element of intent that is the most important and can be the most difficult to prove. This is why most, if not all, merchants require that the person has actually passed the last point of sale before allowing a detention. While not an actual element of the crime, this policy assists greatly in helping to prove the element of intent to permanently deprive. While concealment is also a great indicator of intent, shoplifters don't always conceal their merchandise. An employee must be aware of the fact that some shoplifters will simply walk out of the store with the merchandise.

Detention is appropriate only when an employee actually sees the selection and conversion of the merchandise through concealment or other means. The suspect should then be constantly watched. If the merchandise is discarded inside the store, detention is not appropriate. If the suspect is in possession of the merchandise after leaving the store, it is appropriate to stop the suspect. The employee making the stop should anticipate that the suspect will flee or offer resistance, including physical violence. The loss of merchandise is acceptable in lieu of injury to the employee or others.

Detention Strategies

No two detentions are ever the same and approaching a shoplifter with the intent to detain is not a task that should be taken lightly. The primary goal of a detention should be the safe recovery of the merchandise. Subsequent goals include identifying the person and possibly bringing criminal charges against them

Several considerations should be taken into account before actually approaching the shoplifter. The first of these is the behavior of the shoplifter. While it's impossible to exactly predict what a shoplifter will do, paying attention to certain behavioral indicators can help in planning the approach. Does the person appear to be nervous or confident? Did the person take a long time to actually conceal the product or did the person do it quickly? Consideration also needs to be given to the assistance that might be needed. Does the person's size, appearance, or demeanor indicate a type of reaction? If there's a feeling that the person might resist or run, a decision needs to be made to either obtain additional assistance or to simply avoid approaching the individual.

Ideally, shoplifters should be approached with an assertive and confident posture. The tone of voice should be matter of fact but polite. Trigger words such as "thief," "jail," and "police" should be avoided so as to better attain the cooperation of the individual. The approach should be as private as possible, should never be confrontational, and treated simply as a situation that needs resolving. Employees should be prepared for and know what to do if the person resists or runs.

The location of the detention also needs to be considered. If the person resists, is there a possibility of injury to bystanders? What exit routes exist for the person? What exit routes exist for the employee should the person become violent? Are there shopping carts strewn about the entry or other barriers that could make the approach difficult?

By evaluating the totality of circumstances, an employee is better able to decide how to handle the situation.

Making the Detention

Once the decision is made to approach the shoplifter, care must be taken in the way the

approach is made. It is recommended that a minimum of two people should make an approach. The employee should maintain a distance of approximately 6 feet from the shoplifter, and should never stand directly in front. This distance can be closed once the shoplifter's cooperation is attained. The employee should identify himself and invite the individual to a private location to discuss the matter. The employee should be prepared to deal with a reaction such as shock, denial, anger, and bargaining.

To obtain compliance, the employee should have a polite but firm business-like tone and not be diverted from the situation at hand. The employee should not take personally anything the shoplifter might say and avoid arguing or reacting negatively. The employee should expect the shoplifter to attempt to take control of the situation and should simply restate the purpose of the detention. It is crucial to maintain continual observation of the shoplifter throughout the detention process. This cannot be underestimated. Without continual observation, shoplifters have the ability to discard stolen merchandise, become violent, or escape.

Encountering Resistance

Resistance to being detained can be either verbal or physical. A merchant should have a sound and clearly understood policy as to how employees should handle a suspected shoplifting situation. A situation involving resistance can easily get out of control. When it happens, the risk of injury greatly increases. If force is allowed by policy, it should be the minimum amount of force necessary to bring the person under control. In the case of verbal resistance, only verbal control techniques should be utilized. Physical control techniques should be a choice of last resort and should only be undertaken if the employee is trained in physical control techniques. Additionally, the employee should be trained in how to apply handcuffs if their use is allowed by policy. Physical control techniques must be avoided for safety and liability reasons. Lastly, physical control techniques should be abandoned if at any time the employee loses control of the individual.

Processing the Subject

Once the detention has been carried out, the suspect must be processed according to the merchant's policy. A merchant has two choices: recover the merchandise and release the subject with a warning or call for police assistance and make a complaint. It is essential that the employee take notes and later enter them into an incident report. Of importance are actions made and words spoken by the suspect. Of greater importance is a written statement in which the suspect makes an admission or confesses. Everything said and done by the employee and the suspect will be closely scrutinized if the suspect is prosecuted. The same applies if the suspect files a civil action alleging negligence, false arrest, false imprisonment, or mistreatment.

Conclusion

Detention of a shoplifter is far more difficult than it might seem. Many issues are involved: safety, recovery of property, use of force, police arrest, and prosecution. An employee dealing with a suspected shoplifting must follow procedures that are set out by a sound policy and obey the law.

Ken Bierschbach

EXPERT WITNESS: THE DEPOSITION

A deposition is a legal proceeding conducted for the purpose of preserving the testimony of a witness for use in court. In this case, we are talking about a witness who is an expert witness. The deposition is usually held in a reasonably comfortable and private setting, very often the conference room of an attorney's office. The persons present are the witness, a notary public to administer an oath, a court reporter (usually a notary), and lawyers for all parties. The parties themselves or their representatives have a right to attend but seldom choose to do so.

The deposition begins by administering an oath to the witness. The lawyers take turns in asking the witness questions. A lawyer may skip a turn or take more than one turn. The proceeding is relatively informal, although serious to the outcome of the lawsuit. The reporter

takes down everything said and the reporter's record will later be typed and bound in a document called a deposition or a transcript. The deposition is essentially a tool for opposing lawyers to discover what a witness' testimony will be at trial. For example, the plaintiff's lawyer in deposing an expert witness for the defense:

- Will want to discover what the expert knows concerning the facts involved in the matter being litigated. The search here is for evidence that the expert will present in support of the defendant.
- Will want to discover if the expert knows of any facts that may be damaging to the defense, e.g., that the defendant may have been careless or failed to do something.
- Will want to commit the expert to the statements made under oath so that at trial the expert's testimony cannot be changed (at least not without difficulty and damage to the defense).
- Will look for ways to discredit the expert's testimony or to use the expert's testimony to discredit the testimony of other defense witnesses. Minor contradictions among witnesses are inevitable, while major contradictions or the appearance of them can be damaging.
- Will attempt to learn the basic theory and strategy that the defense will rely on at trial. The plaintiff's attorney may decide that the defense will be formidable against the claim as stated and that the claim needs to be changed.

Although a deposition can embarrass or even damage the reputation of an expert witness, this is not a legitimate purpose of the proceeding. When it happens, it is often the result of inadequate preparation by both the expert witness and the attorney that engaged the witness.

The expert witness has three fundamental obligations. First, is to tell the truth, even if the truth will hurt. This is an obligation that sits above the outcome of the lawsuit. Second, is to be fair. This does not mean that the witness has to give equal favor to both sides, only that the witness not overstate or color the facts. Third, is to be accurate, and this is where the expert witness plays a critical part in helping the judge and jurors fulfill their responsibilities in seeing that justice is carried out.

John J. Fay

Source Baker, T. 1992. *Operator's Manual for a Witness Chair*. Kansas City: Baker and Sterchi.

INTELLECTUAL PROPERTY RIGHTS

Most countries recognize and grant varying degrees of protection to four basic intellectual property rights: patents, trademarks, copyrights, and trade secrets.

Patents are grants issued by a national government conferring the right to exclude others from making, using, or selling the invention within that country. Patents may be given for new products or processes. Violations of patent rights are known as infringement or piracy. An example of patent protection is the Process Patent Amendments contained in the Omnibus Trade and Competitiveness Act of 1988. The Act treats unlicensed importers, distributors, retailers, and even consumers of standard products as patent infringers, if an unpatented product was produced by a U.S. patented process. The amendments apply to foreign and domestic manufacture and also to end products that are protected by U.S. process patents.

Trademarks are words, names, symbols, devices, or combinations thereof used by manufacturers or merchants to differentiate their goods and distinguish them from products that are manufactured or sold by others. Counterfeiting and infringement constitute violations of trademark rights.

Copyrights are protections given by a national government to creators of original literary, dramatic, musical, and certain other intellectual works. The owner of a copyright has the exclusive right to reproduce the copyrighted work, prepare derivative works based upon it, distribute copies, and perform or display it publicly. Copyright violations are also known as infringement and piracy.

Trade secrets are information such as formulas, patterns, compilations, programs, devices, methods, techniques, or processes that derive economic value from not being generally known and that cannot be ascertained by

unauthorized persons through proper means because they are subject to reasonable efforts to maintain their secrecy. Trade secret violations are known as misappropriation and result from improper acquisition or disclosure. Distinguishing between trade secret safeguards and patent or copyright protection can be difficult. The key elements in a trade secret are the owner's maintenance of confidentiality, limited distribution, and the absence of a patent.

A non-competition or non-disclosure statement is a written agreement that grants protection to an employer from the unauthorized use of the employer's intellectual property by current or former employees. A non-competition statement will typically incorporate one or more of three basic conditions: (1) restrictions on competition by departing employees, (2) definitions of what constitutes property that the employer can legally protect from use by others, and (3) requirements that employees are obligated to cooperate with the employer in efforts to protect its intellectual property.

The Paris Convention is the primary treaty for the protection of trademarks, patents, service marks, trade names, utility models, and industrial designs. Established in 1883, the convention is the oldest of the international bodies concerned with the protection of intellectual properties. It is based on reciprocity: (1) the same protections in member states as that state grants to its own nationals, and (2) equal access for foreigners to local courts to pursue infringement remedies.

Three elements of protection must be in place for the owner to claim violation of intellectual rights: (1) the information is not readily accessible to others, (2) it was created by the owner through the expenditure of considerable resources, and (3) the owner sought to keep the information confidential.

John J. Fay

KEY CONCEPTS IN SECURITY LAW

Corpus Delicti

The term corpus delicti means "body of the crime." It is often used erroneously to describe the body of a victim. Actually, the term relates to the essence of an offense and thus implies that every offense must have a corpus delicti.

In proving an accused's guilt of a specific crime, the prosecution establishes three general facts:

- That an injury or loss particular to the crime involved has taken place.
- That the injury or loss was brought about by somebody's criminality, meaning that the injury or loss resulted from a criminal act as opposed to an accident or other cause.
- That the accused, possessing the requisite state of mind (i.e., intent), was the person who caused the injury or loss.

The first two facts constitute the corpus delicti. The third fact simply establishes the identity of the offender. For example, the corpus delicti in a larceny would be (1) the loss of property (2) by an unlawful taking. In an arson offense, it would be (1) a burned house (2) that was deliberately set on fire.

Criminal Intent

Criminal intent is a clearly formulated state of mind to do an act that the law specifically prohibits, without regard to the motive that prompts the act, and whether or not the offender knows that what he or she is doing is in violation of the law.

It is generally regarded as falling into two categories: general criminal intent and specific criminal intent. General criminal intent is an essential element in all crimes. It means that when the offender acted, or failed to act, contrary to the law, he or she did so voluntarily with determination or foresight of the consequences. For example, general criminal intent is shown in the offense of assault and battery when the offender voluntarily applies unlawful force to another with an awareness of its result. In larceny, general criminal intent (often called larcenous intent) is shown by intent to knowingly take and carry away the goods of another without any claim or pretense of right, with intent wholly to deprive the owner of them or to convert them to personal use.

Specific criminal intent requires a particular mental state in addition to that of general criminal intent. The laws relating to certain crimes may describe an additional, specific mental purpose. For example, the crime of murder has a general criminal intent in that the offender voluntarily applies unlawful force with an awareness of its

result. In addition, the crime of murder in a particular jurisdiction may require a showing that the offender acted with premeditation to commit murder.

The terms *overt act* and *malice* are often associated with criminal intent. An overt act is an outward or manifest act from which criminality may be inferred; for example, an act done to carry out a criminal intention. In the crime of conspiracy, the overt act is an essential element of proof.

Malice is a mental state accompanying a criminal act that is performed willfully, intentionally, and without legal justification. The term malice aforethought is the state of mind or attitude with which an act is carried out, i.e., the design, resolve, or determination with which a person acts to achieve a certain result. In the death of another, it means knowledge of circumstances that according to common experience would indicate a clear and strong likelihood that death will follow the contemplated act. Malice aforethought is usually coupled with an absence of justification for the act.

Motive and intent are separate concepts in criminal law. Motive is the desire or inducement that tempts or prompts a person to do a criminal act. Intent is a person's resolve or purpose to commit the act. Motive is the reason that leads the mind to desire a certain result. Intent is the determination to achieve the result.

Motive is an important investigative consideration, but is not an essential element of a crime. Intent must be established for a crime to exist. A good motive (as might be represented in a mercy killing) does not keep an act from being a crime, and an evil motive will not necessarily make an act a crime. Furthermore, an accused would not be acquitted simply because a motive could not be discovered.

The basic urge that led the offender's mind to want the result of the forbidden act is immaterial as to guilt. Proof of motive, however, may be relevant and admissible on behalf of either side at trial. Motive can be especially pertinent where the evidence in a case is largely circumstantial. In some statutes, proof of motive may be required.

Federal Offenses

There can be no federal crime unless Congress first makes an act a criminal offense by the passage of a statute, affixes punishment to it, and declares what court will have jurisdiction. This means that all federal crimes are statutory. Although many of the statutes are based on common law, every federal statute is an express enactment of Congress. Nearly all crimes are defined in Title 18 of the U.S. Code.

Generally speaking, federal crimes fall into three large areas: crimes affecting interstate commerce, crimes committed in places beyond the jurisdiction of any state, and crimes that interfere with the activities of the federal government.

Crimes affecting interstate commerce are described in a variety of acts, e.g., the Mann Act, the Dyer Act, the Lindbergh Act, the Fugitive Felon Act, etc. They cover a wide variety of offenses over which Congress has plenary control.

Crimes committed in places beyond the jurisdiction of any state might include, for example, murder on an American ship on the high seas or on a federal enclave such as a military reservation ceded to the United States by a state. It should be noted that when an offense, not covered by a federal statute, is committed on a federal enclave, the case can be tried in a federal court under the laws of the state where the enclave is located. The offense of murder, for example, is not defined in a federal statute. If murder occurs on a military reservation in Texas, the federal government can prosecute the case using the Texas statute covering murder. This procedure is authorized by the Assimilative Crimes Act.

Crimes that interfere with the activities of the federal government include fraudulent use of the mails, robbery of a federal bank, violations of income tax laws, espionage, and many similar offenses. Federal courts have no jurisdiction over crimes against the states, and vice versa. It can happen, however, that an offense will violate both a state law and a federal law, e.g., robbery of a federally insured state bank. In such a case, both the federal and state court will have jurisdiction.

Federal death penalty laws include these violations:

- Espionage by a member of the Armed Forces in which information relating to nuclear weaponry, military spacecraft or satellites, early warning systems, war

plans, communications intelligence or cryptographic information, or any other major weapons or defense strategy is communicated to a foreign government.
- Death resulting from aircraft hijacking.
- Murder while a member of the Armed Forces.
- Destruction of aircraft, motor vehicles, or related facilities resulting in death.
- Retaliatory murder of a member of the immediate family of a law enforcement official.
- Murder of a member of Congress, an important executive official, or a Supreme Court justice.
- Espionage.
- Destruction of government property resulting in death.
- First degree murder.
- Mailing of injurious articles with the intent to kill or resulting in death.
- Assassination or kidnapping resulting in the death of the President or Vice President.
- Willful wrecking of a train resulting in death.
- Murder or kidnapping related to robbery of a bank.
- Treason.

Parties to Crime

Persons culpably concerned in the commission of a crime, whether they directly commit the act constituting the offense, or facilitate, solicit, encourage, aid or attempt to aid, or abet its commission are called the parties to the crime. In some jurisdictions, the concept is extended to include persons who assist one who has committed a crime to avoid arrest, trial, conviction, or punishment.

The parties to a felony crime fall into four categories: (1) principals in the first degree, (2) principals in the second degree, (3) accessories before the fact, and (4) accessories after the fact.

Generally, a principal in the first degree is the actual offender who commits the act. If the offender uses an agent to commit the act, the offender is still a principal in the first degree. There may be more than one principal in the first degree for the same offense.

A principal in the second degree is one who, with knowledge of what is afoot, aids and abets the principal in the first degree at the very time the felony is being committed by rendering aid, assistance, or encouragement. A principal in the second degree is typically at the crime scene, nearby, or situated in such a way as to render assistance. Under the concept of "constructive presence," a principal in the second degree could be a considerable distance removed from the crime while it is being committed. An example might be a lookout that monitors police radio communications at a remote location and calls burglar accomplices at the crime scene to alert them of police patrol movements.

An accessory before the fact is a person who, before the time a crime is committed, knows of the particular offense contemplated, assents to or approves of it, and expresses a view of it in a form that operates to encourage the principal to perform the deed. There is a close resemblance between an accessory before the fact and a principal in the second degree. The difference relates to where the accessory was and the nature of the assistance rendered at the time the crime was committed. If a person advises, encourages, and gives aid prior to the act, but is not present at the act and not giving aid at the time of the act, the person would be regarded as an accessory before the fact.

An accessory after the fact is a person who, knowing that another has committed a felony, subsequently aids the felon to escape in any way or prevents arrest and prosecution. The person may help the felon elude justice by concealing, sheltering, or comforting the felon while a fugitive, or by supplying the means of escape or by destroying evidence. An accessory after the fact must have an intention to assist the felon and must actually do so. Mere knowledge of the felon's offense and a failure to report it does not make a person an accessory after the fact.

Preliminary Offenses

There are three crimes that are preparatory in nature and serve as part of a larger purpose. Each of them is a means of reaching a criminal end. These so-called preliminary crimes are: solicitation, attempt, and conspiracy.

Solicitation consists of the offender's oral or written efforts to activate another person

to commit a criminal offense. The essence of the crime is to incite by counsel, enticement, or inducement. The offense of solicitation is complete if the offender merely urges another to violate the law and otherwise does nothing himself.

Attempt has two elements. First, there must be a specific intent to commit a particular offense, and second, there must be a direct ineffectual overt act toward its commission. There must be some act moving directly toward the act. Mere preparation, such as obtaining tools or weapons, may be insufficient to establish the crime, especially when made at a distance in time or place.

Conspiracy is the combination of two or more persons working in some concerted action to accomplish some criminal or unlawful purpose, or to accomplish some purpose in a criminal or unlawful manner. If there is a common understanding among the participants to achieve a certain purpose or to act in a certain way, a conspiracy exists without regard to whether there is any formal or written statement of purpose, or even though there is no actual speaking of words. There may be merely a tacit understanding without any express agreement.

John J. Fay

LAWS AFFECTING SECURITY

Our system of justice places a high value on the rights of citizens. The loss prevention practitioner's work activities in requesting arrests, collecting evidence, interviewing and interrogating witnesses and suspects, preparing reports, seeking prosecution, and recovering company assets places the practitioner within the scrutiny of our justice system. Should the practitioner violate a citizen's rights, he or she may be held personally accountable, and where the violative act was performed as a job duty, the practitioner's employer may also be accountable. When the violative act is a crime, the issue can be decided in a criminal court and the punishment may be imprisonment and/or a fine; and when the violative act is a civil wrong, the issue may be decided in a civil court and redress made through monetary awards.

Criminal law deals with crimes against society. The states and the federal government maintain a criminal code that classifies and defines offenses. Felonies are considered more serious crimes, such as burglary and robbery. Misdemeanors are less serious crimes, such as trespassing and disorderly conduct.

Civil law adjusts conflicts and differences between individuals. Examples of civil law cases in the security field are false arrest, unlawful detention, negligent training of security officers, and inadequate security that results in death or injury. When a plaintiff (i.e., a person who initiates a lawsuit) wins a case against another party, monetary compensation commonly results.

Law Origins

Three major sources of law are common law, case law, and legislative law. English common law is the major source of law in the United States. Common law is an ambiguous term. Generally, it refers to law founded on principles of justice determined by reasoning according to custom and universal consent. The development of civilization is reflected in common law. Specific acts were, and still are, deemed criminal. These acts, even today, are referred to as common law crimes: treason, murder, robbery, battery, larceny, arson, kidnapping, and rape, among others.

Common law is reinforced by decisions of courts of law. After this nation gained independence from England, the common law influence remained. Nineteen states have perpetuated common law through case law (i.e., judicial precedent). Eighteen states have abolished common law and written it into statutes. The remaining states have either adopted common law via ratification or are unclear about exactly how it is reflected in the state system.

Case law, sometimes referred to as "judge-made law," involves the interpretation of statutes or constitutional concepts by federal and state appellate courts. Previous case decisions or "precedent cases" have a strong influence on court decisions because they are used as a reference for decision making. Since the justice system is adversarial, opposing attorneys refer to past cases (i.e., precedents) that support their individual contentions. The court makes a decision between the opposing parties. Societal changes are often reflected in decisions. Since the meaning of legal issues evolves from case law, these court decisions are the law. Of course, later court review of previous decisions can alter legal precedent.

The U.S. Constitution provides the authority for Congress to pass laws. Likewise, individual state constitutions empower state legislatures to pass laws. Legislative laws permit both the establishment of criminal laws and a justice system to preside over criminal and civil matters. A court may later decide that a legislative law is unconstitutional; this illustrates the system of "checks and balances," which enables one governmental body to check on another.

Philip P. Purpura

Source Purpura, P. 2002. *Security and Loss Prevention, 4th Edition*. Boston: Butterworth-Heinemann.

LIABILITY FOR NEGLIGENT TRAINING

Contract security officers, their employers, and the clients they serve continue to be named in lawsuits alleging a wide variety of civil violations. Two factors appear to be at work. First is the increasingly litigious nature of society, and second is an expanding social conscience that favors the little guy. The pattern that emerges from civil actions reveals a pronounced targeting of persons in authority positions, such as security officers and the people who hire and manage them.

Because misconduct litigation is a prominent and highly profitable specialty in the practice of law, there are many who seek careers in it. Seminars on the subject are offered around the country, and how-to manuals are available to guide the novices. Expert witnesses, many of them current and former security professionals, are paid to testify for plaintiffs.

The usual path of pursuit in civil litigation is the negligence theory. In this approach the argument is not that the injurious conduct was malicious in nature, but that the injury and damages resulted from a failure to perform a duty with due care. Liability is the result of negligence or failure to give proper attention or care to one's duty. For the liability to be recognized, it must be the cause of a deprivation of rights secured by the Constitution.

Within the negligence theory, there is a particular vulnerability to accusations of improper training. The courts have consistently ruled in favor of plaintiffs who can show injury caused by negligence resulting from the absence of training or the administration of faulty training. The citizenry and the law impose an affirmative duty upon employers to provide their employees with requisite knowledge and skills. When jobs contain the potential for abuse and injury, as is the case with many jobs in security, the affirmative duty to provide training is expected to be met without qualification.

More often than not, the injured party will file suit against the offending officer, as well as the officer's superiors. The plaintiff's charge will frequently allege that the officer acted intentionally to cause injury and that the superiors should also be held accountable for being negligent in failing to take preventive action.

When a suit is pursued along these lines, the officer and superiors are very apt to come into sharp and bitter disagreement. The officer will argue that his or her actions conformed with policy, procedures, and the training provided by superiors. The superiors will argue that their subordinate's actions were inconsistent with the standards established for the officer. The conflict is certain to weaken their separate defenses and cast a shadow of doubt in the minds of jurors.

The damages that may be assessed in a negligence case are of three types: direct, punitive, and nominal. Direct damages may include such things as medical expenses, lost wages, and the costs of replacing or repairing property. Punitive damages are usually assessed when an element of fraud, malice, or oppression is present. The third type is called nominal damages. If assessed, the amount is usually set at $1, hence the term nominal.

In the concept of proximate cause, a single wrongful act may be caused by two or more persons acting at different points in time. For example, a security officer might make an unlawful arrest. The officer says his action was based on knowledge imparted to him through training given by the officer's employer. The concept of proximate cause supports the plaintiff's charge against the officer and any other persons who contributed to the unlawful arrest. In this example, the contributing persons could be the instructor, the officer's supervisor, and so on right up to senior management.

Lawsuits that allege insufficient instruction serve as reminders that the days of training on a catch-as-catch-can basis are over. Today the techniques of quality control have as much

meaning in the classroom as in any work environment where excellence is the minimum standard. Further, the general public holds high expectations concerning training. The media have helped shape public perceptions, and when training expectations fall short, the community is angered and the injured parties seek justice through the courts.

Any response strategy to counter the potential for civil litigation should be aimed at eliminating in the training domain any conditions that might contribute to charges of improper instruction. Even the finest training operation must anticipate that negligent training lawsuits will be charged. The best answer to charges will be a positive defense based on accurate and detailed documentation.

Five tactics should be included within the strategy:

- Validate training.
- Administer training to specifications.
- Evaluate the trainees.
- Keep training records.
- Impose instructor standards.

Validate Training

Validation means to ensure through an objective process that the training provided corresponds to duties associated with the job. The key objectives of validation are to verify that: (1) doctrinal content and skills development are correct, (2) instructional methods are appropriate and effective, and (3) training is relevant to the workplace and answers the day-to-day needs of job incumbents.

One of the more objective and commonly used techniques of validation is task analysis. Information drawn from task analysis gives to the curriculum designer a wealth of facts obtained from incumbents and others close to the job. The data reveal with high accuracy and specificity the nature and conditions of the trainees' future work environment.

A curriculum constructed from task analysis data will establish the baseline tasks of the job and will highlight tasks that, if not performed or performed incorrectly, could lead to litigation. Further, the task analysis approach uncovers the knowledge and skills that support each task. For example, if a task requires a security officer to use his revolver in defense of human life, the officer must be taught how to handle and fire the revolver (skills), and he must know the deadly force law and be able to differentiate between threatening and non-threatening situations (knowledge). The curriculum will require each officer-trainee to perform the skill part of the task, demonstrating a competency to predetermined standards. The knowledge part of the task might be tested by written examination, again in accordance with high standards.

By far, the most important specifications are the tasks. They serve as the focal points and basic framework of instruction. Other course specifications, such as practical exercises and tests, are derived from and influenced by tasks. When a curriculum has been validated (i.e., determined objectively to be job relevant) and when instructional activities have been executed according to plan, the opportunities for negligence are largely, if not entirely, removed and a strong defense is constructed against accusations of improper training.

Administer Training to Specifications

A minimum of logic must prevail for a training course to be made resistant to charges of negligence. Logic tells us that the success of a training operation cannot exceed the combined capacity of its component parts. The instructors, the logistics, and the students might all be top notch, but the training will be less than successful if the program is poorly conceived or carried out haphazardly.

The curriculum can be the training supervisor's most valuable tool for planning, organizing, and controlling. If the tool is ignored or used without skill, the training will suffer. Sadly, some training supervisors regard a curriculum as something to be merely tolerated, deserving not much more than lip service, and certainly not something to be followed. After all, they might argue, the curriculum was put together by people who have no real appreciation of the problems that confront trainers.

Serious implications are present in a situation where control is lacking over what is being taught and learned. When a training supervisor ignores a curriculum, so will the instructors. It does not take much imagination to speculate on the variety of civil liability risks that are

created when instructors and their supervisors are allowed to teach according to their own dictates. The appropriate remedy is to make clear that curriculum specifications are not negotiable and that if the curriculum requires a change, for whatever reason, it will be done through an established process.

Training that is in progress can be monitored in several ways to ensure that the curriculum is being followed. Trainees can be asked if they personally participated in certain programmed activities; classrooms and training areas can be visited to verify that trainees are engaged in activities that support the training objectives; and tests, scores, critique sheets, and other written materials that reflect the details of training can be examined.

It is far better to discover imperfections during training than to wait until the imperfections produce undesirable consequences on the job. Mistakes noted as they happen are easier to correct and are free of the potential for complaints and redress in the courts.

Evaluate the Trainees

Students are evaluated in two dimensions, general and specific. Generally, they are appraised in terms of personal appearance, demeanor, attitude, motivation, and similar characteristics. In the specific dimension, students are evaluated in objective terms, that is, by the administration of tests. Two types of tests are appropriate in security officer training programs: written examinations to measure knowledge attained, and performance examinations to measure skill development.

Since every task (or training objective) is either knowledge-oriented or skill-oriented, determining the appropriate type of test is not a problem. If the task is to "name the limitations on the use of deadly force," the test is by written examination, and if the task is to "operate a handy-talky radio," the test is by performance or doing.

A written examination may contain one or more classes of questions such as essay, write-in, matching, true/false, and multiple choice. The questions can range from subjective to objective, and operate from the principles of discrimination, recall, and recognition. Subjective questions have a lesser value in entry-level training programs because most knowledge-oriented tasks are either performed correctly or incorrectly, with no tolerance for "in-between" responses. Subjective questions are also difficult to grade and depend on the interpretations and judgments of the grader. By contrast, objective questions do not have these limitations and lend readily to task-centered training.

In testing important knowledge, more than one question needs to be asked, not just to convey importance to the student, but to obtain assurance that the student really possesses the knowledge and did not guess the answer.

The issue of whether or not a question is easy or hard is not a consideration. Certainly, a question should not give away its own answer. The purpose is to determine fairly if the student has attained the required knowledge. Testing is not a contest of wits between the test writer and the student.

Everything that is taught should be tested. Testing some tasks and not others is not an acceptable practice. Neither is testing extraneous and nice-to-know information or information not included in the curriculum. Testing all and only what has been taught is an effective, direct approach.

The testing concept is the same for the skill-oriented task, but with conditions and standards spelled out. For example, if the task being tested is to operate a handy-talky, the test might require the student to turn the radio on, adjust for squelch, and send a message using the 10 series code. Grading would focus on the time required to perform the task and the number of errors made in turning the radio on, adjusting it, and speaking the message using the correct code numbers.

Testing a skill-oriented task is especially demanding of an instructor's time, energy, and resourcefulness. The instructor has to find a testing location and furnish it with the required equipment, recruit assistants, organize the students and get them to the testing location, and conduct the tests.

Instances of instructors allowing some students to pass without being tested or without achieving the minimum competency levels are most likely to occur in the performance examinations. The preventive steps are to make sufficient time available for testing, precede testing with lots of practice, provide plenty of help to the primary instructor, and give slower

learners special attention prior to and during the testing.

Establishing a spread among learners or comparing learners against each other is not necessary. The idea is to find out if the student has reached an acceptable level of competence. This is what we would call a pass/fail situation. It is both pointless and misleading for a grade to be assigned to a task. Why even try to compute a task grade or even a composite grade when the only measurement that really counts is whether or not the student has satisfactorily performed the task?

Keep Training Records

Because documentation can serve as a strong defense to a charge of negligent training, keeping records of every aspect of a student's progress from start to finish makes very good sense. At the front end are documents which reflect the qualifications that a student brings to the course. Licenses, entrance examination scores, aptitude and psychological test scores, high school and college transcripts, and certificates of prior training are examples. These items are indicators of the student's entering abilities and predictors of course performance.

If a course applicant does not meet prerequisites but is nonetheless allowed to enter, a record should be made of who granted the waiver and why. This should serve as a red flag, not to stigmatize the student but to alert the staff to a need for special teaching attention. Whatever extra efforts are expended by the staff and the student to overcome the deficiency should be made a matter of record.

Documents associated with course administration run the gamut from the opening day schedule to the graduation agenda. Within this large collection of written materials are two broad classes: documents that relate to training activities generally, and documents that relate to students individually. One way to organize what can surely be a very large mass of paperwork is to place the general documents in a single, large file and the student documents in separate dossiers.

The general file is for documents from one single course offering, not all offerings of the same course. The general file can be broken down into subcategories such as correspondence and memoranda, course announcement and schedule, curriculum or program of instruction, lesson plans, student handouts, class roster, attendance sheets, etc. Related to the file, but maintained apart from it for security reasons, are the written examinations.

Lesson plans and handouts are excellent documents for refuting negligent training claims. They reflect what the instructors taught and what the students were expected to learn. For example, a lesson plan on self-defense tactics would require an instructor to emphasize the risk of injury to a person being restrained by a choke hold. The student handout would reinforce that important teaching point. The lesson plan and handout would directly rebut a claim of improper training of the choke hold. One note of advice: put preparation/revision dates on lesson plans and handouts.

The attendance sheets can also be important. If the officer in the example just given falsely represents that he was not in class on the day the lesson was taught and the handout distributed, thereby imputing negligence to the training agency, the attendance sheets provide an opportunity for refutation.

A student's dossier contains items that reflect entry into the course, participation in it, and departure from it. There might be evidence of registration, issuance of supplies, disciplining, counseling, academic problems, absences, makeup and remedial training/re-testing, special honors earned, and test results.

From the standpoint of potential civil liability, test results are extremely significant because they substantiate that important, job-related tasks were learned by the trainee. It also helps when the test results are recorded in a format that describes the tasks tested, the names of the evaluator and approving official, whether re-teaching and re-testing were needed, and the initials or signature of the trainee in acknowledgment of the record's entries.

Impose Instructor Standards

Without good instruction, it will not matter if students are bright and eager, facilities first-rate, and the administration efficient. All of these elements are important, but the controlling element will certainly be the competency of instructors.

Instructor qualifications are typically fixed by legislation in states where security officer

training is mandated. A certification process will accompany enforcement in almost every case. Instructor certification may specify minimums that relate to education and training accomplishments, field experience in the subject area to be taught, and successful completion of an approved instructor training course.

An instructor's competency can be judged in two areas: knowledge of subject, and ability to teach. If either area is deficient, it is reasonable to expect that the instructor's performance will be correspondingly deficient.

Each of us at one time or another has been the victim of the knowledgeable instructor who, despite good intentions and best effort, was just not able to get his message across. By contrast, the instructor who is weak in the subject area but strong as a teacher is apt to be less noticeable. Through superior communications, a small amount of information can be stretched a long way.

The exceptional instructor will be solidly proficient in both subject matter knowledge and teaching abilities. The average instructor will have a combination of strengths and weaknesses in each area, and the below-average instructor will be significantly weak in at least one area. If required to select a below-average instructor, a training director would not want the instructor's weakness to be in topic knowledge. This is a problem that cannot be corrected easily or quickly. An instructor who lacks a solid command of his or her subject needs to return to the field and gain more knowledge through job experience and self-development.

The instructor who knows the topic to be taught but cannot teach very well can be improved with much less difficulty and in a reasonable period of time. A certain amount of improvement will inevitably result from the teaching experience itself, and from the process of instructors interacting and learning from one another. Surely the most dramatic improvement can result from attendance at an instructor training course.

A training course for instructors is typically 1 or 2 weeks long and covers topics such as learning theory, instructional strategies and methods, learning aids, lesson plan writing, and development of practical exercises. The 1-week course has only enough time to explain basic teaching concepts; the 2-week course will additionally allow the trainee to make one or more graded presentations using lesson plan materials, learning aids, and handouts developed while in the course.

Where instructor training is required as a condition of certification, the certifying agency will most likely conduct or make available a range of approved courses. In addition to a course that prepares an instructor to teach generally, specialized instructor training courses in firearms may be provided.

The absence of legislated requirements should not be seen as a rationale for not upgrading instructors, and under no circumstances should it be seen as a legal defense to complaints of incompetent instruction. Even where minimum standards prevail, a very persuasive argument can be made that such standards are, after all, only minimums. There is no law against establishing instructor standards where none exist or in setting standards above what are minimally expected. Having no instructor standards or choosing to operate with minimums is an assurance of mediocrity.

Chief security officers need to reduce risks associated with inadequate and poorly operated training programs. A question to be asked is not whether an organization can afford quality training, but whether it can afford not to have it.

John J. Fay

NEGLIGENCE IN PREMISES DESIGN

Criminologists have studied the causation of criminal behavior for the last three hundred years, and have usually associated crime with urban centers. However, the flight from the cities to suburbia over the last three decades has created lucrative magnets of crime in the suburbs such as office parks, apartment complexes, industrial sites, and multi-unit residential properties. The courts are finding the owners liable for criminal acts that occur on their property.

The primary function of security professionals employed by premises owners and operators is to prevent criminal incidents that result from security negligence. This primary function obligates a security professional to:

- Identify the level of criminal activity in the site and the neighborhood. The evaluation should include a three-year history, with periodic annual reviews. The radius

of area for review will vary from site to site but typically will cover a half-mile radius.

- Conduct a security audit that identifies the assets to be protected, the threats, vulnerabilities, and recommendations for security improvement. The principal assets in premises liability are people and their property; the threats are criminal events; the vulnerabilities are security measures that are needed but not in place; the recommendations are those actions that must be taken to eliminate the vulnerabilities. The audit should be factual, well documented, and in writing. It is both a report of findings and a plan of action. The recommended actions should be prioritized according to magnitude of consequences and probability of occurrence.
- Develop a security delivery system that conforms to the findings of the audit. The system will be a combination of three components: (1) physical safeguards, such as locks, fences, and lighting, (2) people, such as security officers and on-site employees, and (3) procedures that guide the people component in using/operating the physical safeguards component. To function at maximum efficiency, the three components must operate in harmony.

In addition to developing and ensuring efficient operation of the security delivery system, the security professional should pose to the owner/operator pertinent questions:

a) Do you maintain good relations with the local police agency and are able to get copies of crime reports of events happening on your property?
b) Do you maintain active membership associations that have strong national standards?
c) Have you established procedures for notifying tenants or residents of crime problems and what to do when suspicious activities are spotted?
d) Do you record incidents and keep them on file for possible later use in defending against civil actions?
e) Have you clearly stated the essential security functions, job duties and tasks, emergency response plans, and security operating procedures?
f) Are you able to provide or ensure that sufficient training is given to security and non-security staff on the proper practices of security?
g) Do you review, update, and document policies and procedures at least annually?
h) Do you ensure that all employees are issued their own copies of procedures and sign off that they have read and understand them?
i) Can you ensure that all locks and locking devices are of sufficient quality and quantity to protect tenants from unauthorized entry?
j) Have locking devices on doors and windows been inspected at least annually, and reviewed as tenants move out and move in?
k) Has periodic testing been done of intercom, security alarm, fire safety, and CCTV systems?
l) Is there adequate lighting in exterior parking areas, walkways, and entries that meet industry standards of the Illumination Engineering Society of North America or local building codes?
m) Is repair and maintenance performed on physical safeguards such as fences, gates, and lighting?
n) Do residential units have door viewers?
o) Are vacant spaces and units kept secured?
p) Are keys inventoried, issued with controls, and kept under lock and key?
q) Is foliage around the grounds and building perimeter trimmed to eliminate hiding spaces and allow exterior lighting penetration?
r) Are roof, basement, and utility and mechanical room doors kept locked?
s) Are fire-escape doors equipped with release hardware?
t) Are visitors, guests, and other non-residents screened at points of entry?
u) Is protection afforded to utilities such as direct electrical power, emergency power, gas lines, HVAC, and water supply?
v) Do advertising and marketing materials accurately represent the security delivery system?

w) Are rental agents, managers, and staff truthful when describing the security delivery system?
x) Are disclaimers included in lease agreements and contracts, and security warnings posted in common areas such as pools, parking areas, and mail areas?
y) Are tenants and residents kept informed of changes in security and criminal events that require warning?
z) Are employees thoroughly screened prior to employment?

These questions will be the first questions asked when negligent security is alleged. Every question that cannot be answered in the owner's favor is a question that will be damaging at trial. As the number of unfavorably answered questions rises, the amount of compensatory and punitive damages can proportionally rise.

Examples of actual security negligence cases:

- A man is robbed in an apartment lobby left unguarded in the afternoon.
- A woman is attacked in a parking lot of a design showroom.
- A faulty door allows a rapist to enter an apartment building and rape a tenant.
- A faulty stairway design allows for a serious injury to an elderly visitor at a condominium.
- A hotel room balcony facing an open atrium is wide enough to allow a child to slip through and fall ten stories.
- An inmate hangs himself from an air return grille over the toilet that is not properly secured.
- A secretary walks into a sliding glass door that had no window markings on it.
- An entry rug in a bank buckles when the doorjamb hits the edge of the carpet and trips an elderly tenant.
- A child is shot inside an apartment walkway by a stray bullet fired during a drug deal.

These are just a few examples of cases litigated under premises' liability case law.

According to a study published in 1984 by Professor Lawrence Sherman, a professor of criminology at the University of Maryland at College Park, the number of major awards reported nationwide each year in security liability cases increased 3000 percent between 1965 and 1982. The average dollar amount awarded in those cases increased by 5000 percent. Moreover, the study suggests that almost half the major awards are from four states: New York, New Jersey, Florida, and the District of Columbia. Security negligence lawsuits are one of the fastest growing civil torts in the United States currently.

To protect against lawsuits, it is wise to hire a security/safety expert to look for vulnerabilities using a risk analysis approach. An expert will look for deviations from fire codes and similar standards, develop crime demographics, and point out the potential for crime and accidents. The expert can also provide counsel on reasonable steps that should be taken to remove the potential, and when those preventative actions are set in place the issue of foreseeability in litigation is removed.

A type of risk analysis approach is the security audit. It is a systematic search for and examination of factors that can lead to adverse events such as rape, robbery, burglary, theft, and accident-related injury. The audit gives direction to the owner for reducing the probability of adverse events through the implementation of sensible, cost-effective countermeasures. When the countermeasures are in place, the owner has met the reasonable standard of care, an extremely important issue in defending against a charge of negligence.

Foreseeability is a key issue in security and safety liability cases. For example, foreseeability is present when a premises has a history of crime, particularly like crimes such as robbery and assault. The owner of the premises knows, or should know, that a problem exists and that reasonable steps must be taken to prevent future robbery and assault. Liability increases dramatically when preventative actions are not taken.

Court decisions have consistently held that the owner/operator of premises, such as an apartment building, has certain duties that cannot be ignored. Among these are (1) a duty to provide reasonable care for tenants and guests and (2) meet contract requirements such as those stipulated in a rental agreement.

Many courts make decisions using a doctrine called "totality of circumstances." All circumstances, not just one major circumstance, are considered. A case that does not have a major

circumstance but has several minor circumstances can be decided in favor of the plaintiff when the "totality of circumstances" doctrine is applied. The more common circumstances in premises liability include:

- Prior crime on the premises.
- Prior crime in the immediately surrounding neighborhood.
- Preventive measures not taken when preventive measures have been taken at like premises nearby.
- Absence of physical security safeguards such as fences, locks, and lights.
- Absence or inadequate maintenance such as broken fence gates and burned out bulbs in hallways and stairwells.
- No security officers or not enough security officers.
- Untrained and poorly supervised security officers.
- No response or poor response to incidents in progress.
- No warnings to tenants of accident hazards or of recently committed crimes.
- Non-compliance with codes, statutes, etc.
- Reduction of security and safety measures such as cutting back on the number of security officers, canceling the roving patrol function, or eliminating the position of lifeguard.

The security professional can be of great help in identifying problematic conditions, hopefully in time to prevent litigation. When preventative steps have not been taken and litigation occurs as a result, the owner/operator can expect to see a security professional working for the plaintiff. Every action not taken by the defendant will be thoroughly exploited.

It needs to be understood that the term "security professional" is a general descriptor. Not all security professionals possess expertise in risk analysis, vulnerability assessment, security design, and expert witness credentials. And the individuals that qualify in these categories are not of equal caliber. The owner/operator has to recognize the distinctions.

Many sites have architectural features that facilitate criminal opportunities. These can include blind spots in a parking lot, malfunctioning access control devices, and CCTV cameras mounted in wrong places. Such features are often the result of not using the services of a security professional when the site was constructed or retrofitted. Left to their own devices, design professionals will in almost every case choose esthetics over security.

Design features that facilitate security in vulnerable areas include clear sight lines, overlapping illumination, sturdy fences, barrier-landscapes, buildings arranged in a pattern that makes criminal intrusion visible, and vehicle/pedestrian pathways that channel traffic away from critical assets.

"Adequacy" of security is subjective, judgmental. Adequacy defined by the plaintiff will be wildly different than adequacy defined by the defendant. An accurate assessment of adequacy is best made by a non-vested consultant having impeccable security credentials. The cost of the service is minuscule in comparison with monetary damages.

A mistake often made by an owner/operator is to hire a consultant that works for a company that sells a security product or service. A prime issue for the consultant will be to help sell the product or service. An owner/operator's biggest mistake would be to accept a "free" consultation.

In summary, security professionals can help the owner/operator avoid civil liability. Nearly all occurrences of negligent security are rooted in dollars. It is sad irony when a failure to pay a few extra dollars upfront to ensure a reasonable level of security leads at a later time to an enormous dollar loss. The security audit, or vulnerability assessment, can be an extremely valuable tool in the hands of the knowledgeable practitioner. The audit identifies security weaknesses and provides a blueprint for remedial action.

Randall I. Atlas

NEGLIGENT HIRING AND DUE DILIGENCE

The threat of negligent hiring litigation is at an all time high. Employers large and small are troubled by lawsuits that allege negligence, workplace violence, and employee theft. A comprehensive background check can arm an employer with a clear picture of a candidate's past work history, education, general character,

criminal history, and propensity to harm others.

The fear of negligent hiring and retention are primary concerns of human resources managers and risk managers. Since 1970 negligent hiring torts have resulted in settlements and awards at the multi-million dollars level. A payout of this magnitude can cripple an organization financially or push it into bankruptcy.

Before fully understanding the risks of not conducting background checks, employers need to understand two very important principles: due diligence and negligent hiring. In the context of pre-employment screening, due diligence refers to the duty of care an employer must take to ensure that persons selected for employment do not pose a threat to others. The employer's duty to exercise due diligence in a hiring situation can be met by conducting a thorough background investigation.

Negligent hiring is the employment of a person that poses danger to others. Negligence is shown when the employer failed or did not try to know of an applicant's undesirable background at time of hire, and at a later time the hired person caused harm to another.

Together, due diligence and negligent hiring can be thought of as a "risk barometer." Due diligence is at the lower end of the barometer. It signifies low risk because applicants are screened before hiring, therefore lowering the risk of harm. Negligent hiring is at the top end of the barometer. It signifies high risk because reasonable steps, such as a background investigation, were not taken to filter out high-risk applicants.

Respondeat superior, or let the master answer, is a premise for negligent hiring claims. An employer (the master) can be held liable under certain circumstances for the wrongful act of an employee (the servant). Many allegations of negligent hiring are based on the *respondeat superior* concept. For example:

- A Florida jury awarded damages of $2,500,000 in Tallahassee Furniture Co., Inc. v. Harrison. An employee of the company savagely attacked a woman customer in her home. According to the facts of the case, the employee had a history of criminal violence, which would have easily been discovered during a background check.
- In Artis vs. Wayside Baptist Church, a Dade County, Florida, jury awarded the plaintiff $6,700,000 which included $2,500,000 in punitive damages. The church's youth minister had molested a boy over a 2.5-year period. Verification of the minister's past employment would have revealed the risk.

An employer should look for application and résumé fraud when conducting background screening. Applicants have several tricks up their sleeves when it comes to crafting a competitive résumé. From lying about past work history and education credentials, to falsifying professional licenses, applicants have thought of just about every way imaginable to place themselves above other job candidates.

Several industry studies indicate that a great many applicants lie on their résumés. A majority of embellishments are in education and employment such as claiming to have a college degree or claiming to have worked in a particular position or at a senior management level. False claims range from stretching the truth to flat out lies.

Information available online at *www.resumefraud.com* indicates that applicants continue to utilize online diploma mills to obtain fictitious credentials. The U.S. Department of Education defines a diploma mill as "an organization that awards degrees without requiring students to meet educational standards for such degrees."

In a recent study, Comprehensive Information Services, Inc. (CIS) purchased from a diploma mill a Bachelor of Business Administration degree in Human Resource Development and Management with a 3.5 grade point average. It cost $519.00 and arrived in a package sent from an overseas company. The package contained an authentic-looking diploma, transcripts, a certificate of participation in the school's student council, and an award of excellence. To make things even more realistic, the package included an alumnus bumper sticker and window decal.

Another tactic used by dishonest job seekers is "date stretching." This ploy is used when a candidate fears that a past employer will not give a favorable opinion. The candidate will stretch the end date of the immediately preceding employment to the start date of the

immediately following period of employment, thus concealing the middle period.

Background checks come in many shapes and sizes. A background check to determine a person's suitability for hire is a special type if only because it is subject to the Fair Credit Reporting Act (FCRA). The FCRA effectively controls the methods by which background screening firms operate. The FCRA, regulated by the Federal Trade Commission (FTC), sets out specific requirements and procedures with regard to notification, authorization, consumer privacy, and the use of a consumer report (background investigation) in making a hiring decision. A consumer report (CRA) generally includes information as to a consumer's credit worthiness, character, general reputation, personal characteristics, and mode of living. This type of screening includes information gathered from credit reports, criminal histories, verification of education credentials, and past employment information. An "investigative consumer report" is one that digs deeper into the applicant's past such as by interviewing persons familiar with the applicant. Both types of screening are conducted by a consumer reporting agency, i.e., a third party hired by the employer to conduct the investigation.

Several federal regulations and state statutes mandate background screening in a variety of industries such as healthcare, finance, and transportation. The Department of Transportation, for example, requires screening of pilots and other persons holding safety-critical positions.

Apart from federal and state mandates, employers have their own options. They can choose to screen all applicants, some applicants, or no applicants, and they can choose to go with bare-bones screening, intermediate level screening, or thorough screening. But before making any choices, the employer should weigh the risk potential. In the simplest sense, the employer can ask, "What risk do I face if I don't screen this type of applicant?" For a person applying for a job in the accounts receivable department, the risk may be embezzlement; for a person applying for a job as a cashier, the risk may be theft from the register; for a person applying for a job that involves stress and close proximity to others, the risk may be violence; and for a person applying for a job as a heavy equipment operator, the risk may be serious accidents. Each risk has its own parameters and not all risks should be measured in dollars alone. The employer has to consider loss of talent, loss of morale, and loss of reputation.

Employers should first develop a pre-employment screening policy that ensures compliance with the FCRA and other applicable laws such as the Americans with Disabilities Act (ADA) and regulations established by the Equal Employment Opportunity Commission (EEOC). The policy can call for a narrow, limited program, such as screening applicants for a single class of work, or a comprehensive program for screening all or most all applicants. Some jobs will stand out as critical. For example, a job that places an employee in close contact with children is a critical job. Background screening program for a job of this type would include ruling out that an applicant is using a false name, making comprehensive searches and examinations of criminal records, and matching the applicant's name against sex offender registries. The human resources department should also administer a battery of psychological tests.

The natural urge to control costs can lead an employer to ineffective screening practices such as making Internet searches or purchasing database searches. Due diligence requires much more. It means accessing the best information sources available, using professionals to extract the relevant information, and making the information available to the person(s) making the hiring decision.

An important information source is the criminal records office at a county courthouse. When it comes to the search of criminal records, employers have many options. For proper due diligence, a search should be conducted at the county of residence for at least the past seven years. Searching criminal records at the county level provides accurate and up-to-date information but care should be taken because many counties have different courts of jurisdiction that handle different types of cases.

A closer look should be taken when considering searching records at the state level. Only a handful of states provide comprehensive databases. Many counties and reporting jurisdictions do not submit their criminal files in a timely manner or may not even send in reports at all. Employers should always consider other database resources such as a national criminal database as a tool to enhance a records search. In addition, some private

and public background screening firms gather electronic information from county, state, and federal repositories and place the information in databases. A single database can have millions of records and be amenable to specialized searches such as for sexual predators.

A disadvantage with databases is that they often have "holes" and contain information that is out-of-date, inaccurate, or only partially accurate. A professional screening firm can verify database information. This practice can provide accurate and current information.

The National Association of Professional Background Screeners (NAPBS) was founded to provide standards, education, and best practices for its members. A recent NAPBS study revealed that there are currently 500-plus screening firms operating in the United States. They come in all shapes, sizes, and capabilities. An employer looking to contract with a screening company would be well advised to closely examine credentials. The two main attributes are quality of work and compliance with the law, most especially the FCRA.

Many states have implemented laws on the collection and use of criminal records as a guide in selecting job applicants. Obtaining arrest and conviction information may also be restricted by use, depending on the income level or earning potential of a candidate. State laws have also been put into place to provide fair treatment of lower income individuals and minorities. Before engaging in any kind of pre-employment screening, an employer must determine and understand the applicable laws of the jurisdiction.

Many screening firms accept online requests for service and provide quick turn-around. For the online work to proceed, the employer must provide certain data such as the applicant's name, date of birth, social security number, and other identifiers. A reputable, well established screening firm will protect the identifying data, usually as well as or better than the employer. Assurance is demonstrated when the screening firm uses standard protections such as passwords, firewalls, and encryption. A less reputable, fly-by-night screening firm may not have any procedures in place to shield the employer's data from prying eyes. While a screening firm's services and prices can be satisfactory, there is a risk that sensitive information is open to exposure.

Human error can account for information that is lost, stolen, damaged, and misfiled. The FBI, which prides itself on quality, has its share of human-error problems. The National Crime Information Center (NCIC) is operated by the FBI in cooperation with state law enforcement agencies. The NCIC maintains a national database of criminal information that is accessible to law enforcement. A study conducted in one state (Florida) revealed errors in 11.7 percent of 93,274 background checks. Even worse, 5.5 percent of more than 10,000 criminal records were in error because the individuals involved had never been convicted of a crime.

Employers need to understand that there are different roadblocks throughout the screening process. Many courts still utilize non-automated and antiquated ways of maintaining criminal records. Restrictions such as "clerk courts" or courts that do not provide public access to records may slow the process and make employers reconsider due diligence. Applicants are not always cooperative. They give partial or inaccurate information that makes it difficult to verify simple facts such as past employment and previous addresses.

A concern to a company is the possibility of a lawsuit alleging invasion of privacy because a former employee's performance information was released to another company that had the former employee under consideration for hire. The practical result is that a former employer will release nothing more than the former employee's dates of employment and job description.

In conclusion, employers are responsible for providing a safe and secure working environment for their employees and others on their premises. This is called duty of care and the duty can be met by due diligence practices such as screening out job applicants that have a history or propensity for violence or dishonesty. The methods of screening are limited to those approved by law such as the FCRA. To obtain the best available information in accordance with the law requires the use of professionals skilled in conducting background investigations.

Robert Capwell

RULES OF EVIDENCE

The rules for presenting evidence in a criminal investigation are as varied as the types of evidence. Let us look at them.

Opinion testimony is a conclusion drawn by a witness, hence the term opinion testimony. Another form of testimonial information is hearsay evidence. Hearsay is a statement that is made other than by a witness. Hearsay cannot be entered into evidence unless the maker of the statement can be cross-examined.

Privileged communication is confidential information between two persons recognized by law as coming within the so-called privileged relationship rule. The following relationships are generally recognized: a husband and wife, an attorney and client, a physician and patient, and a law enforcement officer and informant.

Character evidence is evidence introduced by either defense or prosecution witnesses to prove the accused's good or bad character. Character evidence is usually introduced only when the defense raises the issue of the accused's character.

Direct evidence is evidence presented by a person who actually witnessed something. Contrast this with circumstantial evidence, which is evidence that proves other facts from which a court may reasonably infer the truth.

Admissibility is a characteristic or condition of evidence. To be admissible, evidence must be material, relevant, and competent. Evidence is material when it plays a significant part in proving a case. Examples of material evidence might be fingerprints of the accused that were found on the murder weapon, an eyewitness account of how the accused committed the crime, or stolen property found in the possession of the accused. Evidence is relevant when it goes directly to the proof or disproof of the crime or of any facts at issue. Examples of relevant evidence might be a death certificate or a medical examiner's report. Evidence is competent when it is shown to be reliable. Examples of competent evidence might be accurate business records or the testimony of an expert fingerprint examiner.

Burden of proof is a rule which holds that no person accused of a crime is required to prove his or her innocence. The prosecution must prove the guilt of a defendant beyond a reasonable doubt. Reasonable doubt means the jury must believe the charges to be true to a "moral certainty." On the other hand, the accused must prove his or her contentions. Such defenses as self-defense, insanity, and alibi are affirmative defenses that must be proved by the accused.

A presumption is a conclusion that the law says must be reached from certain facts. Presumptions are recognized because experience has shown that some facts should be accepted or presumed true until otherwise rebutted. For example, defendants are presumed to be sane at the time the crime was committed, and at the time of trial, in the absence of proof to the contrary. Presumptions are of two classes: conclusive and rebuttable. A conclusive presumption is one that the law demands be made from a set of facts, e.g., a child under 7 years of age cannot be charged with a crime. A rebuttable presumption can be overcome by evidence to the contrary, e.g., presumption of death after being unaccounted for and missing for 7 years.

Rules of Exclusion

In general, rules of exclusion deal with conditions in which evidence will not be received. They limit the evidence a witness may present to those things of which he had direct knowledge, i.e., what he saw, smelled, tasted, felt, or heard.

All evidence, direct and circumstantial, if relevant, material, and competent is admissible provided it is not opinion testimony, hearsay evidence, or privileged communication. There are exceptions regarding the admissibility of opinion testimony and hearsay evidence. An exception to the rule against opinion testimony can be made when no other description could be more accurate. For instance, a witness is allowed to testify on such matters as size, distance, time, weight, speed, direction, drunkenness, and similar matters, all of which require the witness to state an opinion. There is no requirement for the witness to be an "expert" when testifying to facts such as these.

Exceptions to the rule against hearsay can be made for the dying declaration and the spontaneous declaration. The admissibility of a dying declaration is limited to homicide cases. Because of the seriousness of homicide, a dying declaration is an exception. A dying declaration is admissible either for or against the accused. The statement must have been made when the victim believed he was about to die and was without hope of recovery. The admissibility of the declaration will not be affected as long as the victim dies; otherwise, the issue would not arise since there would be no charge of homicide.

The spontaneous declaration, a statement made under conditions of shock or excitement, may be admitted as another exception to the hearsay rule. Normally, such a statement is made simultaneously with an event or act and there is not time or opportunity to fabricate a story. It is generally accepted that the statement will be admitted if it precedes, follows, or is concurrent with the act. The statement cannot have been made in response to a question and must pertain to the act that produced it. The spontaneity of the statement is sufficient guarantee of truthfulness to compensate for the denial of cross-examination.

In prosecutions for sexual offenses, evidence that the victim made a complaint within a short time after the offense occurred (i.e., a fresh complaint) is admissible in certain cases. The fact that the complaint was made is relevant for corroborating the testimony of the victim. The statement may relate only to who and what caused the conditions, and merely indicate the credibility of the victim as a witness.

An official statement in writing made as a record of fact or event by an individual acting in an official capacity (called a "business record") is admissible to prove the truth of a matter. Records are of two types: private and public. To introduce private records, someone associated with the business must introduce them. He must show that the company kept records, that the record produced was one of these records, and that the record was the original or certified copy of the original. Public records are usually introduced by presenting certified copies.

A confession is a statement or complete acknowledgment of guilt. An admission is a statement which does not amount to a complete acknowledgment of guilt, but links the maker with a crime. Admissions are forms of hearsay. A court is inclined to apply the same rules of admissibility to admissions as for confessions.

John J. Fay

Source Fay, J. 1987. *Butterworths Security Dictionary: Terms and Concepts*. Boston: Butterworth-Heinemann.

SEARCH AND SEIZURE

The Fourth Amendment to the Constitution of the United States guarantees the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures. The words used in the Constitution are directed at unreasonable searches and seizures conducted by the government. Unfortunately, however, the Constitution does not go on to define what is meant by the term "unreasonable," nor does the law discuss any provision for punishment of persons who violate the Fourth Amendment. It has been left up to the U.S. government and the various states to create definitions of search and seizure violations, and to provide suitable punishment when violations are proven. At the federal level, Title 18 of the United States Code provides fines and imprisonment for persons found guilty regarding searches. Most states have tended to model their search and seizure laws in conformance with the federal law. Where differences might exist between a particular state and the overall guiding federal law, the difference is more likely to be a matter of semantics rather than spirit or intent of the law.

In addition to possible criminal prosecution for violations of law regarding illegal search and seizure, the offending person is likely to be charged in a civil suit for damages resulting from the violation. A defense is possible, however, if it can be shown that the searching official was acting in good faith, according to an official duty. An official who uses bad judgment and conducts an illegal search has an excuse, but when the search is conducted illegally by intent, or not in connection with official duties, then the official can be charged with a violation.

Search

The term "search" denotes the examination of an alleged or suspected offender or his house or other building or property. The examination must be conducted in the normal course of enforcing the law or maintaining order. The examination must have a purpose of looking for some specific item or items. Items looked for will fall into one or more of the following categories: contraband, tools of a crime, fruits of a crime, or incriminating evidence. For an examination to be properly called a "search," the person conducting the examination must have some legal status. Not only must the searcher be duly empowered by law to make searches, but he must also possess a specific authority for

conducting a particular search at a particular place at a particular time to look for particular items. There are several ways for a searching official to demonstrate his authority to search. Most common among these is the search warrant. The term "search" does not include other kinds of "looking" functions. For example, an inspection of a place with a view towards reducing fire hazards is not a search. The close examination of an entry pass by a security officer is not a search.

The plain view doctrine is a rule of law that states it is not a search within the meaning of the Fourth Amendment to observe that which is open to view, provided that the viewing officer has a lawful right to be there. No warrant is required to seize items in plain view. Plain view exists when an officer who had justification for intrusion in the course of official duties inadvertently comes into contact with contraband in open view, and prior to the discovery was unaware of the existence of the contraband before coming upon it unexpectedly. The doctrine relies on the presumption that the officer has a right to be in a place where evidence or contraband is seen in an area open to plain viewing. An example would be an officer who is called to the scene of an assault and observes cocaine on a coffee table. The officer is legally on the premises and can seize the cocaine. However, if the cocaine was viewed by an officer observing through an open window, not in connection with official police business, the plain view doctrine would not apply. In this case, a search warrant would be required to make a search and seizure.

Seizure

The term "seizure" denotes the taking of contraband, fruits of a crime, tools of a crime, or incriminating evidence. The person taking the items must be empowered to make the seizure, and the items seized must be protected until disposed of in some proper fashion. If, for example, the item seized is a stolen ring, the ring will be safeguarded as evidence until the trial is completed. When the judicial action against the offender is ended, the ring will be returned to the owner. For some kinds of seized items, final disposition might be destruction. Narcotics, certain kinds of weapons, and illegal whiskey are examples of items that are usually destroyed after court action has ended.

Search Warrant

The term "search warrant" means a written order issued by competent legal authority that directs a search to be conducted. The warrant specifies who is to conduct the search, who or what place is to be searched, and the items to be looked for during the search. The warrant is made valid for only a certain limited period of time. In some cases a warrant might direct that the search be made at some particular time of night or day, but a warrant is never prepared so that the searcher can wait many days or weeks before deciding to carry out the warrant. A warrant is issued on the basis of a need that exists at the time the warrant is requested. The need cannot be interpreted to spread out over a long period of time. It should also be noted that the word "warrant" itself means an order. Although the person or agency carrying out the warrant was the requester of the warrant in the first place, it is the issuing judge who gives the order for a search to be conducted. A warrant is therefore not simply a permit granted to someone to conduct a search, it is an order to do so. That order is very specific in what must be done. The warrant will name a person or small number of persons who will carry out the warrant. The warrant will name the person, place, or property to be searched. Knowing the details of the area to be searched is sometimes of great importance to the requester of a warrant. For example, it might be very important to know that the building to be searched has a separate shed. Unless the shed is included in the warrant, it cannot be lawfully searched. It might be that the items to be looked for are in the shed. A little advance knowledge on the part of the searcher is important in getting a properly worded warrant. Along the same line, it is important that the warrant include mention of all items that are useful as evidence. If the case involves a search for an automatic rifle, the person requesting the warrant would want to include mention of ammunition, ammunition clips, magazines, or parts pertaining to the type of automatic rifle involved. If the warrant simply names the rifle as the item to be looked for, the searcher cannot technically seize anything except the rifle and

misses the chance of getting other pieces of evidence related to the same crime. Advance preparation in the wording of a warrant is therefore important.

A warrant is specific in one other regard. The judge's order will direct that any seized property be taken to some designated place or agency. Seized items are sometimes regarded as property of the court until such time as the items are properly disposed of, with disposition instructions normally issued by the court in writing. The proper safeguarding of seized property requires that the property be inventoried at the time it is seized. The inventory is placed into writing, usually on a receipt type of form that lists all items taken. The copy of the receipt is given, with the search warrant, to the person from whom the items were taken. If no such person is available, the receipt and search warrant are left at the place of seizure. The original copy of the receipt remains with the seized items and is used to account for the property from the time of seizure until the time of final disposition.

Affidavit

The term "affidavit" describes a written document that is used to support or justify the issuance of a search warrant. An affidavit is nothing more than a written statement made under oath. It sets forth details that provide the issuing judge with enough information for him to conclude that a crime was committed and that a search of a certain place will probably reveal the presence of some evidence pertaining to that crime. The affidavit therefore provides the type of information that is sometimes called "probable cause."

An affidavit might read as follows:

> I, John Doe, having been duly sworn, on oath depose and state that at 11:30 p.m., July 1st, 2006, at the premises of ABC Company, 1000 Main Street, Houston, Texas, a person unknown did steal a carton containing a Carrier air-conditioning unit, model X, serial number 123456, valued at $800.00. The affiant further states that Alfred Aware, a security officer at the premises, reported that at 11:30 p.m., July 1st, 2006, he observed a person exit a rear loading door of the building and place a large carton into the rear of a station wagon. Before Mr. Aware could reach the scene, the station wagon fled the area. Mr. Aware did, however, note the license plate number of the station wagon. A check with the license plate bureau revealed the owner of the suspect station wagon to be Billy Badguy, a tenant at 1115 North Street, Houston, Texas. An interview with Mrs. Betty Busybody, landlady at 1115 North Street, revealed that after midnight on July 1st, 2006, she observed Mr. Badguy carry a large carton into his rented room. She described the carton as having writing that said the carton contained a Carrier air-conditioning unit. In view of the foregoing, the affiant requests that authorization be issued for a search of rooms at 1115 North Street, Houston, Texas, that are rented and controlled by the person identified as Mr. Badguy, and that such authorization include seizure of a Carrier air-conditioning unit, serial number 123456.
>
> Signed, John Doe
>
> Sworn to and subscribed before me this Third Day of July 2006, at Houston, Harris County, State of Texas.
>
> Signed, Lawrence Law, District Attorney

In this fictionalized sample of an affidavit, the most important pieces of information were provided by a security officer. The security officer provided the time, date, place, a description of the property stolen, and certain other details that led to an identification of the suspect.

In other words, the security officer observed and made notes as to the who, what, when, where, and how elements of an offense. It is this kind of basic information that will add up to a total picture so as to provide probable cause for a judge to issue a search warrant. The basic information in the affidavit demonstrates firstly that a crime happened. The affidavit then leads to a reasonable conclusion that some evidence of that particular crime will probably be found at a certain place. When these requirements are satisfied, a judge will likely grant the request for a search warrant.

A few other terms need to be explained regarding searches. We have already mentioned the terms "contraband," "fruits of the crime," "tools of the crime," and "incriminating evidence." Items to be looked for and seized

in connection with a search will fall into one or more of these four categories.

Contraband

Contraband is any item that, by itself, is a crime to have. Bootleg whiskey is contraband because possession of it is against the law. The same holds true for certain types of firearms, explosives, illegal narcotics, marijuana, pornographic materials, and counterfeit money. Search warrants are issued to cover the seizure of contraband when it is known in advance that contraband is present at a certain place. If such contraband is seized without getting the search warrant, the seizure is illegal; however, contraband that is discovered accidentally can be seized without a warrant. In regard to contraband, it can always be seized. How it was seized will determine whether the contraband can be used as evidence against the person responsible for it.

Fruits of the Crime

This is a term referring to that advantage which is derived by the criminal who commits a crime. A stolen television set and swindled money are all examples of fruits of crime.

Tools of the Crime

This term refers to the devices used in the commission of the illegal act. Tools in this sense obviously include burglary devices such as a jimmy, lock pick, bolt cutter, and so forth. Tools also include a worthless check, a false document, or even a fraudulent advertisement.

Incriminating Evidence

The term "incriminating evidence" covers a wide range of items. In this category are items that tend to show involvement of a suspect or an accomplice in a criminal activity. The item could be a shirt bearing blood stains acquired during the crime, it could be a diary containing references to a crime, it could be a photograph showing some relationship to a crime, or it could even be a tape recording of accomplices discussing a crime.

Reasonableness

An understanding of the foregoing terms will be of assistance in understanding further concepts associated with search and seizure. One other term, which is common to everyday language, should be looked at in respect to the matter of legal searches. The term "reasonable" is sometimes used to describe the nature of a search conducted with authority of a search warrant. Since probable cause has to be present for a search warrant to be issued, it can be said that the search was reasonable. The term reasonable then becomes almost identical with words like "constitutional," "lawful," or "legal." The term "unreasonable" is therefore just the opposite of "reasonable" in meaning. "Unreasonable" has often been used to describe searches that were conducted without benefit of a search warrant. An example of an "unreasonable search" would be an examination of a place for the purpose of finding any kind of evidence that might possibly be used against a person. This type of search is unreasonable because it is not specific in terms of what item or items are expected to be found. Such a search is exploratory and is in the nature of a fishing expedition.

Search Without a Warrant

This does not mean that only searches conducted with warrants can be properly called reasonable. A search with a warrant is certain to be reasonable, but other searches can be considered reasonable, if they are conducted under certain conditions. Let us look at those situations in which it is possible to conduct reasonable searches without the use of a search warrant.

Search Incidental to Arrest

Perhaps the most common type of search is the search made in connection with an arrest. A check of a person's possessions at the time he is taken into custody is mainly intended to discover the presence of weapons that can be used against the arresting person. The arresting person has a right to protect himself from attack by a weapon concealed on the body of the arrested person. A search at the time of arrest is mainly directed toward this consideration. A second consideration for the arresting person is to see if the offender has

any evidence on his person that is connected with a crime. It is important that the evidence be taken before the suspect has an opportunity to destroy or discard it. A frisk or wall search will normally reveal the presence of weapons or destructible evidence. The frisk and wall search are called precautionary searches because they are designed to take precautions against attack and against the chance of losing valuable evidence. Property in the possession of the arrested person can be searched. This would include packages, brief cases, and the like. The place under immediate control of the arrested person can be searched for evidence connected to the crime. Thus, when a person is arrested in his private office, the unlocked areas of the office can be legally searched. If the arrest is made in a building lobby, the lobby cannot be searched because it is not under immediate control of the suspect at the time of arrest. Vehicles driven by an arrested person can be searched, but only those areas of the vehicle that are controlled by the suspect. The trunk of a vehicle is not considered to be under control of the suspect at the time of arrest. If it is felt that a search of the trunk will probably yield evidence connected to a crime, a search warrant can be requested. If the arrested person is a woman, the search can include only the purse, coat, parcels, baggage, or other articles not worn by her.

The Emergency Search

Another type of lawful search and seizure is the looking for and taking of criminal goods before those goods can be disposed of. This form of search is in the nature of an emergency action that is taken to prevent the removal, destruction, or further hiding of property illegally held by a suspect. To illustrate, assume a company employee discovers that three rolls of 25-cent pieces are missing from a box containing the company's petty cash fund. The employee calls the security office and explains that he knows the missing rolls of quarters were in the box minutes prior to the time the cleaning man had access to the cash box, and the cleaning man is getting ready to leave the company premises. Under circumstances like this, a search of the cleaning man would be justified. A search is justified because facts show that a crime was committed, that the stolen property is probably in the possession of the suspect, that the suspect is leaving and there is no time to obtain a search warrant, and that to recover the stolen property it is necessary to take emergency action before the suspect can leave with the stolen money.

Search with Consent

Another kind of search not requiring a warrant is search by consent. The consent must be freely and intelligently given. Consent cannot be obtained through the use of threats or trickery. The person giving permission to search his person or property must do so in a completely willing manner. For the consent to be intelligently given, the person must be able to recognize the consequences of permitting a search. A person who is too young, too old, too drunk, retarded, ill, or insane cannot intelligently give consent to a search. Also, mere submission or giving in to a request for consent is not the same as giving a free consent. In order to demonstrate that consent to search was freely and intelligently given, the security officer should obtain the consent in writing. The writing itself, the words used, and the physical act of writing help to demonstrate that the consent was properly obtained.

Any consent obtained must be obtained from the person who has a right to give the consent. A hotel manager cannot give consent to search a paying guest's hotel room. A person sharing an apartment cannot give consent to a search of another person's property within the apartment. This is an important point to remember when asking for consent to conduct a search.

Purposes of a Search

It can be said that a search and seizure action has two overall purposes. One is to discover and obtain evidence that will bring the criminal to justice. The other is to recover property that belongs to another person. A search and seizure that achieves both these purposes is what we strive for.

Sometimes, because of improper methods in a search, the goal of justice is not realized. Evidence is inadmissible in a court of law if it was obtained as the result of an unlawful search or seizure. The law also goes on to provide that other evidence obtained later, quite lawfully, cannot be used if it was connected in any way with a preceding unlawful search. For instance, assume that an unlawful search resulted in the discovery

of a notebook containing information that led to the identification of other accomplices and hiding places of stolen property. Any evidence discovered from lawful searches made of the accomplices and the hiding places cannot be made in court. For this reason it is important to keep in mind the major points of law dealing with search and seizure.

John J. Fay

SENTENCING OF CORPORATIONS: FEDERAL GUIDELINES

In 1984 the Sentencing Reform Act established the U.S. Sentencing Commission. The Commission's mandate was to create guidelines designed to eliminate disparity in sentences being meted out by federal courts. The idea was to replace a very loose sentencing approach with an approach that would be consistent and impose punishments equal to the crimes committed.

In creating the Commission, Congress was making it clear that indeterminate sentencing had grown excessively lenient and that a tougher stance on crime was needed. Congress instructed the Commission to "insure that the Guidelines reflect the fact that, in many cases, current sentences do not accurately reflect the seriousness of the offense." The Commission's response to Congressional concern was its stated objective to "avoid unwarranted sentencing disparities among defendants with similar records who have been found guilty of similar criminal conduct while maintaining sufficient flexibility to permit individualized sentences when warranted by mitigating or aggravating factors not taken into account in the establishment of general sentencing practices."

Accordingly, the Commission established Guidelines for determining sentences, including whether to impose a sentence of probation, fine, or imprisonment, and if so, how long and/or how much; whether the defendant should be placed on supervised release after imprisonment; and whether multiple sentences should run concurrently or consecutively. Most observers agree that the Guidelines have generated more and longer prison terms and heavier fines.

In 1988, the mandate of the Commission was expanded to include development of Guidelines for the sentencing of corporations. The stated purposes were to (1) substantially increase most of the fines imposed on companies convicted of crime, (2) introduce a concept of "corporate probation," and (3) call for self-reporting of crimes discovered by corporate management. The interesting and important part is that a corporate defendant's culpability can be mitigated by having a program in place to detect violations and by self-reporting of offenses prior to investigation. In effect, a corporate defendant has a measure of control over the leniency or severity of its sentence by its own action taken before and after its violation of the law. The Guidelines provide strong incentive for compliance and self-policing. Indeed, the U.S. Sentencing Commission has said that the purposes of the Guidelines are to "provide just punishment, adequate deterrence, and incentives for organizations to maintain internal mechanisms for preventing, detecting and reporting criminal conduct."

On November 1, 1991, the Guidelines became law. If the same tough stance that has been applied in individual sentencing is carried over to business organizations, corporate management should be concerned. A sense of foreboding can be found in the new corporate Guidelines in the statement that the "goals and purposes of sentencing for organizations are identical to those for individuals."

At present, the impact of the law on corporate behavior is uncertain, but many commentators anticipate that because sentences will be defined and judicial discretion reduced, punishment for corporate crime will be more predictable. It is certain, however, that the intent of the government is to seek increased penalties against companies for anti-trust and other violations. The Department of Justice is on record about its intent to vigorously pursue corporate offenders.

Guidelines

Prevention and Detection. The Guidelines call for a credible effort to detect and deter crime. The elements of a compliance program are spelled out. Anything less will expose a corporation and its officers to substantial punishment.

Remedies. A convicted organization must notify the victims of the crime and take appropriate action to compensate them or remedy the harm. Full restitution either as part of the sentence or as a condition of probation is provided, trust funds for victims may be ordered, and community service is an option.

COMPLIANCE POLICY: CONCERNING CORPORATE CONDUCT

(Sample)

The Company and each of its subsidiaries will establish and maintain an effective compliance program that conforms to the standards established in the Sentencing Guidelines promulgated by the U.S. Sentencing Commission. The program will be designed, implemented, and enforced with the purpose of being effective in preventing and detecting criminal conduct.

The Company will exercise due diligence in attempting to prevent and to detect criminal conduct by its employees and agents. To those ends the Company will establish and maintain the policies and practices set forth as follows:

1. The Company will determine the likelihood that there is a substantial risk that certain types of criminal offenses may occur.

2. The Company will establish and maintain compliance standards and procedures to be followed by its employees and agents which are reasonably capable of reducing the prospect of criminal conduct.

3. Specific high-level individuals within the Company shall be assigned overall responsibility to oversee compliance with such standards and procedures. Division and subsidiary presidents and vice presidents in charge of corporate staff functions are hereby assigned such responsibility for their respective divisions, subsidiaries, and departments.

4. The Company will not delegate substantial discretionary authority to any individual it knows, or through the exercise of due diligence should have known, had a propensity to engage in illegal activities.

5. The Company will take reasonable steps to communicate effectively its standards and procedures to all employees and other agents.

6. The Company will take reasonable steps to achieve compliance with its standards. Such reasonable steps include the establishment of monitoring and auditing systems that are reasonably designed to detect unlawful conduct by employees and agents, and establishing, monitoring, and publicizing a reporting system whereby employees and other agents can report abuse by others within the organization without fear of retribution.

7. The Company will consistently enforce its standards through appropriate disciplinary mechanisms, including, as appropriate, discipline of individuals responsible for the failure to detect an offense.

8. If a criminal offense is detected, the organization must take all reasonable steps to respond appropriately to the offense and to prevent similar offenses.

9. Each division and subsidiary will establish one or more committees to assist the president of the division or subsidiary in the implementation and enforcement of this program.

10. These compliance statements are intended to establish a procedural framework; they are not intended to set forth in full the substantive compliance programs and practices of the Company and its subsidiaries. Additional standards for compliance are established and maintained by virtue of the practices, procedures, and policies of the Company and the form of organization that manages the Company, and those additional practices, procedures, policies, and organization are an integral part of the compliance program.

Fines. Fines are assessed using a complicated formula that considers the seriousness of the offense and the culpability of the offending organization. The first step is to determine a base fine that is the greater of the dollar value of the gain to the offender/loss to the victim, or an amount determined by a table of fines set out in the Guidelines.

The second step is to determine a "culpability score" based on aggravating and mitigating factors. Aggravating factors might be foreknowledge by management, concealment of the offense, and a history of prior offenses; mitigating factors might be the existence of a compliance program, prompt reporting of the offense, and cooperation in the investigation. The culpability score is cross-referenced to minimum and maximum multipliers.

In the third step, the multiplier is applied to the fine. A low culpability score can lead to a fine smaller than the base fine while a high culpability score may lead to a fine many times larger.

To illustrate, assume that the victim's damages were $100,000 and that the court used this amount as the base fine. The judge noted that the culpability score is 10 points based on aggravating factors. In looking at the Guidelines table, the minimum multiplier is 2 and the maximum is 4. The judge can set the fine no lower than $200,000 and no higher than $400,000.

Probation. In addition to requiring payment of damages and a fine, the judge can place a company on probation for up to 5 years. Probation is mandatory if at the time of sentencing the company does not have in place an acceptable compliance program. When this happens, the court will impose a program that it will periodically monitor.

Developing a Compliance Program

The first objective of a compliance program is to keep from violating criminal laws; the second objective is to achieve the lowest possible culpability score if the first objective is not met. A compliance program to meet these two objectives will include:

- Written policy, directives, and procedures to guide employees.
- The assignment to specific senior management of responsibilities for the proper execution of the compliance program.
- Steps to prevent giving discretionary authority to individuals whom the company knew or should have known had a propensity to engage in illegal acts.
- An education component for informing employees of their personal responsibilities under the program.
- A monitoring and auditing system to detect deviations from compliance, including a mechanism for employees to report suspected criminal conduct without fear of retribution.
- Consistent enforcement of compliance standards with appropriate disciplinary sanctions.
- Steps to prevent recurrence of offenses, including needed changes to the program.

The Federal Sentencing Guidelines add a new dimension to corporate accountability by emphasizing compliance programs, self-policing, and reporting of offenses. The sentencing judge is bound to a highly defined, essentially mathematical scheme when determining sentences. The result in many cases will be heavy fines and invasive probation.

John J. Fay

Sources

"Amendments to the Sentencing Guidelines for United States Courts." 1992. *Federal Register*, Vol. 57, No. 91, 1992.

Fett, L. 1991. *New Corporation Sentencing Guidelines: Perils and Possibilities of Compliance Programs and Self-Policing*. Washington: American Corporate Counsel Association.

Machlowitz, D. 1991. *Designing and Implementing Corporate Compliance Policies*. Lyndhurst: General Instrument Corporation.

Murphy, J. 1989. *Corporate Compliance Programs: Counsel's Role*. Washington: American Corporate Counsel Association.

Nord, N. 1991. "Sentencing Guidelines Up the Ante for Corporate Compliance Programs." *American Corporate Counsel Association Docket*, Fall, 1991.

Olson, J. and Mahaffey, D. 1992. *Criminal Exposure in the Corporate Environment*. Washington: American Corporate Counsel Association.

"Sentencing Guidelines and Policy Statements for Federal Courts." *Federal Register*, Vol. 57, No. 1, 1992.

TESTIFYING

The person who has investigated a case is often the most important witness in the trial of that case. He may be the only person with a comprehensive understanding of a crime sufficient to give a complete, coordinated view of what happened. He is, therefore, the main communications system through which evidence of a crime is transmitted to the finder of fact at trial.

The importance of a good presentation by the investigator on the witness stand cannot be overemphasized. Hours and hours of the most competent investigation and preparation may be wasted if the results are improperly presented in court. The trier of fact (usually the jury) comes into court having no prior knowledge of what happened or who is guilty or innocent. The picture the jury gets depends largely on the ability of the investigator to testify truthfully and accurately, and to do so in a manner that impresses everyone present that he is intelligent, honest, competent, and fair. The defense attorney will do everything legally permitted to twist the evidence in his client's favor. If the investigator is confused, hazy, or unsure of important facts, the jury will be similarly confused and hazy. However, if he presents a clear-cut report containing all elements of proof in a calm, unprejudiced manner, the jury will see the case in the same light.

Furthermore, a verdict of guilty accomplishes little if an investigator has testified so poorly that he affords the accused good grounds for a new trial or for a reversal on appeal. Neither does a guilty verdict accomplish the good it should unless the trial has been conducted in such a manner that everyone in the courtroom has been impressed with the dignity and justice of the proceedings. Public confidence in our system of justice is essential to its proper function.

Preparation before Trial

Effective testimony in court depends to a large extent on preparation. Preparation begins with the first notification that a possible crime has been committed. All facts, observations, and actions having to do with the case should be carefully recorded in notes, reports, and photographs, keeping in mind that the information may eventually be introduced in court. Proper investigative procedures cannot be stressed strongly enough, because there are often long delays between the investigation of a case and the trial, and unless information is recorded, much of it is sure to be forgotten in the interim.

Knowledge of the Case. As the time of trial draws near, the investigator should make a complete review of the case and refresh his memory of the facts by carefully reading through all notes and reports. He should also examine physical evidence that has been collected, in the event that it has to be identified or referred to in court. Then he should put his thoughts together so he can visualize the whole case in the sequence in which it happened. Testimony presented to a jury as a chain of events in the order that they occurred is both interesting and convincing.

An investigator may be allowed to refresh his memory on the witness stand by referring to his notes or reports. However, if he does, the defense counsel has a right to examine these notes and question him about them. Therefore, the investigator should discuss with the prosecuting attorney the advisability of taking notes to the witness stand.

Also, the prosecuting attorney may want to confer with the investigator about the facts of the case at a pre-trial session. At this session, the prosecuting attorney may try to re-awaken the investigator's senses to recall parts of the investigation that he deems essential to the case and to go over the investigator's testimony. This is entirely proper and, at this time, the investigator should make sure that the prosecuting attorney knows all the facts of the case, whether favorable or unfavorable to the defendant. The prosecuting attorney may not, however, tell the investigator what to say or influence the investigator to deviate from the truth in any way.

Knowledge of the Rules of Evidence. Besides knowledge of the case being tried, the investigator testifying in court should have a basic knowledge of the rules of evidence. This knowledge will help him to better understand the proceedings and enable him to testify more intelligently, removing the opportunities for

delay and confusion that can occur in the mind of the investigator when placed under pressure in the courtroom.

Appearance and Attitude. When an investigator appears in court, he must observe the highest standards of conduct. The minute he walks to the witness stand, he becomes the focal point of interest and observation by the public.

The key thing for an investigator to impress in his mind when testifying in court is that he is engaged in a very solemn and serious matter. He should look and act accordingly. While waiting to testify, the investigator should not linger outside the door of the courtroom smoking, gossiping, joking, laughing, or engaging in other similar conduct. This distracts attention from the proceedings and shows little regard for the serious nature of the occasion. Rather, the investigator should be seated quietly in the courtroom while awaiting his turn to take the stand, unless he is directed to wait in the witness room.

An investigator's appearance while testifying should be neat and well-groomed. He should wear a clean suit, tie, and shined shoes. Neither should he wear dark glasses, smoke, chew gum, or generally fidget around while on the witness stand. A favorable impression is created if the investigator sits erect but at ease in the witness chair and appears confident, alert, and interested in the proceedings.

Testimony during Trial

Our system of securing information from a witness at a trial is by the question and answer method. The questioning by attorneys on direct examination serves merely to guide the witness in his testimony and to indicate the information that is required. After direct examination, the witness may be subject to cross-examination by the opposing counsel. The questions on cross-examination will have the opposite purpose of those asked on direct examination. Cross-examination questions may be devious, deceptive, or innocent in appearance, masking the opposing counsel's real objective, which is to discredit or minimize, to as great an extent as possible, the effect of the witness's testimony. The investigator is usually a witness for the state. Direct examination is by the prosecuting attorney, with cross-examination by counsel for the defense.

There are no definite rules for testifying effectively in court because each case has its own peculiarities. However, there are general guidelines for answering questions that should be followed in most cases and some specific suggestions designed to aid the witness on cross-examination.

Answering Questions on the Witness Stand

When taking the oath, the investigator should be serious and stand upright, facing the officer administering the oath. He should say "I do" clearly and positively and then be seated to wait for further questioning.

The investigator should listen carefully to the questions asked and make sure he understands each question before answering. If he does not understand, he should say so, and ask to have the question repeated. He should then pause after the question long enough to form an intelligent answer and to allow the attorneys and judge time to make objections.

Answers to questions should be given in a confident, straightforward, and sincere manner. The investigator should speak clearly, loudly, and slowly enough so that all in the courtroom can hear, and he should avoid mumbling or covering his mouth with his hand while talking. He should look at the attorney asking the questions but direct his answers toward the jury. Simple conversational English should be used, and all slang and unnecessary technical terms avoided. Most importantly, the investigator should be respectful and courteous at all times despite his feelings toward the people involved in the case. He should address the judge as "Your Honor," the attorney as "Sir," and the defendant as "the Defendant."

The essential rule to be observed above and beyond all others is to always tell the truth, even if it is favorable to the defendant. Facts should not be distorted or exaggerated to try and aid a conviction, nor should details be added to cover up personal mistakes. Once it has been shown that an investigator has not truthfully testified as to one portion of his investigation, no matter how small and inconsequential, the jury may reject the truthfulness of all other testimony which he may offer. On the other hand, an investigator's testimony will appear strong if it is a truthful recital of what he did and observed,

even though it reveals human error on his part and favors the defendant in some parts.

Answers to questions should go no further than what the questions ask for. The investigator should not volunteer any information not asked for. If a question requests a "yes" or "no" answer and the investigator feels it cannot properly be answered in this manner, he should ask to have the question explained or re-worded, or request the right to explain his answer. He may state that he cannot answer the question by "yes" or "no." This should alert the prosecuting attorney to come to his assistance.

Answers to questions should be given as specifically as possible. However, figures for time, distance, size, etc., should be approximated only, unless they were exactly measured by the investigator.

When an investigator is referring to a map or plan in his testimony, he should identify the point on the map as clearly as possible so it becomes part of the trial record. For example, he should say "the northwest corner of the room" rather than just point to the spot and say "here" or "there." If the investigator does not understand the map or plan that is to be used at trial, he should tell the prosecuting attorney before trial and go over it with the person who prepared it.

If a wrong or ambiguous answer is given, it should be clarified immediately. It is far better for an investigator to correct his own mistakes than to have them pointed out to the jury by the defense attorney or a subsequent witness.

If a judge interrupts or an attorney objects to an investigator's testimony, the investigator should stop talking instantly. However, he should not anticipate an objection when a difficult question is asked but should only pause long enough to form an intelligent answer.

Under no circumstances should an investigator memorize his testimony. It will only sound rehearsed and false, and will not inspire the confidence of the jury. Instead, the investigator should have a thorough knowledge of the facts of the case and organize them in his mind so he can recite them as a narrative. If a particular fact or circumstance becomes hazy or is forgotten, the investigator may be allowed to refresh his memory from his notes as long as this does not become a habit. It is worth noting that if an investigator does refer to notes, they may be examined by the opposing counsel. If for any reason, the judge criticizes an investigator's conduct in court, the investigator should not allow it to disturb his composure. The best policy is to ask the court's pardon for the error committed and proceed as though nothing had occurred.

Cross-Examination

In a criminal trial, it is the duty of counsel for the defendant, as an officer of the court and as an attorney, to use every legal means to secure the acquittal of the client or the best possible verdict under the circumstances. Since the investigator is often a chief witness for the state, the defense attorney, in order to win, must normally discredit or nullify the investigator's testimony, or at least minimize its importance in the eyes of the jury. To do this, he may use every device legally available to him. He may attempt to show that the investigator did not have the proper opportunity to observe the facts, or that he was inattentive or mistaken in his observations. He may try to make it seem like the investigator is lying or leaving out facts which are favorable to the defendant. In trials of crimes that happened some time ago, the defense counsel may try to show that the investigator's recollection of the entire event is bad and that he knows nothing without his notes. He may even try to show that the investigator has a grudge against the defendant. One of the ways of doing this is to goad the investigator into losing his temper to give the appearance of being personally antagonistic to the defendant. Under the proper circumstances, all these approaches are legal and available for the use of defense counsel.

The best defense against the techniques and devices of the defense attorney is thorough preparation. If the investigator has carefully observed the facts at the time of their occurrence, made complete and sufficient notes, reviewed his notes and reports carefully to fix the events in his memory, and testified truthfully, he need have no fear of cross-examination. Nevertheless, there are a few important suggestions regarding cross-examination that help prevent the investigator from falling into the traps laid by a clever defense attorney. Some of these suggestions have been mentioned previously and others apply exclusively to cross-examination.

- The investigator should not become angry or argumentative with the defense attorney. This is exactly what the defense attorney wants. Rather, the investigator should stick to calmly answering all questions unless an objection is sustained by the judge.
- The investigator should make very clear by his attitudes and statements that he has no personal feelings against the accused. If an accused has been nasty, insulting, or even has assaulted the investigator, the defense attorney may make much of such occurrences to persuade the jury that the investigator has a personal grudge in the matter and is "out to get" the accused. Jurors, being only human, are quick to resent any evidence of overbearing conduct or personal animosity on the part of the witness. The investigator, in this situation, should make clear that such things are common occurrences in his line of work and that they have no bearing on the matter as far as the facts are concerned.
- The investigator should not be afraid to admit mistakes made either in his investigation or his prior testimony. No one is perfect and an investigator admitting his errors himself will give defense counsel less fuel for attacking his credibility.
- If a defense attorney's question is not clear, the investigator should tell the court and ask to have it re-stated. An answer to an ambiguous question may very likely be a setup for a contradiction later on.
- The investigator should never be afraid to admit that he had discussed his testimony before trial with the prosecuting attorney, his superiors, or other investigators. This is entirely proper and accepted procedure. However, defense counsel, in the way he asks the question, may try to make it seem improper, and thereby trick the witness into a lie.
- If defense counsel seeks to cut off an investigator in the middle of his testimony, the investigator may turn to the judge and request an opportunity to explain his answer. This request will usually be granted.

Conduct after Trial

When an investigator leaves the witness stand, he should do so quickly and quietly, and return to his seat or leave the courtroom if no longer needed. He should not linger to talk to the prosecutor. If he should have additional information or ideas to tell the prosecutor, they should be written down and passed to the prosecutor with a minimum amount of display. When an investigator leaves the courtroom he should not loiter to talk or gossip with others and, most important, he should not talk to jurors if it is a jury trial.

Convincing and effective testimony by the investigator is essential to successful operation of the criminal justice system and depends on proper preparation, approach, and experience. The suggestions outlined previously are designed to familiarize the investigator with court procedure and improve his testimony as a witness. The preparation and individual effort required in this endeavor is a minimum expectation.

John J. Fay

Source Fay, J. 1979. *Special Agent Manual.* Atlanta: Georgia Bureau of Investigation.

TORT LAW

Public police officers have greater powers than private sector officers. In conjunction with police powers, public officers are limited in their actions by the Bill of Rights. On the other hand, private officers, who possess lesser powers, are, for the most part, not heavily restricted by constitutional limitations. Authority and limitations on private officers result from tort law.

Tort law is the body of state legislative statutes or court decisions that governs citizen actions toward each other and allows lawsuits to recover damages for injury. Tort law is the foundation for civil actions in which an injured party may litigate to prevent an activity or recover damages from someone who has violated his/her person or property. Most civil actions are not based on a claim of intended harm, but a claim that the defendant was negligent. This is especially so in cases involving private security officers. Tort law requires

actions that have regard for the safety and rights of others; otherwise negligence results. The essence of the tort law limitations on private officers is fear of a lawsuit and the payment of damages.

The primary torts relevant to private sector police are as follows:

1. False Imprisonment. The intentional and forceful confinement or restriction of the freedom of movement of another person. Also called "false arrest." The elements necessary to create liability are detention and its unlawfulness.
2. Malicious Prosecution. Groundless initiation of criminal proceedings against another.
3. Battery. Intentionally harmful or offensive touching of another.
4. Assault. Intentional causing of fear of harmful or offensive touching.
5. Trespass to Land. Unauthorized entering upon another person's property.
6. Trespass to Personal Property. Taking or damaging another person's possessions.
7. Infliction of Emotional Distress. Intentionally causing emotional or mental distress in another.
8. Defamation (Libel and Slander). Injury to the reputation of another by publicly making untrue statements. Libel refers to the written word; slander to the spoken word.
9. Invasion of Privacy. Intruding upon another's physical solitude, the disclosure of private information about another, or public misrepresentation of another's actions.
10. Negligence. Causing injury to persons or property by failing to use reasonable care or by taking unreasonable risk.

Civil action is not the only factor that hinders abuses by the private sector. Local and state ordinances, rules, regulations, and laws establish guidelines for the private security industry. This usually pertains to licensing and registration requirements. Improper or illegal action is likely to result in suspension or revocation of a license. Criminal law presents a further deterrent against criminal action by private sector personnel. Examples are laws prohibiting impersonation of a public official, electronic surveillance, breaking and entering, and assault.

Union contracts can also limit private police. These contracts might stipulate, for instance, that employee lockers cannot be searched, and that certain investigative guidelines must be followed.

Contract Law

Torts often result from the failure of a party to meet the requirements of a contract. A contract is basically an agreement between parties to do or to abstain from doing some act. The law may enforce the agreement by requiring that a party perform its obligation or pay money equivalent to the performance. These court requirements are known as remedies for breach of contract. Specific circumstances may create defenses for failure to perform contract stipulations. Contracts may be express or implied. In an express contract—written or oral—the terms are stated in words. An implied contract is presumed by law to have been made from the circumstances and relations of the parties involved.

There are several areas in the security/loss prevention field relevant to the law of contracts. The company that provides a service or device to a client company may be liable for breach of contract. Also, a contract usually states liabilities for each party. For instance, if a third party is harmed (e.g., a person illegally arrested on the premises by a private officer from a contract service hired by a client company), the contract will commonly establish who is responsible and who is to have insurance for each risk. However, in third-party suits, courts have held a specific party liable even though the contract stipulated that another party was to be responsible in the matter.

In the common law principle of *respondeat superior* (i.e., let the master respond), an employer (master) is liable for injuries caused by an employee (servant). Typically, the injured party will look beyond the employee—to the employer—for compensation for damages. Proper supervision and training of the employee can prevent litigation.

Another form of contract is the union contract. If a proprietary force is employed on the premises, a union contract may be in existence. As stated earlier, union contracts for regular employees may have certain guidelines for locker searches and investigations.

Philip P. Purpura

Source Purpura, P. 2002. *Security and Loss Prevention, 4th Edition*. Boston: Butterworth-Heinemann.

TORTS

A crime is a public wrong and a tort is a private wrong. A public wrong is remedied in a criminal proceeding and a private wrong is remedied in a civil proceeding. A single act in some instances will constitute both a crime and a tort. For example, if a person commits an assault and battery upon another, he commits a crime (a public wrong) and a tort (a private wrong). The law will seek to remedy both wrongs, but it will do so in different ways.

The state will move on its own authority to do justice by bringing a criminal action against the offender. The victim is also entitled to bring action against the offender in a civil suit. Tort law gives the victim a cause of action for damages in order that he may obtain sufficient satisfaction. The victim, however, pursues a civil remedy at his own discretion and in his own name. Whether the victim wins his lawsuit or not, the judgment will not prevent prosecution of the offender by the state.

The civil injuries involved in tort cases usually arise from acts of negligence. The fact that by his own negligence the victim contributed to the harm done may afford the offender a defense in a civil action of tort, but it does not constitute a defense to the offender in a criminal prosecution.

The single characteristic that differentiates criminal law from civil law is punishment. Generally, in a civil suit the basic questions are:

- How much, if at all, has the defendant injured the plaintiff, and
- What remedies, if any, are appropriate to compensate the plaintiff for his loss?

In a criminal case, the questions are:

- To what extent has the defendant injured society, and
- What sentence is appropriate to punish the defendant?

Tort Law Purposes

Tort law has three main purposes:

- To compensate persons who sustain a loss as a result of another's conduct
- To place the cost of that compensation on those responsible for the loss
- To prevent future harms and losses

Compensation is predicated on the idea that losses, both tangible and intangible, can be measured in money.

If a loss-producing event is a matter of pure chance, the fairest way to relieve the victim of the burden is insurance or governmental compensation. Where a particular person can be identified as responsible for the creation of the risk, it becomes more just to impose the loss on the responsible person (tortfeasor) than to allow it to remain on the victim or the community at large.

The third major purpose of tort law is to prevent future torts by regulating human behavior. In concept, the tortfeasor held liable for damages will be more careful in the future, and the general threat of tort liability serves as an incentive to all persons to regulate their conduct appropriately. In this way, tort law supplements criminal law.

Damages: Compensatory and Punitive

When one person's tortious act injures another's person or property, the remedy for the injured party is to collect damages. The common law rules of damages for physical harm contain three fundamental ideas:

- Justice requires that the plaintiff be restored to his pre-injury condition, so far as it is possible to do so with money. He should be reimbursed not only for economic losses, but also for loss of physical and mental well-being.

- Most economic losses are translatable into dollars.
- When the plaintiff sues for an injury, he must recover all of his damages arising from that injury, past and future, in a lump and in a single lawsuit.

If the defendant's wrongful conduct is sufficiently serious, the law permits the trier of fact to impose a civil fine as punishment to deter him and others from similar conduct in the future. Punitive damages (also called exemplary or vindictive damages) are not really damages at all since the plaintiff has been made whole by the compensatory damages awarded in the same action. Punitive damages are justified as:

- An incentive for bringing the defendant to justice.
- Punishment for offenses that often escape or are beyond the reach of criminal law.
- Compensation for damages not normally compensable, such as hurt feelings, attorneys' fees, and expenses of litigation.
- The only effective means to force conscienceless defendants to cease practices known to be dangerous and which they would otherwise continue in the absence of an effective deterrent.

The Intentional Tort of Intrusion

Interference with the right to be "let alone" can be grouped into four categories: intrusion, appropriation of one's name or likeness, giving unreasonable publicity to private facts, and placing a person in a false light in the public eye. The latter three of these are founded upon improper publicity, usually in the public press or electronic media. They are beyond the scope of this concept and will not be discussed.

Intrusion is an intentional tort closely related to infliction of emotional distress. Both torts protect a person's interest in his mental tranquility or peace of mind. A person has a basic right to choose when and to what extent he will permit others to know his personal affairs. Essentially, intrusion is an intentional, improper, unreasonable, and offensive interference with the solitude, seclusion, or private life of another. It embraces a broad spectrum of activities. It may consist of an unauthorized entry, an illegal search or seizure, or an unauthorized eavesdropping, with or without electronic aids.

The tort is complete when the intrusion occurs. No publication or publicity of the information obtained is required. It is, of course, essential that the intrusion be into that which is, and is entitled to remain, private. Additionally, the harm must be substantial. The intrusion must be seriously objectionable, not simply bothersome or inconvenient.

John J. Fay

Source Fay, J. 1987. *Butterworths Security Dictionary: Terms and Concepts*. Boston: Butterworth-Heinemann.

VI: Physical Security

ACCEPTANCE TESTING

Technology continues to advance and physical security systems advance with it. Today's security systems are becoming more and more complex. The introduction of information technology into physical security systems has made the pace of technological change so rapid that physical security components moving along the assembly line can almost become obsolete before they reach the shipping dock. In the rush to get products to end-users, some manufacturers begin shipping "the next version" of products and systems before they have been fully tested. This one fact alone is reason enough for end-users to require extensive testing of physical security systems prior to accepting them.

Does the System Work Correctly?

For the end-user the important issue is not whether each of the long list of security system features will work properly; the interest is in the specific system features that address the user's security needs. The important questions in the end-user's mind will be:

- Do the features of the system support my security objectives?
- Are these features set up correctly?
- Do these features operate correctly?
- Do they operate the way I expect them to operate?

The last three questions can only be answered by testing. What follows is a baseline of best practices for acceptance testing.

System Testing

System testing is a primary element of on-schedule and in-budget security system projects. The larger the project, the more critical the testing becomes—but testing is important in a project of any size. An electronic security system integrates multiple components such as alarms, access control, and CCTV. In some cases, the components were acquired from more than one manufacturer, yet they are interdependent and communicate with each other. A system can have almost any combination of components for the simple reason that almost all facilities have different security needs. A mix of components can also result from adding or changing out the components of an existing system.

A separate circumstance that affects testing is bringing a newly acquired system into operation before testing can be done or even started. This often occurs when installation of a new system runs behind schedule and a deadline must be met.

Scenario-Based Testing

A purpose of scenario-based testing is to ensure that the system will operate according to the organization's security plans and procedures such as those that deal with responses to various emergencies. This form of testing is also used to evaluate the system's efficiency under normal, routine conditions. An emergency scenario could be the simulation of a serious fire or an attempt to breach the facility's outer fence line. A routine scenario could be a test to determine if an access control point is capable of admitting a certain number of people in a certain length of time.

What to Test?

Testing can be defined as "a process of ascertaining if a certain thing will perform as expected." Expectations are determined by the user. The user prepares, often with help from a consultant, a written functional requirements document, which says in plain language what these expectations are.

The system provider uses this document to develop a complete specification and equipment list along with descriptive design information that explains how the offered products will meet or exceed expectations. Descriptive materials such as product brochures, data sheets, and specification sheets are usually included in proposals submitted with bids.

In the bidding context, the prospective client's expectations are clearly detailed in specifications that are given to the system provider.

Specifications can be expressed in a variety of documents:

- A functional requirements document.
- Architect and engineer (A&E) documentation. An A&E describes in technical terms the user's requirements. The system provider will make a strong argument that equipment capabilities perfectly match or exceed what the end-user wants.
- A hardware or equipment list that names certain products desired by the end-user.

The end-user clarifies the specifications with the use of a facility walk-through that allows the bidders to see where the system will be installed. Typically, the end-user will show where equipment is to be placed, for example: a console at a security control center, card readers on certain doors, motion detection sensors on a perimeter fence, or CCTV cameras on the top of a building.

If the system to be purchased is complex, a walk-through may not answer all of the bidders' questions. Further clarification can be made by the functional requirements document, which says in plain language what the system should do and how. A bidder can use the functional requirements document to develop a proposal that in part will use plain language to describe how the features of the proposed system will perform the needed functions.

There can be only one basis for testing the operation of a purchased and installed system. That basis is the written information given by the end-user to the system provider. If a system fails to meet a specification, the system provider is at fault; if a system fails to perform a function that is required but not stated in a specification, the end-user is at fault. An installed system is most likely to perform to the satisfaction of the end-user when the end-user has provided detailed, clear specifications.

Acceptance Testing Phases

Four phases of acceptance testing, plus ongoing operational testing, are recommended for a large multi-site physical security system. The tests are described as follows.

Factory Acceptance Test (FAT). A FAT is not necessarily conducted where system components are manufactured. It can be done at an assembly facility or even at the end-user's facility. For this test, all of the major system components are assembled in one place. Although the final, installed system may extend to widely dispersed sites, the FAT will test the system in one manageable area. Using simulations, the test can evaluate the system's network, redundancy, backup/restore, and other functions. The purpose of the FAT is to ensure that the system works to the satisfaction of the provider and the end-user.

Some system providers will try to avoid the FAT because they believe it to be costly, time consuming, and unnecessary. Others will view the FAT as an opportunity to demonstrate system quality and efficiency. These system providers usually know their products well and have high confidence that the FAT will work to their advantage.

The FAT can be important to an end-user because it is the last chance to gain assurance about the critical elements of a system before installation work begins. Depending on contract specifications, the end-user can demand that any glitch, small or large, must be corrected by the system provider before the system can be said to have passed the FAT. A failure to correct a glitch in a pre-agreed time frame can be sufficient justification for the end-user to cancel the contract (a very rare occurrence).

As systems become more and more complex, the FAT becomes more and more important. However, given today's level of technological sophistication, there is little reason for a system to fail a FAT if the system provider performs the appropriate preparations and test setup.

Site Acceptance Test (SAT). The SAT is performed in the "field" and for that reason is sometimes called a field acceptance test. A SAT is used to test system components that are located apart from the main system. A single system can have multiple SATs. It is not uncommon for a SAT to be conducted on an ad hoc basis. The result will be dissatisfaction when an unscheduled SAT reveals problems that could have been avoided by prior planning.

System-Wide Acceptance Test (SWAT). The SWAT is performed after sub-systems at all

sites are up and running. It consists of end-to-end testing under normal and emergency conditions. The central monitoring function is tested when all of the sub-systems are fully operational. In addition to scenario-based testing, the system is also subjected to maximum usage and worst-case conditions. This is extremely important for networked systems, especially security video systems. The network infrastructure must be managed to maintain the availability of the network bandwidth (amount of data the network can transmit) that is required by the security system for its highest anticipated network load even though day-today operations may only require a small portion of the larger network capacity. Where service companies provide a portion of the network infrastructure, benchmarking network requirements during the SWAT provides important input for network Service Level Agreement (SLA) requirements.

Operational Acceptance Test (OAT). This test, sometimes called a field reliability test, usually consists of inspections made of the system in operation over a 30-day period. The purpose of the OAT is to ensure that the system can operate reliably for an extended period of time. Performance exercises are included if normal operations are not expected to sufficiently challenge the system. The OAT can include SATs when other sites are part of the system.

Because the OAT is lengthy compared to other tests and uses a variety of testing techniques, it is fair to call it a test phase.

Ongoing System Operational Test (OSOT). This testing, like some others, has an alternate name; it is sometimes called ongoing maintenance testing. The OSOT is not a single specific test; it is testing performed periodically throughout the life of the system. Ideally, ongoing testing will also test system operators, such as security officers, and the plans and procedures that guide the operators.

The frequency of the periodic testing varies significantly from one facility to another. The cause of schedule variation can be a built-in system requirement, customer or regulatory requirements, or even factors related to a maintenance schedule. Frequency can also be related to the preference of management.

Testing Techniques

All of the previously described tests can be conducted using various techniques, the names of which indicate how the tests are conducted.

- Functionality Testing
- Security Scenario Testing
- Performance Testing
- Stress Testing
- Load and Capacity Testing
- Fault Tolerance Testing
- End-to-End System Testing

Physical security system testing is never simple and easy to do. When done properly, the payoff can be substantial such as savings that result from preventing security-related losses, productivity increases that result from facilitating the movement of people, vehicles, and property, cost reductions that result from automatically turning off lights and the HVAC system when they are not needed, and lastly, money saved by reducing the operating costs of the physical security system.

Ray Bernard and Don Sturgis

ACCESS CONTROL: PEOPLE, VEHICLES, AND MATERIALS

Access controls regulate the flow of people, vehicles, and materials into, out of, and within a protected facility. They apply to many categories of people: employees, visitors, contractors, vendors, service representatives, etc. Access controls apply to vehicles, such as employee automobiles entering and leaving parking lots, and trucks moving to and from shipping and delivery platforms.

Access controls can be applied to materials, such as raw goods moving to the production line and finished goods moving to the shipping department or warehouse. Although access controls are most often in place as a means for protecting assets (which include the people being regulated), they play an important part in facilitating movement in a manner that meets the operating needs of the protected facility.

People Control

Employees. The basic tool for controlling the movement of employees is an identification

card. The use of an employee identification card depends on the number of employees and the sensitivity of the protected facility. A workplace with a few employees in a low security situation will not require an access control system or one that is elaborate in any meaningful respect. A location containing many employees will have difficulty operating without some form of access control. This will be especially true when there is a need also to control access to restricted areas within the protected facility. Large or small, simple or sophisticated, for the system to operate efficiently, it must be clearly understood by those affected by it and be supported by management.

Visitors. A variety of techniques are applicable to visitor access control; for example, a visitors lounge, appointments made in advance and registered with a receptionist, personal vouching by employees, positive identification of the visitor, search of items carried into the premises by the visitor, screening by metal detector, escort while on the premises, and temporary badges that self-destruct.

Relevant information collected at the time of issuing the badge would be the name of the visitor, date of visit, time entering and leaving, purpose, specific location visited, name of sponsoring/escorting employee, and temporary badge number. In a safety-sensitive environment, visitors may be required to be briefed and to wear special protective equipment, such as a helmet, safety glasses, robe, or steel-reinforced footwear. A record or log of visits is wise. In some situations, contact between employees and visitors should be discouraged; for example, on the loading dock where larcenous conspiracies may evolve between truck drivers and employees of the shipping and receiving departments.

Electronic Access. Systems for controlling access by use of electronic technology are appropriate in highly populated working environments and where asset protection is essential. The typical approach is to issue to each authorized person a sturdy key card that contains coded information capable of being read by electronic devices placed at the entry/exit points.

Three traditional types of key cards are the magnetically encoded card, the magnetic pulsing card, and the proximity card. The first has small magnets within the card. When the card is brought into contact with a reader device at the entry point door, the card's magnetically encoded data are transmitted to a computer processor. If the card's data corresponds to the access requirements, entry is granted; if not, entry is denied. Magnetic pulsing works in a fashion similar to the magnetically encoded card. Magnets and wires encased in the card emit positive and negative pulses that are sensed by the reader device at the entry point.

The proximity card contains circuits tuned to a radio frequency emitted by the reader at the point of entry. When the card is brought within the detection range of the radio frequency, the reader will sense the unique characteristics of the card and transmit these data to the computer. If the data meet the entry criteria, the lock mechanism at the entry point disengages. This type of key card is called a proximity card because it does not have to be brought into physical contact with a reader, such as by inserting or swiping, but by placing it in the proximity of the reader.

Then there are the biometric access control systems. They offer a variety of personal identification principles based on fingerprints, signature recognition, voice characteristics, retinal patterns, and hand geometry. Also available are applications that incorporate in a single system two or more biometric principles such as fingerprint, facial, and iris recognition.

Among the biometric choices, fingerprint systems are widely used. They work well and are relatively inexpensive to purchase and install. Also new in the marketplace are access control systems that use radio frequency identification (RFID) and so-called "spoof protection" that can trigger automatic responses to suspected intrusion attempts. To guard against compromise, the system itself can be protected with encrypting software.

Access control systems are used in many facilities such as airports, offices, computer centers, factories, special weapons depots, warehouses, jails, prisons, police stations, courthouses, Federal buildings, U.S. intelligence offices, border crossing points, and military installations. Many locations that are separated by great distances can be protected by a single system.

However, systems that record time and attendance are not control-oriented. The principal users are human resources and payroll departments.

In this category also are systems devoted to investigation. They are linked to closed circuit television systems that can help the user spot crimes in progress, identify the culprits, and visually demonstrate vulnerabilities that need to be eliminated. Forgery can be detected and the forger apprehended with a combination of signature recognition and a live-sensing and communicating capability.

Traffic Control

In comparison to people control, traffic control can be relatively simple yet extremely frustrating. This is because automobiles can, for some individuals, be an emotional issue. Where employees park and how they park, although uncomplicated, can be difficult to manage.

Traffic control at a protected facility can begin at points outside of the property line. Whether the control is administered by local police officers or security officers who have been deputized for the limited purposes of traffic control, the essential point is that some degree of influence can be brought to bear on vehicles before they cross the property line or enter the facility. Once inside the facility, control of vehicles can be enhanced through pre-designed roadway features such as gates, jersey barriers, median dividers, one-way travel, signage, traffic signals, and bollards. Uniformed security officers at traffic control points can be an added feature.

Multiple entrances, especially to restricted areas, can require multiple security officers. Management may decide that during times of high vehicle traffic, typically the morning and evening rush hours, normally closed entry/exit points at non-restricted areas can be opened without having an officer present at every one. Electrically operated gate arms can be set to automatically open during rush hours without presentation of access cards, and to operate in the normal mode during other hours.

From the standpoint of theft prevention, traffic control around the facility's loading dock is important. To ensure that the vehicles and drivers in the loading dock are there on legitimate business, the access control system may feature closed-circuit television (CCTV) cameras to monitor activity; a loading dock door that can be operated remotely from an interior location, such as the security center; an intercom for drivers to obtain notice of arrival and opening of the loading dock door; and the presence of a security officer to monitor and/or inspect departing cargo.

Traffic control may also involve control of vehicles moving within the protected facility. An out-of-doors holding area for cargo received at a seaport may, for example, have trucks and heavy loading and stacking machinery moving simultaneously throughout a relatively large and congested area. Control in this situation can be directed at both theft prevention and accident prevention.

Materials Control

An access control system can be engineered to regulate free movement and tracking of materials such as the mail, supplies and raw goods that feed the business, unfinished products being created within, and finished goods leaving. Included in this capability are the tools used by the business such as computers, manufacturing equipment, and vehicles.

Three physical security features have been found to be successful: metal-detectors at entrances, RFID or similar technologies that monitor materials moving inside the facility, and controlled barriers at exits.

Inspection of Entering Packages. This method of access control is intended to prevent introduction to the premises of dangerous or undesirable items such as bombs and handguns. Packages are inspected visually and with devices such as metal detectors and x-ray machines. The inspection point is usually a gate outside the blast zone (that area in which property and life are at risk from an explosion). Packages can be briefcases, purses, backpacks, mail bags, and courier-delivered containers.

Inspection is usually made by security officers that have been trained in how to use detection equipment, spot the visual indicators of bombs and chemical/biological agents, evacuate people, and notify first-responders. Ideally, the place of inspection will be isolated and if indoors will be entirely enclosed and have its own air conditioning system. Inspection will be focused on detecting mass destruction weapons and may include attention to other undesirable items such as illegal drugs and alcohol.

Accounting for Property Removed. In this method, the employer is attempting to exercise control of company-owned property leaving the protected facility. The arrangement usually involves cooperation between supervisory personnel and the security officer force. Supervisors authorize subordinates to remove company property from the premises for a business-related purpose, such as taking a personal computer home to work on a word processing project, and security officers inspect departing property to insure that removal authority has been given. Typically, a property removal pass, signed by the supervisor, describes the property to be removed; the supervisor keeps a copy of the pass; the employee presents the original and a copy of the pass to the security officer at the exit point; the security officer compares the pass against the property, retains the copy of the pass, and allows the employee to proceed; and the security department holds its copy of the pass as a record of property having left the premises. When the employee returns the property, the supervisor signs and files the original copy held by the employee.

Inspection of Departing Vehicles. This method is also intended to control removal of company property. In some industries, removal of property is based on safety considerations such as in the chemicals industry where the taking of a toxic chemical would constitute a hazard to public safety. Whatever the industry and whatever the reason for making inspections, management will have observed certain necessary prerequisites: ensuring that the inspection program will not violate laws, contracts, or agreements with a bargaining unit or the employees; ensuring that the employees, visitors, or others affected by the inspection program have been informed; and training the security officers to conduct the inspections in a manner that will not violate constitutional protections and reasonable standards of fairness and privacy.

Management may decide that inspection need not be made of all departing vehicles but at an inspection rate high enough to discourage attempts to leave the premises with restricted material. When this option is taken, the method for selecting the vehicles to be inspected is based on random selection. If the objective is to inspect 20 percent of departing vehicles, a random selecting device at the exit point will keep count and an enunciator, such as a horn, will let the security officer know that that the next vehicle should be inspected. A driver immediately behind a vehicle undergoing an inspection has no assurance that his vehicle will not be inspected.

John J. Fay

ALARM SYSTEM MANAGEMENT

Alarms are tools that make security incident response possible. Management of alarms is shared by the chief security officer (CSO) and the end user, i.e., the CSO's employer. A third player is the alarm consultant, a person with expertise in designing an alarm system, integrating it with other systems, and solving problems that arise.

The CSO is concerned with:

- Ensuring that the alarm system meets the security needs of the organization.
- Ensuring that the alarm system operates in harmony with other systems.
- Ensuring that the alarm system's components are of high quality, installed correctly, and perform as intended.
- Ensuring that the alarm system does not interfere with business operations.
- Ensuring that the costs to purchase and maintain the alarm remain within the boundaries of the budget.
- Ensuring that the alarm system is cost-effective, i.e., that the value of benefits derived from the system are at least equal to the costs of the system.

The Human Component

The effectiveness of an alarm system cannot exceed the competency of the persons that monitor and operate it. Included in the word "competency" is (1) knowing the purpose of the system and its functional arrangement; (2) knowing how to turn the system on and off and how to correct minor, anticipated glitches; and (3) knowing the meaning of alarm signals, i.e., differentiating between fire, intrusion, duress, and touching or tampering.

The enemy of competency is lack of knowledge. Too often, alarms are misinterpreted, resulting in a failure to initiate a response when response was essential or initiating a response inappropriate to the alarm-reported condition. Misinterpretation

can occur, for example, when the system operator thinks that a signal indicating an open door to a restricted area is the result of an employee propping the door open and for that reason ignores the signal, or when the system operator initiates a full-blown response when the signal was clearly the result of a nuisance such as a small animal tripping an intrusion sensor on the outer perimeter.

When a security program is in effect at a protected facility, the system operators are almost always security officers. This places a responsibility on the alarm system designer and/or installer to thoroughly teach the officers how to operate the system prior to final acceptance of it. The CSO's responsibility is to ensure that security officers are proficient in system operation prior to and following acceptance.

Alarm Points

Alarm point is a misnomer because an alarm is the result of a sensor activating. For example, a smoke detector will activate when it detects smoke indicative of fire. Activation of the detector sends a signal. The signal is the alarm and the signal is manifested in a way that can be registered by humans. The ululating sound of a siren is registered in the human consciousness as a message that says fire is nearby. A flashing red light on a console tells the alarm system controller that an intrusion has occurred or that something which should not be touched has been touched.

Alarm points are essentially substitutes for security officers. If a certain place requires protection, such as a door that provides access to valuable property, the CSO can either place a guard at the door or install an alarm point at the door. The less expensive of the two options is the alarm point. Qualitative differences are arguable.

The selection of an alarm point is influenced by:

- Normal operations of the protected organization, i.e., an alarm should not interfere with the orderly conduct of work.
- A protection need, e.g., a critical asset that needs to be protected against theft, damage, or destruction.
- A detection need, e.g., a place that presents an opportunity for unauthorized entry.
- A safety need, e.g., fire sprinklers in a high-rise office building.

An alarm point is often an element of a physical safeguard or countermeasure. A fence is a physical safeguard. A vibration sensor mounted on a fence is an alarm point. Alarm points can be coded to facilitate human understanding, and the codes can be associated with zones. For example, the northeast section of an out-of-doors storage area has three alarm points. The codes for the alarm points are NE-1, NE-2, and NE-3. A map viewable to the alarm system operator depicts the precise locations of the alarm points. In another example, a protected building has alarm points on doors, windows, and interior rooms. The code for the main entrance door is D-1, the rear door D-2, etc. A window on the 2nd floor is 2W-1 and a room on the 3rd floor 3R-1. Using codes in lieu of geographic descriptions helps the system operator communicate quickly and accurately when dispatching a response unit and the response unit is aided in figuring out which asset may be in jeopardy.

Further, in the case of intrusion, an alarm point activated at a particular spot on a fence line, followed by an alarm point activated at a particular spot inside the fence line, followed by an alarm point activated at the entry point to a particular building can possibly reveal to the alarm system operator the path of the intruder and the speed at which the intruder is moving.

The locations of alarm points correspond to the organization's overall security plan. They do not determine the design of the plan; the opposite is true. From the point of view that the vulnerability assessment process determines the security plan, the security plan incorporates countermeasures that offset vulnerabilities. In turn, countermeasures incorporate alarms.

Alarm Communication and Display

The heading of this section means exactly what it says: an alarm is communicated and it is displayed. Communication begins when a sensor activates, it moves to a computer that assesses the activation, and communication ends when the assessment reaches the monitoring station such as a security control center. Display is the presentation of information to the alarm system operator in a meaningful format.

A meaningful format could be a red light on a panel board, with red meaning that a sensor has activated; a yellow light meaning that

a certain sensor is in the off mode; and green meaning that the sensor is active and stable. The positioning of lights on the panel and/or adjacent labels can indicate the type of alarm and its location.

The format, whatever it may be, has to tell the operator: (1) the nature of the alarm, (2) the place where the alarm went off, and (3) when the alarm happened.

Communication from the sensor to the monitoring station moves through a wire or fiber-optic cable. (A wireless connection may be acceptable in a low-security situation. When wireless technology reaches a level of reliability equal to hard wires, it will be suitable for high-security situations. When that point is reached, hard wires will go the way of the dinosaur.)

An alarm system is worthless if the wire or cable is severed. It does not matter if the break is accidental or intentional, the effect is the same. To guard against a break, the wire or cable needs to run inside a conduit and, if possible, the conduit should be buried. Because sensors tend to be added later, it makes sense to place extra wires and cables inside the conduit when the system is initially installed.

A function called line supervision monitors the link between the sensor and the monitoring station. A break in the link or an indication of tampering sends a warning signal to the system operator. Supervision can be static or dynamic. In static supervision, a secure condition is represented when a supervising signal remains constant. In dynamic supervision, a secure condition is represented when the supervising signal is continually changing.

Assessment

A secure communicating method is essential, so also are qualitative characteristics of the information being transported. These include:

- Quantity of data.
- Reliability that the data will reach the assessing computer intact and uncontaminated.
- Speed at which the data moves.

The assessing computer analyzes the alarm data and sends to the monitoring station the appropriate message, which could be a report of fire in the southwest quadrant of the 16th floor or interruption of a photoelectric beam in Room 304 or the pressing of a duress button in the executive suite. The assessing computer can send messages to display devices in multiple locations within the protected facility and to outside locations such as the fire department, police department, or medical emergency agency.

The Alarm History File

A step in managing an alarm system is to set up and maintain a file that records the history of alarm initiations. The file is maintained by the CSO or a person responsible to the CSO. The file is organized so that each alarm has an individual record. A record will reflect:

- When the alarm went off.
- The sensor that triggered the alarm.
- The cause of the alarm.
- Actions taken in response to the alarm.
- The name of the system operator when the alarm went off.

The CSO's examination of the file might reveal:

- Alarms and/or sensors that are in need of calibration, repair, or replacement.
- Malfunctioning ancillary equipment such as a lock that will not fully engage.
- Alarms and/or sensors that do not operate well due to environmental conditions such as extreme temperatures, rain, heavy winds, and ground vibrations.
- A frequency of enunciation indicating that an alarm is asynchronous to the security program; for example, a receiving dock door that is in the active alarm mode when the dock is in use.
- A correlation between alarm frequency and the identity of the person operating the alarm system at that time.
- A correlation between alarm frequency and a security operation; for example, an alarm that activates whenever a roving patrol passes nearby.
- A discrepancy between the criticality of the alarm and the nature of the response.
- A discrepancy between the performance of an alarm and the alarm manufacturer's

and/or the alarm system designer's representations.
- Poor alarm performance at highly critical locations.

The alarm history file can include multiple forms of documentation such as security department incident reports, complaint reports from end-user employees, and computer printouts generated whenever an alarm is activated.

John J. Fay

Source Garcia, M. 2001. *The Design and Evaluation of Physical Protection Systems*. Boston: Butterworth-Heinemann.

BURIED LINE SENSORS

Buried line sensors protect an area along the ground just above the sensor transducer cable or sensors by detecting anyone crossing the protected zone. Someone who crosses the sensitive area induces both seismic energy and exerts pressure in the ground. Buried sensors are available that detect strain and seismic energy. Another type of buried line sensor is available that detects the presence of ferrous metals being carried or worn by the person crossing the transducer cable, as well as detecting local induced pressure.

Piezoelectric transducers are used primarily to detect short-range pressure disturbances in the ground, and geophones are primarily used to detect longer-range seismic waves. These are basically the same devices used for the fence disturbance sensor transducers, and in some cases they are the same device.

Geophone Transducers

Buried geophones detect the low-frequency seismic energy induced in the ground by someone crossing the protected area above the sensors, and convert this energy into electrical signals. The electrical signals correspond to the frequency of the induced seismic energy, and they are proportional in amplitude to the magnitude of the energy. These induced signals are sent to the signal processor, where they are filtered before entering the signal processor. The band-pass of the filter corresponds to the seismic energies with frequencies or signatures typical of someone crossing the geophone sensors. When the characteristics of the induced signals satisfy the processor alarm criteria, an alarm is initiated.

A geophone consists of a movable spring-balanced coil of fine wire suspended around a permanent magnet. The coil of fine wire is cylindrical to slide over the magnetic rod fixed to the geophone housing. When the geophone is acted upon by the seismic energy, the permanent magnet vibrates with the geophone housing at the frequency of the induced energy. The vibrating magnet moves in line with the coil of fine wire, which tends to stay near rest. It stays near rest because the fine spring holding the wire coil in suspension around the magnet offers very little resistance to the moving geophone housing. As the magnet vibrates in the coil, the magnetic lines of force associated with the permanent magnet induce an electromotive force (emf) in the coil. This emf, or electrical signal, is the signal that is monitored by the signal processor.

Geophones are very sensitive to detecting even low-level seismic energies generated by moving objects anchored in the ground such as trees, fences, light poles, or telephone poles. When these objects are subjected to wind loads, the overturning forces are absorbed by the ground. As the winds vary, the objects move, inducing seismic energy in the ground. To help reduce the need for the signal processor to differentiate between these energies and valid intrusion signals, the geophones should be installed a reasonable distance from this type of object. A reasonable distance is difficult to define because of all the varying parameters in any given installation. However, the following minimum distances can be used as guides: about 30 feet from tree-drip line, 10 feet from fences, and a distance about equal to the height of the light pole or telephone pole away from the pole.

Piezoelectric Transducers

Piezoelectric transducers detect the stresses or pressure induced in the ground by anyone crossing the protected area above the sensor line. The transducer consists of a quartz crystal that is secured to the transducer case such that when an external pressure is applied to the transducer the crystal generates a voltage. In operation, when someone steps on the ground

above the transducer, the pressure from the person's weight stresses the piezoelectric crystal. The stressed crystal generates an electrical signal that is proportional to the applied pressure. When the characteristics of the signal satisfy the processor alarm criteria, an alarm is initiated.

Strain/Magnetic Line Sensors

The combined strain and magnetic line sensors detect both the pressure or strain induced in the ground by someone crossing the sensor line and the presence of ferrous material carried or worn by the person crossing. The sensor consists of a passive transducer cable and an alarm electronics module. The passive transducer cable uses a magnetic material wound with a pair of sense coil windings. This assembly is wrapped with a stainless steel jacket and covered with an outer plastic jacket. The two sense windings are wound on the magnetic core and connected together in a manner to cancel far-field seismic and magnetic disturbances.

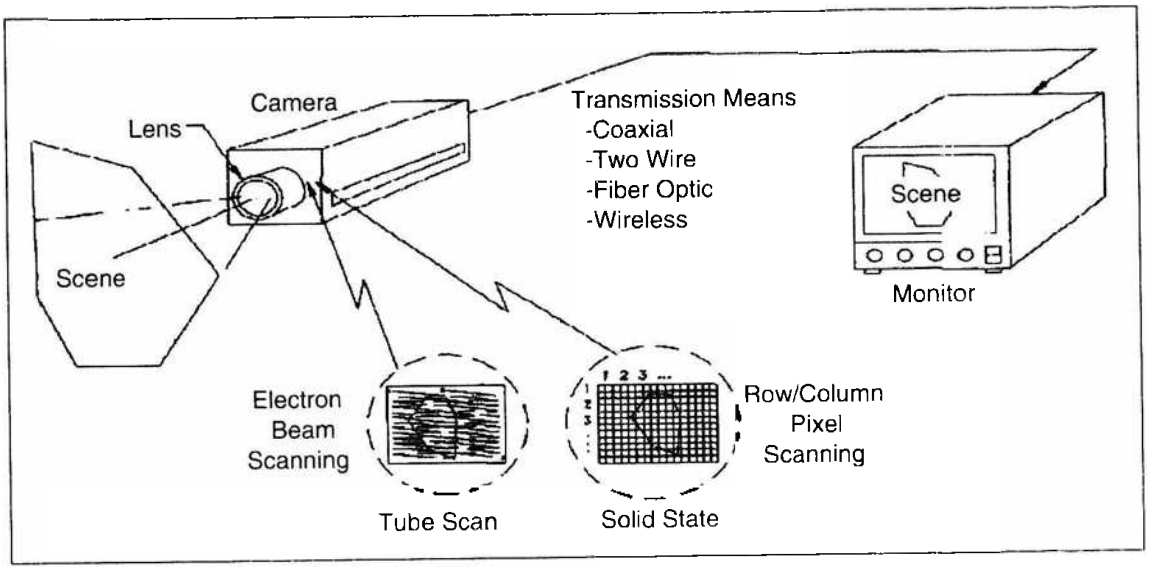
In operation, the residual flux density of the ferromagnetic core material and the flux density of the earth's magnetic field remain constant during normal circumstances. The weight of anyone crossing the sensitive area above the transducer cable stresses the ferromagnetic core material. The induced stress alters the magnetic flux that generates a voltage in the sense winding overlay around the coil. A voltage is also induced in the sense winding when someone crosses the transducer cable carrying or wearing ferrous material. In this case, the ferrous materials distort the earth's magnetic field. The changing magnetic field alters the coil magnetic flux density, generating a voltage in the sense winding. Signals resulting from either the mechanical stresses or from the presence of ferrous materials, or these combined signals, are processed and analyzed by the signal processor in the alarm electronics module. Before the signal is analyzed and when their characteristics satisfy the established alarm criteria, an alarm is initiated. The purpose of the dual-channel signal processing is to reduce false alarms from wind and electrical interference.

Robert L. Barnard

Source Barnard, R. 1988. *Intrusion Detection Systems, 2nd Edition.* Boston: Butterworth-Heinemann.

CCTV: CAMERAS FOR SECURITY

The closed-circuit television (CCTV) camera's function is to convert the focused visual (or infrared) light image from the camera lens into a time-varying electrical video signal that contains the intelligence in the scene image. The lens



CCTV System with Lens, Camera, Transmission Means, and Monitor

Figure 16. This diagram shows how scene images are captured, processed, and sent to a monitoring station.

collects the reflected light from the scene and focuses it onto the camera image sensor. The camera processes the information from the sensor and sends it to a viewing monitor via coaxial cable or other transmission means.

There are two generic types of CCTV sensors: (1) tube and (2) solid-state. The solid-state type represents the majority of existing security installations. The tube cameras use electron beam scanning techniques while the solid-state cameras use the charge coupled device (CCD) or the complementary metal-oxide device (CMOS) sensor.

Camera Scanning Function

The monochrome or color television camera in the security CCTV system analyzes the scene by scanning it in a series of closely spaced lines in the case of a tube camera, or picture elements (pixels) in the case of a solid-state camera. This technique generates the codes and electrical signal as a function of time so that the scene can later be reconstructed on the monitor.

Unlike film cameras or the human eye, or low-light-level television image intensifiers that see a complete picture one frame at a time, a television camera sees an image point by point until it scans the entire scene. In this respect the television scan is similar to the action of a typewriter where the type element starts at the upper left-hand corner of the page, moves across the page to the right-hand corner, and in this way a single line of type is completed. The typewriter carriage then returns to the left-hand side of the paper, moves down to the third line (skips a line), and starts over again. At the left-hand side the typewriter carriage again moves from the left to the right, typing out another line, then returns and moves down again, with this action continuing until the typewriter has reached the bottom of the page. This completes one field or half the television picture. If the page is then moved back so that the typewriter begins typing on the second line at the left just below the first line and the same action continues again, moving down two lines at a time, each line in-between the originally typed lines is filled in, and by the time the typewriter gets to the bottom of the page, the full page is completely typed. This completes two fields and is equivalent to one full video frame.

Scanning is accomplished in the tube camera, through the use of magnetic or electrostatic deflection of an electron beam whereas in the solid-state camera electrical clocking circuits are used to scan the sensor pixel array.

The television camera consists of: (1) an image sensor, (2) some form of electrical scanning system with synchronization, (3) timing electronics, (4) video amplifying and processing electronics, and (5) video signal synchronizing and combining electronics to produce a composite video output signal. The camera has synchronizing signals so that a monitor, a recorder, a printer, or other CCTV routing or processing equipment can be synchronized to produce a stable display or recording.

In operation, the lens forms a focused image on the camera sensor. In the tube camera the television picture is formed by extracting the light information on the target area as the electron beam moves across the light-sensitive area of the tube in a process called linear (or raster) scanning. The entire picture is called a frame and is composed of two fields. Each frame contains 525 horizontal lines in the U.S. National Television System Committee (NTSC) system based on the 60-Hz power line frequency and duration of 1/30 second per frame (30 frames/second). The European system, based on a 50-Hz power line frequency, has 625 horizontal lines and 1/25 second per frame. In the NTSC system the electron beam scans the picture area twice, with each scan producing a field. Each field contains 262-1/2 television lines with the two fields producing a complete frame having 525 television lines total. A 2:1 interlaced scanning technique is used to reduce the amount of flicker in the picture and improve motion display. This scanning mode is called two-field, odd-line scanning.

For the solid-state camera, in place of the moving electron beam in the tube, the light-induced charge in the individual sites—picture elements (pixels)—in the sensor are clocked out of the sensor into the camera electronics. The time-varying video signal from the individual pixels clocked out in the horizontal rows and vertical columns generate the two interlaced fields.

Sensor Types

The most popular tube type sensor used for many years was the vidicon. Now the most popular

type cameras use solid-state type sensors: charge transfer devices (CTD), charge coupled device (CCD) and complementary metal-oxide semiconductor (CMOS), and charge injection device (CID) solid-state types. The most widely used are the CCD and the CMOS.

In LLL applications these tube and solid-state sensors are combined with image intensifiers to produce the silicon intensified target (SIT), intensified SIT (ISIT), and intensified CCD (ICCD) cameras. The most commonly used is the ICCD.

Solid-State Cameras

The solid-state camera uses a silicon array of photo-sensor sites (pixels) to convert the input light image into an electronic video signal, which is then amplified and passed on to a monitor for display.

Most solid-state sensors fall into the category of devices called charge transfer devices (CTD), which can be subdivided into three groups depending on the manufacturing technology used: (1) charge coupled device (CCD), (2) complementary metal-oxide semiconductor (CMOS), (3) charge priming device (CPD), and (4) charge injection device (CID). By far the most popular devices used in security camera applications are the CCD and CMOS. The CID is reserved primarily for military and industrial applications. The solid-state imaging devices used in security CCTV applications are small, light weight, rugged, and consume low power.

Solid-State Sensor

The solid-state sensor CCTV camera performs a function similar to that of the tube camera, but the sensor and scanning system is significantly different. It has no electron beam scanning of the visual image on the sensor area, and an area array of pixels replaces the camera tube. The typical sensor has hundreds of pixels in the horizontal and vertical directions equivalent to several hundred thousand pixels over the sensor area. A pixel is the smallest sensing element located on the sensor that converts the light energy into an electrical charge and signal.

Scanning and Timing. The CCD imager works by a process called charge coupling. It is the collective transfer of the electrical charges produced by the image stored in the CCD storage element (pixel) and moved to an adjacent storage element by the use of external synchronizing or clocking voltages that, in effect, push out the signal, line by line, at a precisely determined clocked time and produce the video signal. The signal represents the light intensity at each pixel location, which is the intelligence in the picture.

Typical device parameters for a CCD available in the market today are 488 by 380 pixels (horizontal × vertical) in formats of 1/4-, and 1/3-inch, in a 4 × 3 (H × V) aspect-ratio television presentation.

The CMOS-type sensor exhibits high picture quality but has a lower sensitivity than the CCD. In the CMOS device the electric signals are read out directly through an array of MOS transistor switches, rather than line by line as in the CCD sensor.

The CID device differs from all other solid-state devices in that any of the pixels can be addressed or scanned in a random scan sequence rather than in the row/column sequence used in the other sensors. The advantage of this capability has not been realized in the security field but is used in industrial and military applications where non-raster scan sequences or patterns offer advantages.

Most CCD image sensors have wide spectral ranges and are usually useful over the entire visible range and into the near infrared (IR) spectral region above 800 to 900 nanometers.

One of the significant advantages of charge coupled image sensors over vacuum tube sensors is the precise geometric location of the pixels with respect to one another. In a camera tube the video is "read" from a photosensitive material by a scanning electron beam.

The position of the beam is never precisely known because of some uncertainty in the sweep circuits resulting from random electrical noise, variations in power supply voltage, or other variations.

CCTV Resolution

CCTV resolution is a critical measure of the television picture quality; the higher the resolution, the higher the level of information.

CCTV resolution is measured by the number of horizontal and vertical television lines that can be discerned in the monitor picture.

The U.S. NTSC standard provides a full video frame composed of 525 lines, with 504 lines for the image, and a vertical blanking interval composed of the remaining 21 retrace lines. The television industry has adopted the practice of specifying horizontal resolution in television lines per picture height. The horizontal resolution on the monitor tube depends on how fast the electron beam can change its intensity as it traces the image on a horizontal line.

With the 525-line NTSC system, the maximum vertical resolution achievable in any CCTV system is approximately 353 television lines. The 625-line system can produce a maximum vertical resolution of 438 television lines. While the vertical resolution is determined solely by the number of lines chosen (U.S. standard 525 lines), the horizontal resolution is dependent upon the electrical performance bandwidth of the individual camera, transmission, and monitor system.

Most standard cameras with a 4.5-MHz bandwidth produce a horizontal resolution of 550 television lines. The traditional method of testing and presenting CCTV resolution test results is to use the Electronic Industry Association (EIA) resolution target.

One comparison made between the solid-state and tube camera is resolution, i.e., how much detail is seen in the picture. The resolution for a good tube security camera is 500 to 600 television lines. Solid-state data sheets often quote the number of picture elements (pixels) instead of television lines of resolution. However, unless the number of horizontal pixels is converted into equivalent television lines, the horizontal resolution is not known.

To approximate the horizontal resolution from the horizontal pixel count, multiply the number of horizontal pixels by 0.75. Only recently have solid-state sensors been available that can match the resolution of average tube cameras.

Low-Light-Level Sensors

LLL cameras such as the SIT, ISIT, and ICCD share many of the characteristics of the tube and solid-state types described previously but include means to respond to much smaller light levels found in scenes illuminated by natural moonlight, starlight, or some other very LLL artificial illumination. These cameras use image intensifiers coupled to imaging tubes or solid-state sensors, and can amplify the available light up to 50,000 times and view scenes hundreds to thousands of feet from the camera under nighttime conditions. Complete SIT tube and ICCD camera systems have sufficient sensitivity and automatic light compensation to be used in surveillance applications from full sunlight to overcast moonlight conditions.

The ICCD camera is a new LLL camera class whose sensitivity approaches that of the best SIT cameras and eliminates the blurring characteristics of the SIT under very LLL conditions. The ICCD camera combines a tube or micro-channel plate (MCP) intensifier with a CCD image sensor to provide a sensitivity similar to that of an SIT camera.

For dawn and dusk outdoor illumination, the best CCD cameras can barely produce a usable video signal. SIT and ICCD cameras can operate under the light of one-fourth moon with one 0.001 foot candle (FtCd) of illumination. The ISIT camera can produce an image from only 0.0001 FtCd, which is the light available from stars on a moonless night. SIT, ISIT, and ICCD offer a 100 to 1,000 times improvement in sensitivity over the best CCD cameras because these cameras intensify light whereas the tube and CCD cameras only detect it. By contrast, the best CCD camera has a minimum sensitivity of 0.00093 FtCd.

Format Sizes

There are four existing image format sizes for solid-state and tube sensors. These are 1/4-, 1/3-, 1/2-, and 2/3-inch. All sensor formats have a horizontal × vertical geometry of 4 × 3 (H × V) aspect ratio as defined in the EIA and NTSC standards. For a given lens, the 1/4-inch format sensor sees the smallest scene image (smallest angular field of view) and the 2/3-inch sees the largest. The 1/4- and 1/3-inch solid-state formats are presently the most popular, with the direction going toward the smaller sensors. The SIT tube cameras using the 1-inch tube to provide LLL capabilities are likewise being replaced by their solid-state counterpart, the ICCD.

Color Cameras

Solid-state color cameras developed for the consumer video cassette recorder (VCR) and camcorder use a single solid-state sensor with an integral three-color filter and automatic white balancing circuits. These sensors incorporated into a CCTV camera provide a stable, long-life color camera with good sensitivity suitable for indoor and outdoor security application.

There are presently two techniques to produce the color video signal from the image sensor produced by the color visual image from the lens: (1) single sensor and (2) triple sensor with prism. Most color cameras used in the security industry are of the single sensor type. The single sensor camera has a complex color imaging sensor with three integral optical filters on the image sensor to produce the three primary colors—red, green, and blue (R, G, B). These colors are sufficient to reproduce all the colors in the visible spectrum.

Solid-state CCD and MOS color cameras are available in 1/3-, 1/2-, and 2/3-inch formats. Most of those used in security applications have single-chip sensors with three-color stripe filters integral with the image sensor. Typical color sensitivities for these cameras range from 0.7 to 1.4 FtCd (7 to 15 lux) for full video, which is less sensitive than their monochrome counterpart. The resolution of most color cameras ranges from 350 to 410 television lines.

Cameras with higher resolutions of 420 to 470 television lines are available for use with the higher resolution digital video recorders (DVR), S-VHS, and Hi-8 (8-millimeter) recorders. Color cameras with a 1/2-inch format producing 250 to 350 television line resolution require an array with 780 (H) × 490 (V) (380,000 pixels).

Most color cameras incorporate automatic white balance compensation as an integral part of the camera so that when the camera is initially turned on, it properly balances its color circuits to a white background as determined by the type of light illuminating the scene. The camera constantly checks the white balance circuitry and makes any minor compensation for variations in the illumination color temperature (spectrum of colors in the scene it is viewing).

The availability of solid-state color cameras has made a significant impact on the security CCTV industry. Color cameras provide enhanced television surveillance because of the increased ability to identify objects and persons when using color rather than monochrome.

Lens Mounts

All security cameras have a lens mount in front of the sensor to mechanically couple whatever objective lens or optical system is used to image the scene onto the camera.

The two widely used lens mounts in the CCTV industry are the C and CS mounts. Until recently, all 1-, 2/3-, and 1/2-inch cameras used an industry standard mount to couple the lens to the camera called the C mount. This camera mount has a 1-inch diameter hole with 32 threads per inch (TPI). The lens has a matching thread (1-32 TPI) that screws into the camera thread. The distance between the lens rear mounting surface and the image sensor for the C mount is 0.69 inches (17.526 millimeters).

A second new mount adopted by the CCTV industry for 1/3- and 1/2-inch sensor format cameras is the CS mount, in which the camera has a 1-inch diameter hole with a 32 TPI thread (same as the C mount) and the lens has a matching thread. The distance between the lens rear-mounting surface and the image sensor for the CS mount is, however, 0.492 inches (12.5 millimeters), which is 5 millimeters (0.2 inches) shorter than for the C mount. This shorter distance means that the lens collecting light for the sensor is closer to the sensor by 5 millimeters and can be made smaller in diameter for an equivalent FOV.

A C mount lens can be used on a CS mount camera if a 5-millimeter spacer is interposed between the lens and the camera, and the lens format covers the camera format size. The advantage of the CS mount system is that the lens is smaller, lighter, and less expensive than its C mount counterpart.

Herman A. Kruegle

CCTV: COVERT TECHNIQUES

Overt closed-circuit television (CCTV) security equipment is installed in full view of the public, and is used to observe action in an area while simultaneously letting the public know that CCTV surveillance is occurring. This technique often has the effect of deterring crime. Covert CCTV is used so that the offender is not

aware he or she is under surveillance and to produce a permanent recording on a digital video recorder (DVR) or a video cassette recorder (VCR), for later use in confronting, dismissing, or prosecuting the person committing the offense. The covert camera and lens are out of view of anyone in the area under surveillance, and therefore unsuspecting violators are viewed on CCTV, their actions recorded, and often are apprehended while committing the illegal act. Although the camera uses small optics and is hidden, the result can be a high-quality CCTV picture of the area and activity.

An independent reason for using covert CCTV is to avoid changing the architectural aesthetics of a building or surrounding area. Covert CCTV cameras are concealed in common room objects or are located behind a small hole in an opaque barrier such as a wall or ceiling. Cameras are camouflaged in common objects such as lamps and lamp fixtures, table and wall clocks, radios, books, etc. A very effective covert system uses a camera and lens camouflaged in a ceiling-mounted sprinkler head.

A small-diameter front lens can view a scene through a 1/16-inch diameter hole. These lenses have a medium to wide field of view (FOV) from 12 to 78 degrees to cover a large scene area, but still permit identification of persons, and monitoring activities and actions. Other special pinhole lens variations include right angle, automatic iris, sprinkler head, and fiber optic, and small pinhole cameras combining a mini-lens and sensor into a small camera head and other complete miniature cameras.

In low-light-level (LLL) applications, a charge coupled device (CCD) camera with a very sensitive sensor and infrared (IR) light source or an image intensifier are used. Since many covert installations are temporary, wireless transmission systems are used to send the CCTV camera signal to the monitor, VCR, or video printer.

CCTV lens and camera concealment is accomplished by having the lens view through a small hole, a series of small holes, or from behind a semi-transparent window.

A number of suitable lens and camera locations include: (1) ceiling, (2) wall, (3) lamp

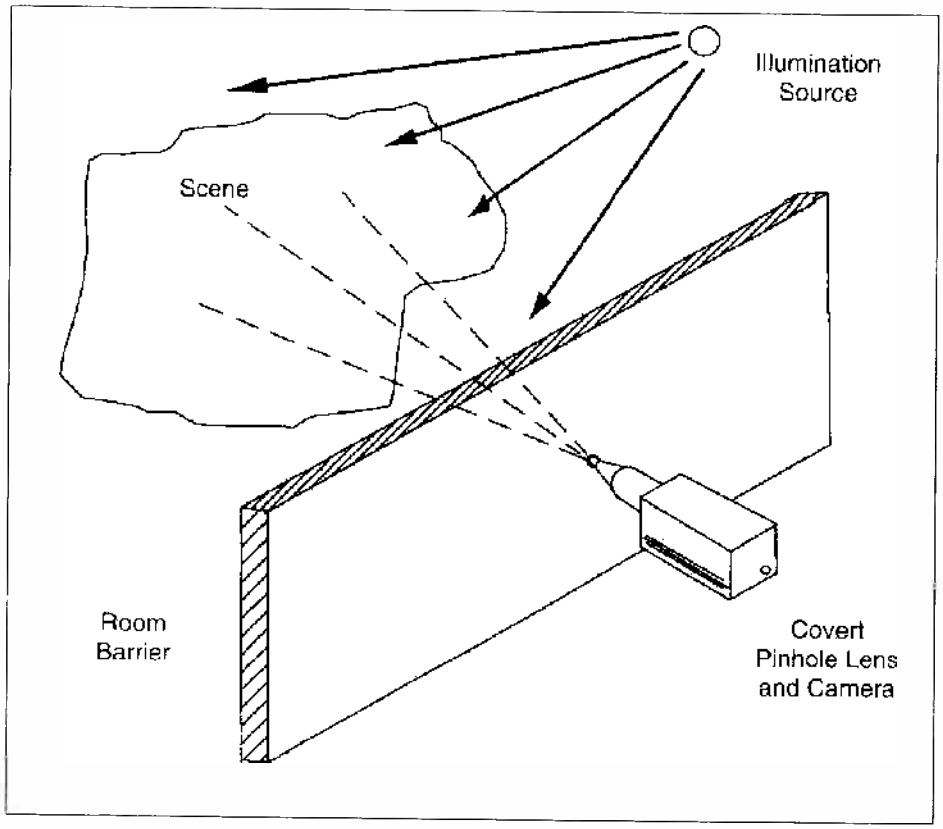


Figure 17. A CCTV camera hidden behind a wall can reveal and record suspicious activities.

fixture, (4) furniture, and (5) other articles normally found in a room. CCTV cameras are installed in one or more locations in the room, depending on the activity expected.

Since the diameter of the front lens viewing the scene must, by necessity, be small to hide it, these lenses are optically fast, and collect and transmit as much light as possible from the reflected scene to the television sensor. As a consequence, small-diameter lenses, referred to as pinhole lenses, are used. The term pinhole is a misnomer, as these lenses have a front diameter anywhere from 1/8 to 1/2 inch.

The lens/camera requirement is to receive reflected light from an illuminated scene, have the lens collect and transmit the light to the camera sensor, and then transmit the video signal to a video monitor and/or VCR and video printer.

The hole in the barrier is usually chosen to be the same diameter (d) or smaller than the pinhole lens-front lens element. When space permits, the straight-type installation is used. In confined or restricted locations with limited depth behind the barrier, the right-angle pinhole lens/camera is used. In both cases to obtain the full lens FOV, it is imperative that the pinhole lens-front lens element be located as close to the front of the barrier as possible to avoid "tunneling" (vignetting). When the pinhole lens-front element is set back from the barrier surface, the lens is, in effect, viewing through a tunnel, and the image as viewed on the camera sensor has a narrower FOV than the lens can produce. This is seen on the monitor as a porthole-like (vignetted) picture.

Pinhole Lenses

Pinhole lenses and cameras can be mounted behind a wall, with the lens viewing through a small hole in the wall. A generic characteristic for almost all pinhole-type lenses is that they invert the video picture and therefore the camera must be inverted to get a normal right-side-up picture. Some right-angle pinhole lenses reverse the image right to left and therefore require an electronic scan reversal unit to regain the correct left-to-right orientation.

Pinhole lenses have been manufactured for many years in a variety of focal lengths (FL) (3.8, 4, 5.5, 6, 8, 9, 11 millimeters), in straight, right angle, manual-, and automatic-iris configurations. The focal length (FL) of most of these lenses can be doubled to obtain one-half the FOV by using a 2× extender. The 16- and 22-millimeter FL are achieved by using a 2× magnifier on the 8- and 11-millimeter lenses, between the lens and the camera. This automatically doubles the optical speed or f/number (F/#) of each lens (halves the optical speed). In many applications, the required FL and configuration are not known in advance, and the user must have a large assortment of pinhole lenses, or take the risk that the job will be done using an incorrect lens. This dilemma has been solved with the availability of a Pinhole Lens Kit.

With this kit of pinhole lens parts, eight different FL lenses can be assembled in either a straight or right-angle configuration in minutes. An additional four combinations can be assembled for a disguised sprinkler head covert application. All lenses have a manual iris (automatic-iris optional).

Mini-Lenses

Mini-lenses are small fixed focal length (FFL) objective lenses used for covert surveillance when space is at a premium. The lenses will typically have focal lengths of 3.8, 5.5, 8, and 11 millimeters and front barrel diameters between 3/8 and 1/2 inch, making them easy to mount behind a barrier or in close quarters. These small lenses do not have an iris, and therefore, should be used in applications where the scene light level does not vary widely or with shuttered cameras. Mini-lenses, like other FFL lenses and unlike standard pinhole lenses, do not invert the image on the camera.

Mini-lenses have only three to six optical lens elements, fast optical speeds of f/1.4 to f/1.8. Pinhole lenses, on the other hand, are 3 to 5 inches long, and have as many as 10 to 20 optical elements and optical speeds of f/2.0 to f/4.0. This makes the mini-lens approximately five times faster (five times more light) than the pinhole lens.

Small Covert Camera

The most compact covert CCTV installation uses a flat board CCD camera and integral mini-lens. The complete camera is only 1.38 × 1.38 × 2.2

inches long. The 11-millimeter FL lens extends 0.3 inches in front of the camera. The camera operates directly from 12-volt DC, requires only 2.5 watts of power, and produces a standard composite video output.

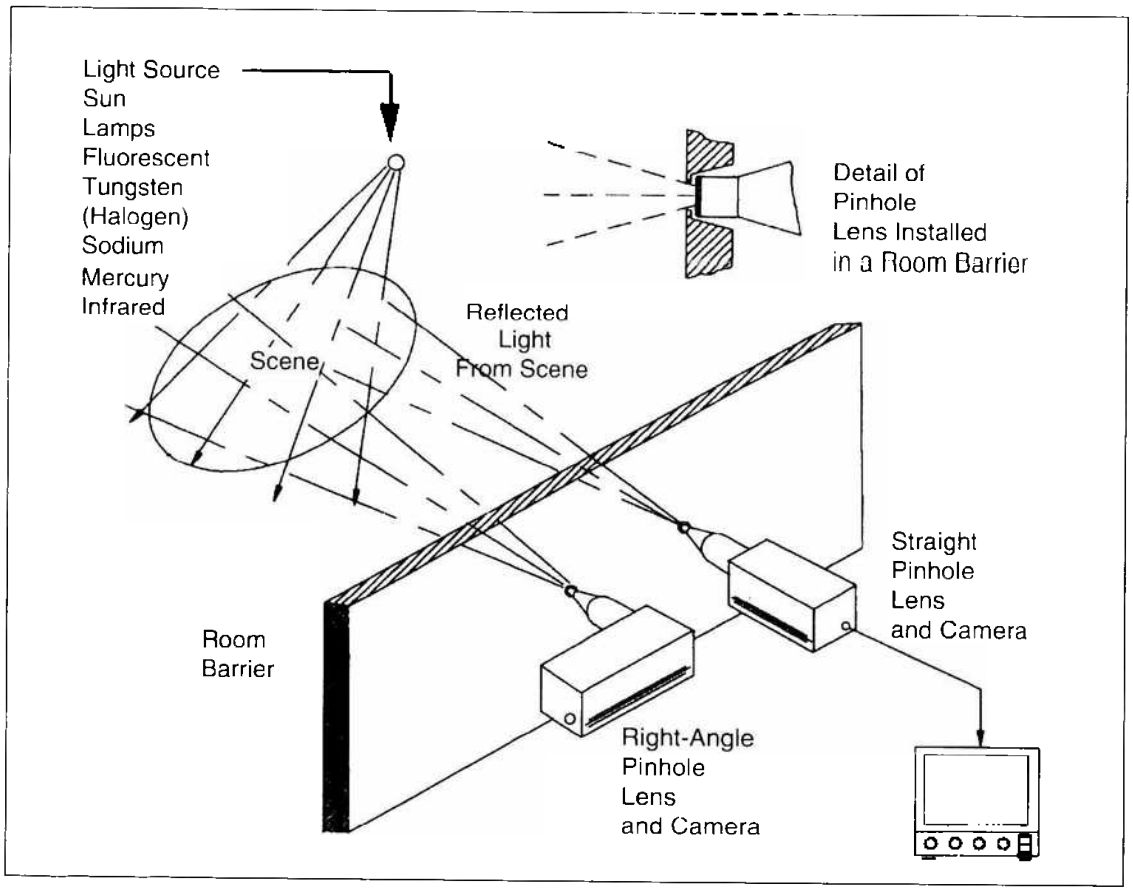
Sprinkler Head Pinhole Lens

A very effective covert system uses a camera and lens camouflaged in a ceiling-mounted sprinkler head. Of the large variety of covert lenses available for the security television industry (pinhole, mini, fiber-optic), this unique lens hides the pinhole lens in a ceiling sprinkler fixture, making detection of it extremely difficult for an observer standing at floor level. This unique combination of pinhole lens and overhead ceiling-mounted sprinkler head provides an extremely useful covert surveillance television system.

The covert surveillance sprinkler installed in the ceiling in no way affects the operation of the active fire suppression sprinkler system; however, it should not be installed in locations that have no sprinkler system so as not to give the false impression to fire and safety personnel that there is a real and active sprinkler system.

The only portion of the system visible from below is the standard sprinkler head and the small (3/8 × 5/8 inch) mirror assembly. In operation, light from the scene reflects off the small mirror which directs it to the front of the pinhole lens. The 11- or 22-millimeter pinhole lens in turn transmits and focuses the light onto the camera sensor. The small mirror can be adjusted in elevation to point at different scene heights. To point in a particular azimuth direction, the entire camera-sprinkler lens assembly is rotated with the mirror pointing in the direction of the scene of interest.

If the sprinkler head assembly is removed from the right-angle lens, all that protrudes below the ceiling is a small mirror approximately 3/8 × 5/8 inch. This technique provides



Straight and Right-Angle Pinhole Lens Installations

Figure 18. A sprinkler head unit is an investigative tool because it is difficult to see.

a very low profile and is difficult to detect by an observer at ground level.

The pinhole/mirror system provides an alternative to some dome applications. The system can be fixed or have a 360-degree panning range, or a limited pan, tilt, and zoom capability, depending on the design.

Fiber-Optic Lenses

In applications where it is required to view a scene where the camera is located 6, 8, or 12 inches behind a thick concrete wall, a rigid coherent fiber-optic conduit or a borescope lens is used to extend the objective lens several inches to several feet in front of the camera sensor.

Difficult television security applications are sometimes solved by using coherent fiber-optic bundle lenses. They are used in surveillance applications when it is necessary to view a scene on the other side of a thick barrier or inside a confined area.

The lens is installed behind a thick barrier (wall) with the objective lens on the scene side, the fiber-optic bundle within the wall, and the camera located on the protected side of the barrier. The lens viewing the scene can be a few inches or a few feet away from the camera. The rigid fiber version is a fused array of fibers and cannot be bent.

The fiber-optic lens should not to be confused with the single or multiple strands of fiber commonly used to transmit the time-modulated television signal from a camera over a long distance (hundreds of feet or miles), to a remote monitor site. The fiber-optic lens typically has 200,000 to 300,000 individual fibers forming an image-transferring array.

A minor disadvantage of all fiber-optic systems is that the picture obtained is not as "clean" as that obtained with an "all lens" pinhole lens. There are some cosmetic imperfections that look like dust spots, as well as a slight geometrical pattern caused by fiber stacking. For most surveillance applications the imperfections do not result in any loss of intelligence in the picture.

Configuration

In the case of the rigid fiber-optic bundle, the individual fibers are fused together to form a rigid glass rod or conduit. The diameter of the rigid fiber-optic bundle is approximately 0.4 inch for a 2/3-inch format sensor, 0.3-inch diameter for a 1/2-inch format, and 0.2-inch diameter for a 1/3-inch format. The rod is usually protected from the environment and mechanical damage by a rigid metal tube (0.5 inches in diameter for 2/3-inch format). It should be noted that the image exiting the fiber-optic lens is inverted with respect to the image produced by a standard objective lens. This inversion is corrected by inverting the camera.

Infrared (IR) Sources

There are numerous commercially available thermal lamp and light-emitting diode (LED) IR sources for covert CCTV applications. They vary from short range, low power, wide-angle beam to long range, high power, narrow-angle beam types.

A single IR LED emits enough IR energy to produce a useful picture at ranges up to 5 or 10 feet with a CCD camera. By stacking many (several hundred) LEDs in an array, higher IR power is directed toward the scene and a larger area at distances up to 50 to 100 feet may be viewed.

Special Configurations

CCTV cameras and lenses are concealed in many different objects and locations. Examples of some objects include an overhead track lighting fixture, emergency lighting fixture, exit sign, table top radio, table lamp, wall or desk clock, shoulder bag, attaché case, etc.

The emergency lighting fixture operates normally and can be tested for operation periodically. The fixture's operation is in no way affected by the installation of the CCTV camera.

The exit light fixture is another convenient form for camouflaging a covert CCTV camera system. The right-angle pinhole lens and CCD camera are located inside the unit and view out of either arrow on the exit sign, providing an excellent covert CCTV camera system.

A large wall-mounted clock is an ideal location for camouflaging covert CCTV camera/lens combination. The lens views out through one of the black numerals. In this case, the flat camera (approximately 7/8-inch deep) and

right-angle mini-lens is mounted directly behind the numeral 11 on the clock. The camera uses offset optics so that the camera views downward at approximately a 15-degree angle even though the clock is mounted vertically on the wall.

Wireless Transmission

Covert CCTV applications often require that the camera/lens system be installed and removed quickly from a site, or that it remain installed on location for only short periods of time. This may mean that a wired transmission means cannot be installed and that a wireless transmission means from camera to monitor (or VCR) is necessary. This takes the form of a VHF or UHF radio frequency (RF), microwave, or lightwave (IR) video transmitter of low power mounted near the television camera. The RF transmitters are of low power—from 100 milliwatts to several watts—and transmit the video picture over ranges from 100 feet to several miles.

Microwave transmission systems operate in the 2- to 22-gigahertz range and require FCC licensing and approval, but can be used by government agencies and commercial customers as well. One condition in obtaining approval is to have a frequency search performed to ensure the system causes no interference to existing equipment in the area. Most microwave systems have a more directional transmitting pattern than for the RF transmitters. Most microwave installations are line of sight, but the microwave energy can be reflected off objects in the path between the transmitter and the receiver to direct the energy to the receiver. The higher frequency of operation and directionality makes microwave installation and alignment more critical than the RF transmitters.

Pinhole lenses are used for surveillance problems that cannot be adequately solved using standard FFL or zoom lenses. The fast f/#s of some of these pinhole lenses make it possible to provide covert surveillance under normal or dimly lighted conditions. The small size of the front lens and barrel permit them to be covertly installed for surveillance applications.

A large variety of mini-, pinhole, fiber-optic, and borescope lenses are available for use in covert security applications. These lenses have FL ranges from 3.8 to 22 millimeters, covering FOVs from 12 to 78 degrees. Variations that include manual and auto iris, standard pinhole, mini and off-axis-mini, fiber optic, and borescope provide the user with a large selection from which to choose.

Herman A. Kruegle

CCTV: THE MANY ROLES OF CCTV IN SECURITY

Closed-circuit television (CCTV) is a reliable, cost-effective deterrent to crime and a means for the apprehension and prosecution of offenders. In view of high labor costs, CCTV more than ever before has earned its place as a cost-effective means for expanding security and safety, reducing asset losses and reducing the cost of security. Most safety and security applications require several different types of equipment including CCTV surveillance, fire and intrusion alarm, and access control.

Theft Reduction

Thievery causes loss of assets and time, and is a growing cancer in our society. It reduces the profits of all organizations, be they government, retail, service, manufacturing, etc. CCTV is effective in counteracting these losses in small and large companies alike, thereby increasing corporate profits. The public at large has accepted the use of CCTV systems in public and industrial facilities while the reaction by workers to its use is mixed.

The integration of CCTV with a properly designed security system can be an extremely profitable investment to any organization. One objective of the CCTV system should be to deter crime so as to prevent thievery. It has been shown that CCTV is an effective psychological deterrent to crime. If an organization or company can prevent an incident from occurring in the first place, the problem has been solved.

A second objective is the apprehension of offenders and successful dismissal or prosecution of them. A successful thief needs privacy in which to operate and it is the function of the CCTV system to prevent this. The number of thefts cannot be counted exactly, but the reduction in shrinkage can be measured.

Theft takes the form of removing valuable property and/or information from a facility.

Lost information takes the form of computer software, magnetic tape and disks, optical disks, microfilm, data on paper, etc. Real property losses include vandalizing and defacing buildings; graffiti on facilities and art objects; and destroying furniture, business machines, or other valuable equipment. CCTV surveillance systems provide a means for successfully deterring such thievery and/or detecting or apprehending the offenders.

Management Function

The protection of assets is a management function. Three key factors that govern the planning of an assets protection program are: (1) preventing losses from occurring, (2) providing adequate countermeasures to limit actual losses and to limit unpreventable losses, and (3) obtaining top management support.

The Role of CCTV in Assets Protection

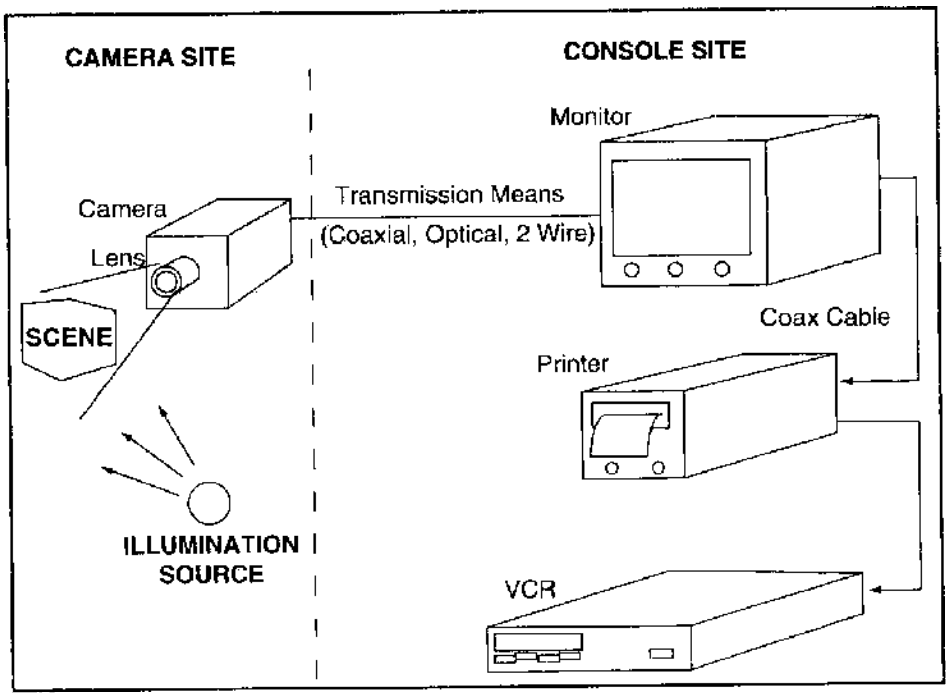
CCTV plays an important role in the protection of assets by permitting detection of unwanted entry into a facility beginning at the perimeter location and by monitoring internal activity.

The CCTV security system consists of an illumination source, lens, camera, transmission, switching, recording, and printing means. To make best use of all aspects of CCTV technology, the practitioner and end user must understand the lighting sources needed to illuminate the scene, the CCTV equipment and its capabilities, and the surveillance limitations during daytime and nighttime operation.

Videocassette recorders (VCRs) and hard-copy video printers provide CCTV security with a new dimension, i.e., going beyond real-time camera surveillance. This archiving ability is of prime importance since it permits permanent identification of activities and personnel necessary for dismissal or prosecution of an offender in a court of law at a future time.

Color vs. Monochrome

Most CCTV surveillance applications use monochrome equipment, but the solid-state camera has made color systems practical. The driving functions responsible for the accelerated development and implementation of the excellent CCTV equipment available today has been the widespread use of CCTV by consumers, made



Single Camera System

Figure 19. A single camera system has multiple components and relies on a source of illumination.

possible through technological advances and the resulting availability of low-cost VCRs and associated camera equipment. Solid-state color cameras for the consumer VCR market accelerated the availability of reliable, stable, long-life color cameras and time-lapse VCRs for the security industry. Color is important in surveillance applications because objects that are easily identified in a color scene are difficult to identify in a monochrome scene. For this reason, color cameras will replace most monochrome types as the sensitivity and resolution increases, and the cost decreases.

CCTV as Part of the Emergency and Disaster Plan

An organization should have a method to alert employees in the event of a dangerous condition, and a plan to provide for quick law enforcement, fire and/or emergency response. Every organization regardless of size should have an emergency and disaster control plan that includes CCTV as a critical component. CCTV can:

1. Protect human life by enabling security or safety officials to see remote locations, to view what is happening, where it is happening, what action is most critical, and what areas to attend to and in what priority.
2. Warn of an oncoming disaster.
3. Prevent or at least assess document or assets removal by intruders or unauthorized personnel.
4. Document via VCRs the equipment and assets in place prior to the disaster for comparison to the remaining assets after the disaster.
5. Help in restoring the organization to normal operation and procedures.
6. Reduce exposure of physical assets and optimize loss control.

Documentation of the Emergency

CCTV can aid in determining whether machinery, utilities, boilers, furnaces, etc., have been shut down properly, whether personnel must enter the area to do so, or whether other means must be taken to take it off-line. It can be used to verify that all personnel have left a potentially dangerous area.

The use of CCTV is an important tool that can be used to monitor assets during and after a disaster to ensure that material is not removed and that it is monitored. After the emergency situation has been brought under control, CCTV and security personnel provide the functions of monitoring the situation and maintaining the security of assets.

For insurance purposes, and for critique by management and security, documentation provided by CCTV recordings of assets lost or stolen and personnel injuries or deaths can support that the company was not negligent, and that a prudent emergency and disaster plan was in effect prior to the event.

CCTV can play a critical role in evaluation of a disaster plan to identify shortcomings and to illustrate correct and incorrect procedures to personnel.

Stand-By Power and Communications

It is likely that during any emergency or disaster, primary power and/or communications from one location to another will be disrupted. Stand-by power will keep emergency lighting, communications, and strategic CCTV equipment on line as needed during the emergency. When power is lost, the CCTV equipment is automatically switched over to the emergency power backup equipment (gas-powered generator) or uninterruptible power supply (UPS). A prudent security plan anticipating an emergency will include a means to power vital safety and security equipment to ensure its operation during a crisis event. Since critical CCTV and audio communications must be maintained over remote distances during such an occurrence, an alternate means of communication (signal transmission) from one location to another should be supplied either in the form of protected auxiliary hard-wired cable or a wireless system.

Security Investigations

CCTV is used for covert security investigations where the camera and lens are hidden from view by any personnel in the area so that

The definitive reference for security management professionals

Encyclopedia *of* Security Management

Second Edition

John J. Fay

The *Encyclopedia of Security Management* is a valuable guide for all security professionals.

This Second Edition emphasizes topics not covered in the First Edition, particularly those relating to homeland security, terrorism, threats to national infrastructures such as transportation, energy and agriculture, risk assessment, disaster mitigation and remediation, and weapons of mass destruction (chemical, biological, radiological, nuclear, and explosives). Fay also maintains a strong focus on security measures required at special sites such as electric power, nuclear, gas, and chemical plants; petroleum production and refining facilities; oil and gas pipelines; water treatment and distribution systems; bulk storage facilities; entertainment venues; apartment complexes and hotels; schools; hospitals; government buildings; and financial centers. The articles included in this revision also address protection of air, marine, rail, trucking, and metropolitan transit systems.

Key Features:

- Completely updated to include new information concerning homeland security and disaster management
- Maps to the domains of knowledge covered in the Certified Protection Professional examination
- Convenient new organization groups articles with related topics for ease of use

John Fay was a special agent of the U.S. Army Criminal Investigation Division (CID) and later the Director of the National Crime Prevention Institute at the University of Louisville. He was a manager of security for British Petroleum's operations in the Gulf of Mexico, as well as an adjunct professor at the University of North Florida and the University of Houston. He holds the Master of Business Administration degree from the University of Hawaii, and is a well-known and respected author of many books, including *Butterworth's Security Dictionary: Terms and Concepts; Drug Testing*, and *Model Security Policies, Plans, and Procedures*, all by Butterworth-Heinemann.

Related Titles:

Contemporary Security Management, Second Edition
John Fay
ISBN: 978-0-7506-7928-2

Security and Loss Prevention, Fifth Edition
Philip Purpura
ISBN: 978-0-12-372525-7

Risk Analysis and the Security Survey, Third Edition
James Broder
ISBN: 978-0-7506-7922-0

ELSEVIER
B H
Butterworth-Heinemann
An imprint of Elsevier
books.elsevier.com/security

ISBN: 978-0-12-370860-1
90000
9 780123 708601