COMPUTER SECURITY HANDBOOK

COMPUTER SECURITY HANDBOOK

Fifth Edition

Volume 1

Edited by

SEYMOUR BOSWORTH

M.E. KABAY

ERIC WHYNE

WILEY

John Wiley & Sons, Inc.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data

Computer security handbook. – 5th ed. / edited by Seymour Bosworth, M.E. Kabay, Eric Whyne.
p. cm.
Includes index.
ISBN 978-0-471-71652-5 ((paper) (set)) – ISBN 978-0-470-32722-7 ((vol 1)) – ISBN 978-0-470-32723-4 ((vol 2)) 1. Electronic data processing departments–Security measures. I. Bosworth, Seymour. II. Kabay, Michel E. III. Whyne, Eric, 1981–
HF5548.37.C64 2009
658.4′78–dc22

2008040626

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

CONTENTS

PREFACE

Computers are an integral part of our economic, social, professional, governmental, and military infrastructures. They have become necessities in virtually every area of modern life, but their vulnerability is of increasing concern. Computer-based systems are constantly under threats of inadvertent error and acts of nature as well as those attributable to unethical, immoral, and criminal activities. It is the purpose of this *Computer Security Handbook* to provide guidance in recognizing these threats, eliminating them where possible and, if not, then to lessen any losses attributable to them.

This *Handbook* will be most valuable to those directly responsible for computer, network, or information security as well as those who must design, install, and maintain secure systems. It will be equally important to those managers whose operating functions can be affected by breaches in security and to those executives who are responsible for protecting the assets that have been entrusted to them.

With the advent of desktop, laptop, and handheld computers, and with the vast international networks that interconnect them, the nature and extent of threats to computer security have grown almost beyond measure. In order to encompass this unprecedented expansion, the *Computer Security Handbook* has grown apace.

When the first edition of the *Handbook* was published, its entire focus was on mainframe computers, the only type then in widespread use. The second edition recognized the advent of small computers, while the third edition placed increased emphasis on PCs and networks.

Edition	Publication Date	Chapters	Text Pages
First	1973	12	162
Second	1988	19	383
Third	1995	23	571
Fourth	2002	54	1,184
Fifth	2009	77	2,040

The fourth edition of the *Computer Security Handbook* gave almost equal attention to mainframes and microcomputers.

This fifth edition has been as great a step forward as the fourth. With 77 chapters and the work of 86 authors, we have increased coverage in both breadth and depth. We now cover all 10 domains of the Common Body of Knowledge defined by the International Information Systems Security Certification Consortium $(ISC)^2$:

1. Security Management Practices: Chapters 10, 12, 13, 14, 15, 19, 10, 31, 43, 44, 45, 46, 47, 48, 49, 50, 51, 54, 55, 62, 63, 64, 65, 66, 67, 68, 74, 75, 76

2. Security Architecture and Models: Chapters 1, 2, 3, 8, 9, 24, 26, 27, 51
3. Access Control Systems and Methodology: Chapters 15, 19, 28, 29, 32
4. Application Development Security: Chapters 13, 19, 21, 30, 38, 39, 52, 53
5. Operations Security: Chapters 13, 14, 15, 19, 21, 24, 36, 40, 47, 53, 57
6. Physical Security: Chapters 4, 13, 15, 19, 22, 23, 28, 29
7. Cryptography: Chapters 7, 32, 37, 42
8. Telecomm, Networks, and Internet Security: Chapters 4, 5, 6, 13, 14, 15, 16, 17, 18, 20, 21, 24, 25, 26, 27, 30, 31, 32, 33, 34, 35, 41, 48
9. Business Continuity Planning: Chapters 22, 23, 56, 57, 58, 59, 60
10. Law, Investigations, and Ethics: Chapters 11, 12, 13, 31, 42, 61, 63, 64, 69, 70, 71, 72, 73

In addition to updating every chapter of the fourth edition, we have added chapters on:

- History of Computer Crime
- Hardware Elements of Security
- Data Communications and Information Security
- Network Topologies, Protocols, and Design
- Encryption
- Mathematical Models of Information Security
- The Dangerous Information Technology Insider: Psychological Characteristics and Career Patterns
- Social Engineering and Low-Tech Attacks
- Spam, Phishing, and Trojans: Attacks Meant to Fool
- Biometric Authentication
- Web Monitoring and Content Filtering
- Virtual Private Networks and Secure Remote Access
- 802.11 Wireless LAN Security
- Securing VoIP
- Securing P2P, IM, SMS, and Collaboration Tools
- Securing Stored Data
- Writing Secure Code
- Managing Software Patches and Vulnerabilities
- U.S. Legal and Regulatory Security Issues
- The Role of the CISO
- Developing Classification Policies for Data
- Outsourcing and Security
- Expert Witnesses and the *Daubert* Challenge
- Professional Certification and Training in Information Assurance
- Undergraduate and Graduate Education in Information Assurance
- European Graduate Work in Information Assurance and the Bologna Declaration

We have continued our practice from the fourth edition of inviting a security luminary to write the final chapter, "The Future of Information Assurance." We are pleased to include a stellar contribution from Dr. Peter G. Neumann in this edition.

SEYMOUR BOSWORTH
Senior Editor
January 2009

ACKNOWLEDGMENTS

Seymour Bosworth, Senior Editor I would like to give grateful recognition to Arthur Hutt and Douglas Hoyt, my coeditors of the first, second, and third editions of this *Handbook*. Although both Art and Doug are deceased, their commitment and their competence remain as constant reminders that nothing less than excellence is acceptable. Mich Kabay, my coeditor from the fourth edition, and Eric Whyne, our new third editor, continue in that tradition. I would not have wanted to undertake this project without them.

We mark with sadness the passing of our friend and colleague Robert Jacobson, who contributed to Chapter 1 (Brief History and Mission of Information System Security) and wrote Chapter 62 (Risk Assessment and Risk Management). Bob was a significant and valued contributor to the development of our field, and we miss his cheerful intelligence. We also miss Diane Levine, who contributed so much to both the third and fourth editions. She wrote four chapters in the third edition and six in the fourth. We are honored to continue to list her as a coauthor on five updated chapters in the fifth edition.

Thanks are also due to our colleagues at John Wiley & Sons: Tim Burgard as Acquisitions Editor, Stacey Rympa as Development Editor, Natasha Andrews-Noel as Senior Production Editor, and Debra Manette as Copyeditor and Joe Ruddick as Proofreader. All have performed their duties in an exemplary manner and with unfailing kindness, courtesy, and professionalism.

M. E. Kabay, Technical Editor The contributions from my faculty colleagues and from our alumni in the Master of Science in Information Assurance (MSIA) program at Norwich University are noteworthy. Many of the *Handbook*'s authors are graduates of the MSIA program, instructors in the program, or both.

I am immeasurably grateful to Sy for his leadership in this project. In addition to the inherent value of his decades of experience in the field of information security, his insightful editorial comments and queries have forced everyone on the project to strive for excellence in all aspects of our work. He is also fun to work with!

Our coeditor Eric Whyne has loyally persevered in his editorial tasks despite ducking bullets in the war in Iraq, where he has served honorably throughout most of the project. Our thanks to him for his service to the nation and to this project.

Our authors deserve enormous credit for the professional way in which they responded to our requests, outlines, suggestions, corrections, and nagging. I want to express my personal gratitude and appreciation for their courteous, collaborative, and responsive interactions with us.

Finally, as always, I want to thank my beloved wife, Deborah Black, light of my life, for her support and understanding over the years that this project has taken away from our time together.

Eric Whyne, Associate Editor There is an enormous amount of work put into a text of this size. The diligent and gifted authors who have contributed their time are some of the brightest and most experienced professionals in their fields. They did so not for compensation but because they love the subjects which they have put so much effort into mastering. The *Computer Security Handbook* will continue its tradition of being a collection point for these labors so long as there are great minds in love with the challenging problems of computer security and willing to devote their time to sharing solutions.

At the time I started on the project, I was a Marine Officer working in the data communications field in Ramadi, Iraq. I worked the night shift and spent my afternoons perched in a folding chair, under the relatively cool Iraq winter sun, writing correspondence and doing first-past edits of the chapters of the *Handbook*. Upon my return to the United States, my spare evenings along the North Carolina coast were dedicated to the *Handbook* as I worked my day job as the Marine Corps Anti-Terrorism Battalion Communications Officer. Since then I have deployed once more to Iraq as an advisor to the Iraqi Army. Everywhere I have gone, and with every job I have held, I have been able to apply and refine the principles covered in this *Handbook* and in previous versions. From the most high-tech cutting-edge, multiplexed satellite communications system used in military operations in Iraq, to the relatively mundane desktop computer networks of offices in the United States, to the ancient weathered computers the Iraqi Army totes around with them and ties into the power grid at any opportunity, computer security is critical to the accomplishment of the most basic tasks these systems are used for.

Unarguably, the exchange of information and ideas has been the largest factor in the shaping and betterment of our world throughout history. Having spent the last year of my life living as a local in a third-world country, that fact is fresh on my mind. In that spirit, computers are recognized as the most powerful and universally applicable tool ever devised. This book's purpose is to help you ensure that your computers remain powerful and successfully applied to the tasks for which you intend them to be used.

I am grateful to Sy Bosworth and Mich Kabay for their faith in bringing me into this project, and for their guidance and leadership along the way. They are both great people, and it has been an honor and a joy to work with them.

ABOUT THE EDITORS

Seymour Bosworth, MS, CDP (e-mail: *sybosworth55@gmail.com*) is president of S. Bosworth & Associates, Plainview, New York, a management consulting firm specializing in computing applications for banking, commerce, and industry. Since 1972, he has been a contributing editor of all five editions of the *Computer Security Handbook,* and he has written many articles and lectured extensively about computer security and other technical and managerial subjects. He has been responsible for design and manufacture, systems analysis, programming, and operations, of both digital and analog computers. For his technical contributions, including an error-computing calibrator, a programming aid, and an analog-to-digital converter, he has been granted a number of patents, and is working on several others.

Bosworth is a former president and CEO of Computer Corporation of America, manufacturers of computers for scientific and engineering applications; president of Abbey Electronics Corporation, manufacturers of precision electronic instruments and digital devices; and president of Alpha Data Processing Corporation, a general-purpose computer service bureau. As a vice president at Bankers Trust company, he had overall responsibility for computer operations, including security concerns.

For more than 20 years, Bosworth was an Adjunct Associate Professor of Management at the Information Technologies Institute of New York University, where he lectured on computer security and related disciplines. He has conducted many seminars and training sessions for the Battelle Institute, New York University, the Negotiation Institute, the American Management Association, and other prestigious organizations. For many years he served as Arbitrator, Chief Arbitrator, and Panelist for the American Arbitration Association. He holds a Master's degree from the Graduate School of Business of Columbia University and the Certificate in Data Processing of the Data Processing Management Association.

M. E. Kabay, PhD, CISSP-ISSMP (e-mail: *mekabay@gmail.com*) has been programming since 1966. In 1976, he received his PhD from Dartmouth College in applied statistics and invertebrate zoology. After joining a compiler and relational database team in 1979, he worked for Hewlett Packard (Canada) Ltd. from 1980 through 1983 as an HP3000 operating system performance specialist and then ran operations at a large service bureau in Montréal in the mid-1980s before founding his own operations management consultancy. From 1986 to 1996, he was an adjunct instructor in the John Abbott College professional programs in Programming and in Technical Support. He was Director of Education for the National Computer Security Association from 1991 to the end of 1999 and was Security Leader for the INFOSEC Group of AtomicTangerine, Inc., from January 2000 to June 2001. In July 2001, he joined the faculty at Norwich University as Associate Professor of Computer Information Systems in the

School of Business and Management. In January 2002, he took on additional duties as the director of the graduate program in information assurance in the School of Graduate Studies at Norwich, where he is also Chief Technical Officer.

Kabay was inducted into the Information Systems Security Association Hall of Fame in 2004. He has published over 950 articles in operations management and security in several trade journals. He currently writes two columns a week for *Network World Security Strategies*; archives are at *www.networkworld.com/newsletters/sec/*. He has a Web site with freely available teaching materials and papers at *www2.norwich.edu/mkabay/index.htm*.

Eric Whyne (e-mail: *ericwhyne@gmail.com*) is a Captain in the United States Marine Corps. He joined the Marine Corps in the Signals Intelligence field and received two meritorious promotions before being selected for an officer candidate program and finally commissioning into the communications occupational specialty. His billets have included commanding a data communications platoon, managing large-scale communications networks, advising the Iraqi Army, and serving as the senior communications officer for the Marine Corps Anti-Terrorism unit. Whyne holds a BS in Computer Science from Norwich University as well as minor degrees in Mathematics, Information Assurance, and Engineering. He has presented about communications security and other technology topics at many forums and worked as a researcher for the National Center for Counter-Terrorism and Cyber Crime Research. After nine honorable years of service and two tours to Iraq totaling 18 months, Whyne is transitioning out of the military and pursuing a career in the civilian industry in order to more effectively and freely apply his skills and abilities to cutting-edge technological trends and problems.

ABOUT THE CONTRIBUTORS

Mani Akella, Director (Technology), has been actively working with information security architectures and identity protection for Consultantgurus and its clients. An industry professional for 20 years, Akella has worked with hardware, software, networking, and all the associated technologies that service information in all of its incarnations and aspects. Over the years, he has developed a particular affinity for international data law and understanding people and why they do what they do (or do not). He firmly believes that the best law and policy is that which understands and accounts for cross-cultural differences, and works with an understanding of culture and societal influences. To that end, he has been actively working with all his clients and business acquaintances to improve security policies and make them more people-friendly: His experience has been that the best policy is that which works with, instead of being anagonistic to, the end user.

Rebecca Gurley Bace is the President/CEO of Infidel, Inc., a strategic consulting practice headquartered in Scotts Valley, California. She is also a venture consultant for Palo Alto–based Trident Capital, where she is credited with building Trident's investment portfolio of security product and service firms. Her areas of expertise include intrusion detection and prevention, vulnerability analysis and mitigation, and the technical transfer of information security research results to the commercial product realm. Prior to transitioning to the commercial world, Bace worked in the public sector, first at the National Security Agency, where she led the Intrusion Detection research program, then at the Computing Division of the Los Alamos National Laboratory, where she served as Deputy Security Officer. Bace's publishing credits include two books, an NIST Special Publication on intrusion detection and prevention, and numerous articles on information security technology topics.

Susan Baumes, MS, CISSP, is an information security professional working in the financial services industry. In her current role, Ms. Baumes works across the enterprise to develop information security awareness and is responsible for application security. Her role also extends to policy development, compliance and audit. She has 11 years experience in application development, systems and network administration, database management, and information security. Previously, Ms. Baumes worked in a number of different sectors including government (federal and state), academia and retail.

Kurt Baumgarten, CISA (e-mail: *kurtb@peritussecurity.com*) is Vice President of Information Security and a partner at Peritus Security Partners, LLC, a leader in providing compliance-driven information security solutions. He is also a lecturer, consultant, and the developer of the DDIPS intrusion prevention technology as well as a pioneer in

using best practices frameworks for the improvement of information technology security programs and management systems. Baumgarten has authored multiple articles about the business benefits of sound information technology and information assurance practices, and assists businesses and government agencies in defining strategic plans that enhance IT and IA as positive value chain modifiers. He holds both a Master's of Science in Information Assurance and an MBA with a concentration in E-Commerce, and serves as an Adjunct Professor of Information Assurance. He has more than 20 years of experience in IT infrastructure and Information Security and is an active member of ISSA, ISACA, ISSSP, and the MIT Enterprise Forum. Baumgarten periodically acts as an interim Director within external organizations in order to facilitate strategic operational changes in IT and Information Security.

Kevin Beets has been a Research Scientist with McAfee for the past five years. His work has concentrated on vulnerability and malware research and documentation with the Foundstone R&D and Avert Labs teams. Prior to working at McAfee, he architected private LANs as well as built, monitored, and supported CheckPoint and PIX firewalls and RealSecure IDS systems.

Matt Bishop is a Professor in the Department of Computer Science at the University of California at Davis and a Codirector of the Computer Security Laboratory. His main research area is the analysis of vulnerabilities in computer systems, especially their origin, detection, and remediation. He also studies network security, policy modeling, and electronic voting. His textbook, *Computer Security: Art and Science,* is widely used in advanced undergraduate and graduate courses. He received his PhD in computer science from Purdue University, where he specialized in computer security, in 1984.

Kip Boyle is the Chief Information Security Officer of PEMCO Insurance, a $350 million property, casualty, and life insurance company serving the Pacific Northwest. Prior to joining PEMCO Insurance, he held such positions as Chief Security Officer for a $50 million national credit card transaction processor and technology service provider; Authentication and Encryption Product Manager for Cable & Wireless America; Senior Security Architect for Digital Island, Inc.; and a Senior Consultant in the Information Security Group at Stanford Research Institute (SRI) Consulting. He has also held director-level positions in information systems and network security for the U.S. Air Force. Boyle is a Certified Information System Security Professional and Certified Information Security Manager. He holds a Bachelor's of Science in Computer Information Systems from the University of Tampa (where he was an Air Force ROTC Distinguished Graduate) and a Master's of Science in Management from Troy State University.

Timothy Braithwaite has more than 30 years of hands-on experience in all aspects of automated information processing and communications. He is currently Deputy Director of Strategic Programs at the Center for Information Assurance of Titan Corporation. Before joining Titan, he managed most aspects of information technology, including data and communications centers, software development projects, strategic planning and budget organizations, system security programs, and quality improvement initiatives. His pioneering work in computer systems and communications security while with the Department of Defense resulted in his selection to be the first Systems Security Officer for the Social Security Administration (SSA) in 1980. After developing security policy and establishing a nationwide network of regional security officers,

Braithwaite directed the risk assessment of all payment systems for the agency. In 1982, he assumed the duties of Deputy Director, Systems Planning and Control of the SSA, where he performed substantive reviews of all major acquisitions for the Associate Commissioner for Systems and, through a facilitation process, personally led the development of the first Strategic Systems Plan for the administration. In 1984, he became Director of Information and Communication Services for the Bureau of Alcohol, Tobacco, and Firearms at the Department of Treasury. In the private sector, he worked in senior technical and business development positions for SAGE Federal Systems, a software development company; Validity Corporation, a testing and independent validation and verification company; and J.G. Van Dyke & Associates, where he was Director, Y2K Testing Services. He was recruited to join Titan Corporation in December 1999 to assist in establishing and growing the company's Information Assurance practice.

Paul J. Brusil, PhD (e-mail: *brusil@post.harvard.edu*) founded Strategic Management Directions, a security and enterprise management consultancy in Beverly, Massachusetts. He has been working with various industry and government sectors including healthcare, telecommunications, and middleware to improve the specification, implementation, and use of trustworthy, quality, security-related products and systems. He supported strategic planning that led to the National Information Assurance Partnership and other industry forums created to understand, promote, and use the Common Criteria to develop security and assurance requirements and to evaluate products. Brusil has organized, convened, and chaired several national workshops, conferences, and international symposia pertinent to management and security. Through these and other efforts to stimulate awareness and cooperation among competing market forces, he spearheaded industry's development of the initial open, secure, convergent, standards-based network and enterprise management solutions. While at the MITRE Corp, Brusil led research and development critical to the commercialization of the world's first LAN solutions. Earlier, at Harvard, he pioneered research leading to noninvasive diagnosis of cardiopulmonary dysfunction. He is a Senior Member of the IEEE, a member of the Editorial Advisory Board of the *Journal of Network and Systems Management* (*JNSM*), has been Senior Technical Editor for *JNSM,* is the Guest Editor for all *JNSM*'s Special Issues on Security and Management, and is a Lead Instructor for the Adjunct Faculty supporting the Master's of Science in Information Assurance degree program at Norwich University. He has authored over 100 papers and book chapters. He graduated from Harvard University with a joint degree in Engineering and Medicine.

David Brussin is Founder and CEO of Monetate, Inc. Monetate powers Intelligent Personal Promotions™ for online retailers. Brussin is a serial entrepreneur recognized as a leading information security and technology expert, and was honored by MIT's *Technology Review* as one of the world's 100 top young innovators. In January 2004, Brussin cofounded TurnTide, Inc. around the antispam router technology he had invented. As Chief Technology Officer, he also managed engineering and technical operations. TurnTide was acquired by Symantec six months later. Previously, Brussin cofounded and served as Chief Technology Officer for ePrivacy Group, Inc., which created the Trusted Sender program and Trusted Email Open Standard to protect and grow the e-mail marketing channel. Brussin created products to help e-mail marketers increase response and conversion by protecting their trusted relationship with consumers. In 1996, he cofounded and served as Vice President of Technology for InfoSec Labs,

an information security company dedicated to helping Fortune 1000 companies safely transition their businesses into the online world. Partnering with his clients, Brussin balanced security with the emerging technical challenges of doing business online and helped many established bricks-and-mortar businesses become multichannel. InfoSec Labs was acquired by Rainbow Technologies, now part of SafeNet, in 1999. Brussin is a frequent speaker and writer on entrepreneurship and technology. He also serves on the Board of Directors of Invite Media, Inc., a stealth-mode start-up working to analyze and optimize online display advertising.

Michael Buglewicz spent approximately 10 years in law enforcement carrying out a variety of duties, from front-line patrol work through complex investigations. After concluding his law enforcement career. Buglewicz brought his experiences to technology and held a variety of roles within First Data Corporation, including Internet banking and online payment systems. Buglewicz has worked for Microsoft Corporation since 1996 in a variety of roles and has taught in Norwich University's Information Assurance program. Buglewicz holds an undergraduate degree in Fine Arts from the University of Nebraska at Omaha and graduate degrees from Illinois State University as well as a Master's degree in Information Assurance from Norwich University. His current interests focus on corporate risk management.

Nancy Callahan is Vice President, AIG Executive Liability, Financial Institutions Division. AIG is the world's leading international insurance and financial services organization, with operations in approximately 130 countries and jurisdictions. AIG member companies serve commercial, institutional, and individual customers through the most extensive worldwide property-casualty and life insurance networks of any insurer. An expert on privacy and identity theft, Callahan is a frequent speaker at industry conferences throughout the United States and is a much-sought-after media resource, having been quoted in the *Wall Street Journal* and Associated Press. Callahan joined AIG in 2001. Prior to AIG, Callahan worked in e-commerce and financial services. She spent 13 years at Reuters, where her final position was Executive Vice President, Money Transaction Systems. Callahan is a Chartered Property and Casualty Underwriter and Certified Information Privacy Professional. She has a Master's of Business Administration and a BS in Systems Engineering from the University of Virginia.

Q. Campbell (e-mail: *qcampbell@hushmail.com*) has worked in the information security field for over six years. He specializes in information technology threat analysis and education.

Wendy Carr, CISSP (e-mail: *wendylcarr@gmail.com*) is a Senior Consultant with Booz, Allen & Hamilton on a client-site in New England. Her focus on addressing security concerns related to the implementation of products and applications includes concentrations in the areas of Certification and Accreditation (Commercial/DITSCAP/DIACAP), risk analysis, compliance testing and vulnerability assessment, forensic examination, incident response, disaster recovery, authentication, and encryption for both physical and wireless environments in the fields of Military, Government and Banking. She holds an MS in Information Assurance from Norwich University and is a member of $(ISC)^2$, InfraGard, and the Norwich University *Journal of Information Assurance* Editorial Review Board as well as several organizations dedicated to the advancement of information security.

Santosh Chokhani (e-mail: *schokhani@cygnacom.com*) is the Founder and President of CygnaCom Solutions, Inc., an Entrust company specializing in PKI. He has made numerous contributions to PKI technology and related standards, including trust models, security, and policy and revocation processing. He is the inventor of the PKI Certificate Policy and Certification Practices Statement Framework. His pioneering work in this area led to the Internet RFC that is used as the standard for CP and CPS by governments and industry throughout the world. Before starting CygnaCom, he worked for The MITRE Corporation from 1978 to 1994. At MITRE, he was senior technical manager and managed a variety of technology research, development, and engineering projects in the areas of PKI, computer security, expert systems, image processing, and computer graphics. Chokhani obtained his Master's (1971) and PhD (1975) in Electrical Engineering/Computer Science from Rutgers University, where he was a Louis Bevior Fellow from 1971 to 1973.

Christopher Christian is an aviator in the United States Army. He received a Bachelor's degree in Computer Information Systems at Norwich University class of 2005. His primary focus of study was Information Assurance and Security. He worked as an intern for an engineering consulting company for three years. He developed cost/analysis worksheets and floor-plan layouts to maximize workspace efficiency for companies in various industries. Christian graduated flight school at Fort Rucker, Alabama, there he trained on the H-60 Blackhawk. He serves as a Flight Platoon Leader in an Air Assault Battalion. First Lieutenant Christian is currently serving in Iraq in support of Operation Iraqi Freedom 08–09.

Chey Cobb, CISSP (e-mail: *cheycobb@gmail.com*) began her career in information security while at the National Computer Security Association (now known as TruSecure/ICSA Labs). During her tenure as the NCSA award–winning Webmaster, she realized that Web servers often created security holes in networks and became an outspoken advocate of systems security. Later, while developing secure networks for the Air Force in Florida, her work captured the attention of the U.S. intelligence agencies. Cobb moved to Virginia and began working for the government as the Senior Technical Security Advisor on highly classified projects. Ultimately, she went on to manage the security program at an overseas site. Cobb, who is now semiretired, writes books and articles on computer security and is a frequent speaker at security conferences.

Stephen Cobb, CISSP (e-mail: *sc@cobbassociates.com*) is an independent information security consultant and an Adjunct Professor of Information Assurance at Norwich University, Vermont. A graduate of the University of Leeds, Cobb's areas of expertise include risk assessment, computer fraud, data privacy, business continuity management, and security awareness and education. A frequent speaker and seminar leader at industry conferences around the world, Cobb is the author of numerous books on security and privacy as well as hundreds of articles. Cobb cofounded several security companies whose products expanded the range of security solutions available to enterprises and government agencies. As a consultant, he has advised some of the world's largest companies on how to maximize the benefits of information technology by minimizing IT risks.

Caleb S. Coggins, MSIA, CISSP, is a Corporate Auditor for Bridgestone Americas. His areas of interest include vulnerability management, network security, and information assurance. Prior to Bridgestone, Coggins served as the Information Manager

for a private company as well as an information security consultant to business clients. He holds a BA from Willamette University and an MS in Information Assurance from Norwich University.

Bernie Cowens, CISSP, CISA (e-mail: *bcowens@usa.com*) is Chief Information Security Officer at a Fortune 500 company in the financial services industry. He is an information risk, privacy, and security expert with more than 20 years experience in industries including defense, high technology, healthcare, financial, and Big Four professional services. Cowens has created, trained, and led a number of computer emergency, forensic investigation, and incident response teams over the years. He has real-world experience responding to attacks, disasters, and failures resulting from a variety of sources, including malicious attackers, criminals, and foreign governments. He has served as an advisor to and a member of national-level panels charged with analyzing cyber-system threats to critical infrastructures, assessing associated risks, and recommending both technical and nontechnical mitigation policies and procedures. Cowens holds a Master's degree in Management Information Systems along with undergraduate degrees and certificates in systems management and information processing.

Christopher Dantos is a Senior Architectural Specialist with Computer Science Corporation's Global Security Solutions Group. His areas of expertise include 802.11, VoIP, and Web application security. Prior to joining CSC, he spent 10 years as a Security Architect with Motorola Inc., including 5 years in the Motorola Labs Wireless Access Research Center of Excellence. He holds a Master's of Science degree in Information Assurance from Norwich University and a Bachelor's of Science degree in Marine Engineering from the Maine Maritime Academy.

Chris Davis, CISA, CISSP, has trained and presented in information security, advanced computer forensic analysis, hardware security design, auditing, and certification curriculum for government, corporate, and university requirements. He was part of the teams responsible for Hacking Exposed Computer Forensics, IT Auditing: Using Controls to Protect Information Assets, and the Anti-Hacker Toolkit. His contributions include projects and presentations for SANS, Gartner, Harvard, BlackHat, CEIC, and 3GSM. He has enjoyed positions at ForeScout, Texas Instruments, Microsoft Technology Center, and Cisco Systems. He holds a Bachelor's degree in Nuclear Engineering Technologies from Thomas Edison, and a Master's in Business from the University of Texas at Austin.

Seth Finkelstein (e-mail: *sethf@sethf.com)* is a professional programmer with degrees in Mathematics and in Physics from MIT. He cofounded the Censorware Project, an anti-censorware advocacy group. In 1998, his efforts evaluating the sites blocked by the library's Internet policy in Loudoun County, Virginia, helped the American Civil Liberties Union win a federal lawsuit challenging the policy. In 2001, he received a Pioneer of the Electronic Frontier Award from the Electronic Frontier Foundation for his groundbreaking work in analyzing content-blocking software. In 2003, he was primarily responsible for winning a temporary exemption in the Digital Millennium Copyright Act allowing for the analysis of censorware.

Urs E. Gattiker is an internationally-renowned security and risk technologist, both a Founder and the Chief Technology Officer of CyTRAP Labs GmbH. CyTRAP Labs

provides corporate governance and social media services to organizations worldwide. Using sophisticated analysis and correlation tools, CyTRAP Labs' expert Internet Analysts monitor suspicious internal and external activities, user and community behavior, business goals, and web technology to craft and deliver long term successful web and corporate risk management programs for companies.

Urs is the inventor of the ComMetrics benchmark battery of tools. One of these, the FT/ComMetrics corporate blog index, empowers the FT Global 500 companies to compare the value of their blogging activities against to that target information security prevention and safety, with other enterprises. He is the author and co-author of several books on computer viruses, technology and risk management. Gattiker holds a PhD in business focusing on computing/informatics and an MBA (international marketing) both from Claremont Graduate University (Claremont Colleges) and a BS in public administration/informatics from the HWV Zurich.

Robert Gezelter, CDP, has over 33 years of experience in computing, starting with programming scientific/technical problems. Shortly thereafter, his focus shifted to operating systems, networks, security, and related matters, where he has 32 years of experience in systems architecture, programming, and management. He has worked extensively in systems architecture, security, internals, and networks, ranging from high-level strategic issues to the low-level specification, design, and implementation of device protocols and embedded firmware.

Gezelter is an alumnus of the IEEE Computer Society's Distinguished Visitor Program for North America, having been appointed to a three-year term in 2004. His appointment included numerous presentations at Computer Society chapters throughout North America.

He has published numerous articles, appearing in *Hardcopy, Computer Purchasing Update, Network Computing, Open Systems Today, Digital Systems Journal,* and *Network World*. He is a frequent presenter at conference sessions on operating systems, languages, security, networks, and related topics at local, regional, national, and international conferences, speaking for DECUS, Encompass, IEEE, ISSA, ISACA, and others. He previously authored the mobile code and Internet-related chapters for the 4th edition of this *Handbook* (2002) as well as the "Internet Security" chapters of the 3rd edition (1995) and its supplement (1997).

He is a graduate of New York University with BA (1981) and MS (1983) degrees in Computer Science. Gezelter founded his consulting practice in 1978, working with clients both locally and internationally. He maintains his offices in Flushing, New York. He may be contacted via his firm's www site at www.rlgsc.com.

Anup K. Ghosh is President and Chief Executive of Secure Command, LLC, a security software start-up developing next-generation Internet security products for corporate networks. Ghosh also holds a position as Research Professor at George Mason University. Ghosh was previously Senior Scientist and Program Manager in the Advanced Technology Office of the Defense Advanced Research Projects Agency (DARPA), where he managed an extensive portfolio of information assurance and information operations programs. Ghosh previously served in executive management as Vice President of Research at Cigital, Inc. He has served as principal investigator on contracts from DARPA, NSA, and NIST's Advanced Technology Program and has written more than 40 peer-reviewed conference and journal articles. Ghosh is also author of three books on computer network defense and serves on the editorial board of *IEEE Security and Privacy Magazine* and has been guest editor for *IEEE Software* and *IEEE Journal*

on Selected Areas in Communications. Ghosh is a Senior Member of the IEEE. For his contributions to the Department of Defense's information assurance, Ghosh was awarded the Frank B. Rowlett Trophy for Individual Contributions by the National Security Agency in November 2005, a federal government–wide award. He was also awarded the Office of the Secretary of Defense Medal for Exceptional Public Service for his contributions while at DARPA. In 2005, Worcester Polytechnic Institute awarded Ghosh its Hobart Newell Award for Outstanding Contributions to the Electrical and Computer Engineering Profession. Ghosh has previously been awarded the IEEE's Millennium Medal for Outstanding Contributions to E-Commerce Security. Ghosh completed his PhD and Master of Science in Electrical Engineering at the University of Virginia and his Bachelor of Science in Electrical Engineering at Worcester Polytechnic Institute.

Donald Glass, CISA, CISSP (e-mail: *donald@donaldglass.com*) has over 15 years of experience in the IT Auditing and Information Security fields. He's the current Director of IT Audit for Kerzner International. Author of several information security and IT audit articles, Donald is recognized as a leader in the IT audit field and information security.

Robert Guess is a Senior Security Engineer at a Fortune 500 firm and an Associate Professor of Information Systems Technology. Guess possesses a Master's of Science in Information Assurance from Norwich University and has over a dozen industry certifications, including the National Security Agency INFOSEC Assessment Methodology, National Security Agency INFOSEC Evaluation Methodology, and Certified Information Systems Security Practitioner. His professional efforts include work in the defense sector, serving as primary subject matter expert on a National Science Foundation Cybersecurity Education Grant, and the development of Department of Defense workforce certification standards for information assurance professionals. Guess's work in recent years has focused on security assessment, penetration testing, incident response, and the forensic analysis of digital evidence.

David Gursky is an Information Assurance manager and researcher at Raytheon Integrated Defense Systems working in Crystal City, Virginia. He is principal investigator for behavior-based intrusion detection systems, attribute-based access control, and resource-efficient authentication techniques. He held several senior positions as a Department of Defense Contractor supporting Information Assurance programs and has over 30 years' experience in information technology and information security. He has conducted numerous security audits for PriceWaterhouse and Coopers. Gursky has Bachelor's of Science degree in Business Management from Southern New Hampshire University, a Master's of Science degree from Norwich University, and an MBA from from Northeastern University. In addition, he holds a CISA, CISM and CISSP certifications. He lives in Northern Virginia and is an active member of $(ISC)^2$ and ISACA.

Jennifer Hadley (e-mail: *hadley.jennifer@gmail.com*) is a member of the first Master of Science in Information Assurance graduating class at Norwich University. She is the primary Systems and Security Consultant for Indiana Networking in Lafayette, Indiana, and has served as both a network and systems administrator in higher education and private consulting. She has almost 10 years' experience as a programmer and instructor of Web technologies with additional interests in data backup, virtualization,

authentication/identification, monitoring, desktop and server deployment, and incident response. At present Hadley serves as a Technology Consultant for Axcell Technologies, Inc. Previously she worked as a tester for quality and performance projects for Google, Inc., and as a collegiate adjunct instructor in computer technologies. Hadley received a Bachelor's of Science degree in Industrial and Computer Technology from Purdue University.

Carl Hallberg, CISSP, has been a Unix Systems Administrator for years as well as an Information Security Consultant. He has also written training courses for subjects including firewalls, VPNs, and home network security. He has a Bachelor's degree in Psychology. Currently he is a senior member of an incident response team for a major U.S. financial institution.

Kevin Henry has been involved in computers since 1976, when he was an operator on the largest minicomputer system in Canada. He has since worked in many areas of information technology, including computer programming, systems analysis, and information technology audit. Henry was asked to become Director of Security based on the evidence of his audits and involvement in promoting secure IT operations. Following 20 years in the telecommunications field, Henry moved to a Senior Auditor position with the State of Oregon, where he was a member of the Governor's IT Security Subcommittee and performed audits on courts and court-related IT systems.

Henry has extensive experience in Risk Management and Business Continuity and Disaster Recovery Planning. He frequently presents papers at industry events and conferences and is on the preferred speakers list for nearly every major security conference. Since joining $(ISC)^2$ as their first full-time Program Manager in 2002, Henry has been responsible for research and development of new certifications, courseware, and development of educational programs and instructors. He has also been providing support services and consulting for organizations that require in-depth risk analysis and assistance with specific security-related challenges. This has led to numerous consulting engagements in the Middle East and Asia for large telecommunications firms, government departments, and commercial enterprises.

Don Holden is a Principal Consultant with Concordant specializing in information security. He has more than 20 years of management experience in information systems, security, encryption, business continuity, and disaster recovery planning in both industry and government. Previously he was a Technology Leader for RedSiren Technologies (formerly SRI Consulting). Holden's achievements include leading a cyber-insurance joint venture project, developing privacy and encryption policies for major financial institutions, and recommending standards-based information technology security policies for a federal financial regulator. Holden is an Adjunct Professor for the Norwich University's Master's of Science in Information Assurance. He received an MBA from Wharton and is a Certified Information System Security Professional and Information System Security Management Professional.

John D. Howard is a former Air Force engineer and test pilot who currently works in the Security and Networking Research Group at the Sandia National Laboratories, Livermore, California. His projects include development of the SecureLink software for automatic encryption of network connections. He has extensive experience in systems development, including an aircraft–ground collision avoidance system for which he

holds a patent. He is a graduate of the Air Force Academy, has Master's degrees in both Aeronautical Engineering and Political Science, and has a PhD in Engineering and Public Policy from Carnegie Mellon University.

Arthur E. Hutt, CCEP. The late Arthur E. Hutt was an information systems consultant with extensive experience in banking, industry, and government. He served as a contributing editor to the 1st, 2nd, and 3rd Editions of the Computer Security Handbook. He was a principal of PAGE Assured Systems, Inc., a consulting group specializing in security and control of information systems and contingency/disaster recovery planning. He was a senior information systems executive for several major banks active in domestic and international banking. His innovative and pioneering development of online banking systems received international recognition. He was also noted for his contributions to computer security and to information systems planning for municipal government. He was on the faculty of the City University of New York and served as a consultant to CUNY on curriculum and on data processing management. He also served on the mayor's technical advisory panel for the City of New York. Hutt was active in development of national and international technical standards, via ANSI and ISO, for the banking industry.

Robert V. Jacobson, CPP, CISSP, deceased was the President of International Security Technology, Inc., a New York City–based risk management consulting firm. Jacobson founded IST in 1978 to develop and apply superior risk management systems. Current and past government and industry clients are located in the United States, Europe, Africa, Asia, and the Middle East. Jacobson pioneered many of the basic computer security concepts now in general use. He served as the first Information System Security Officer at Chemical Bank, now known as J P Morgan Chase. He was a frequent lecturer and had written numerous technical articles. Mr. Jacobson held BS and MS degrees from Yale University, and was a Certified Information Systems Security Professional. He was also a Certified Protection Professional of the American Society for Industrial Security. He was a member of the National Fire Protection Association and the Information Systems Security Association. In 1991, he received the Fitzgerald Memorial Award for Excellence in Security from the New York Chapter of the ISSA.

David J. Johnson is an information security analyst for a Fortune 1000 financial services company where he focuses primarily on information security policy and standard creation and maintenance. Additionally, he also performs analysis of information technology projects, as well as IT and business processes, for security and business continuity impact and system vulnerability management. Johnson's prior work includes nine years designing, building, and maintaining an electronic commerce (EC/EDI) infrastructure and data transfers for a national financial service company. He holds a Bachelor's of Science in Business Administration from Oregon State University and a Master's of Science in Information Assurance from Norwich University.

Sean Kelley is an Adjunct Professor in Information Assurance (IA) for Norwich and Troy University. He also teaches IA and management conferences for the SANS Institute. His information security career is diversified and has taken him to high-level organizations in Washington, DC, including the Attending Physician's Office to Congress, U.S. Capitol, where he was responsible for the development of policy and controls for the secure handling of electronic health records for 535 members of Congress, Supreme Court Justices, and officials. Kelley is a Certified Information

Systems Security Professional and PMP and also holds several NSA certificates. Kelley also holds a Master's degree from Webster University in Computer Resources and Information Management and a second Master's degree from the Naval Postgraduate School in Information Technology, where he concentrated on computer and network security by taking classes through the NPS Center for INFOSEC Studies and Research.

David M. Kennedy, CISSP (e-mail: *david.kennedy@acm.org*) is TruSecure Corporation's Chief of Research. He directs the Research Group to provide expert services to TruSecure Corporation members, clients, and staff. He supervises the Information Security Reconnaissance (IS/R) team, which collects security-relevant information, both above- and underground in TruSecure Corporation's IS/R data collection. IS/R provides biweekly and special topic reports to IS/R subscribers. Kennedy is a retired U.S. Army Military Police officer. In his last tour of duty, he was responsible for enterprise security of five LANs with Internet access and over 3,000 personal computers and workstations. He holds a BS in Forensic Science.

Gary C. Kessler is an Associate Professor of Computer and Digital Forensics and Coordination of Information Assurance Education at Champlain College in Burlington, Vermont, where he is also the Director of the Champlain College Center for Digital Investigation. Kessler is a technical consultant to the Vermont Internet Crimes Task Force and a member of the High Technology Crime Investigation Association and High Tech Crime Consortium; he is also a Certified Information Systems Security Professional and Certified Computer Examiner. Kessler is a frequent speaker at industry conferences, has written two books and over 70 articles on a variety of technology topics, and is an Associate Editor of the *Journal of Digital Forensic Practice* and serves on the editorial board of the *Journal of Digital Forensics, Security, and Law.* He holds a BA in Mathematics, an MS in Computer Science, an EdS in Computing Technology in Education, and is pursuing a doctorate degree.

David A. Land. In the U.S. Army as a Counterintelligence Special Agent, Land and David Christie developed and hosted the first Department of Defense Computer Crimes Conference. Since then Land has investigated espionage cases for both the Army and the Department of Energy. He serves as the Information Technology Coordinator for Anniston City Schools in Alabama and as an Adjunct Professor for Norwich University, his alma mater.

D. T. Lang served in the United States Air Force, retiring as a Special Agent in Charge. As a Special Agent he worked in the areas of antiterrorism, executive and force protection, counterintelligence and counterespionage. Lang is a combat veteran of Operation Desert Storm and was charged with the Joint Force Protection Team for the United Nations Implementation Forces in Zagreb, Croatia. In the 1990s, he held diplomatic status as a U.S. Arms Control Treaty Inspector. In 2003, he was selected by the United Nations to be a UN weapons of mass destruction inspector in Iraq. Lang currently provides consulting support to the U.S. Intelligence Community and served as a senior instructor in the Master's of Science in Information Assurance Program at Norwich University from 2005 to 2008. Lang is a past commander of Civil Air Patrol's Wyoming Wing and a recipient of the Civil Air Patrol Distinguished Service Medal.

David R. Lease, PhD is the Chief Solution Architect at Computer Sciences Corporation. He has over 30 years of technical and management experience in the information

technology, security, telecommunications, and consulting industries. Lease's recent projects include a $2 billion security architecture redesign for a federal law enforcement agency and the design and implementation of a secure financial management system for an organization operating in 85 countries. Lease is a writer and frequent speaker at conferences for organizations in the intelligence community, Department of Defense, civilian federal agencies, as well as commercial and academic organizations. He is also a peer reviewer of technical research for the IEEE Computer Society. Additionally, Lease is on the faculty of Norwich University and the University of Fairfax, where he teaches graduate-level information assurance courses and supervises doctoral-level research.

Corinne Lefrançois is an Information Assurance Analyst at the National Security Agency. She graduated from Norwich University with a Bachelor of Science in Business Administration and Accounting in 2004 and is a current student in Norwich University's Master of Science in Information Assurance program.

Diane ("Dione") E. Levine, CISSP, CFE, FBCI, CPS, deceased, was the President/CEO of Strategic Systems Management, Ltd., and one of the developers of the Certification for Information Systems Security Professionals. She had a notable career in information security as both a developer and implementer of enterprise security systems. Levine held a series of high-level risk management and security positions in major financial institutions, spent many years as an Adjunct Professor at New York University, and was widely published in both the trade and academic press. She contributed numerous chapters to the Third and Fourth Editions of the *Computer Security Handbook*. Ms. Levine split her time between security and business continuity consulting, writing, and teaching worldwide. She was a frequent public speaker and a member of technical panels and regularly contributed articles and columns to *Information Week, Information Security, Internet Week, Planet IT, ST&D, internet.com* and *Smart Computing*. Levine was Active in the Information Systems Security Association (ISSA), the Association of Certified Fraud Examiners (ASFE), the Business Continuity Institute (BCI), the Contingency Planning Exchange (CPE), and the Information Security Auditing and Control Association (ISACA) and had devoted many years serving on the Board of Directors of these organizations.

James Landon Linderman, PhD (e-mail: *jlinderman@aol.com*) is an Associate Professor in the Computer Information Systems department at Bentley College, Waltham, Massachusetts, where he has taught for 30 years. He is a Research Fellow at Bentley's Center for Business Ethics, and past Vice-Chair of the Faculty Senate. A resident of Fitzwilliam, New Hampshire, Linderman is a Permanent Deacon in the Roman Catholic Diocese of Worcester, Massachusetts, and a consultant in the area of computer-assisted academic scheduling and timetable construction.

Steven Lovaas, MSIA, CISSP, is the Information Technology Security Manager for Colorado State University. His areas of expertise include IT security policy and architecture, communication and teaching of complex technical concepts, and security issues in both K–12 and higher education. He has taught for the MS program in Information Assurance at Norwich University, and is pursuing a PhD in Public Communications and Technology at Colorado State University. Lovaas currently holds the position of Editor in Chief for the Norwich University *Journal of Information Assurance*. As part of his

volunteer commitment to educating the next generation of scientists and engineers, he coaches, judges, and writes exams for the Science Olympiad program in Colorado.

Vic Maconachy, PhD, assumed the position of Vice President for Academic Affairs/ Chief Academic Officer at Capitol College, Laurel, Maryland, in October 2007. Maconachy is charged with sustaining and enhancing the academic quality of programs of study ranging from Business Administration through Engineering, Computer Science, and Information Assurance. He also oversees the operations of the Library and the Space Operations Institute. Maconachy holds the rank of Professor and teaches graduate and undergraduate research courses in information assurance.

Prior to joining Capitol College, Maconachy served at the National Security Agency in several leadership positions. He was appointed by the Director of the NSA as the Deputy Senior Computer Science Authority, where he built a development program for a new generation of Cryptologic Computer Scientists. Prior to this position, Maconachy served as the Director of the National Information Assurance Education and Training Program (www.nsa.gov/ia/academia/acade00001.cfm). He was responsible for implementing a multidimensional, interagency program, providing direct support and guidance to the services, major Department of Defense components, federal agencies, and the greater national information infrastructure community. This program fosters the development and implementation of information assurance training programs as well as graduate and undergraduate education curricula. In this capacity, he served on several national-level government working groups as well as in an advisory capacity to several universities. Maconachy was the principal architect for several national INFOSEC training standards in the national security systems community. During his time at the NSA, he held many different positions, including work as an INFOSEC Operations Officer, INFOSEC Analyst and a Senior INFOSEC Education and Training Officer.

Prior to joining the NSA, Maconachy worked for the Department of Navy. He developed and implemented INFOSEC training programs for users and system maintainers of sophisticated cryptographic equipment. He also served as the Officer in Charge of several INFOSEC-related operations for the Department of Navy, earning him the Department of Navy Distinguished Civilian Service medal. Maconachy holds a PhD from the University of Maryland. He has numerous publications and awards related to information assurance and is the recipient of the prestigious National Cryptologic Meritorious Service Medal.

John Mason is a Manager for SingerLewak's Enterprise Risk Management Group. He has over 20 years of combined experience in internal audit, regulatory compliance, information security, investigations, and process reengineering. He has held senior positions, such as Chief Internal Auditor and Vice President of Audit and Compliance in a variety of companies. While at two multibillion-dollar institutions, he was the Chief Information Security Officer and helped establish information risk management programs as well as designed risk-based audit programs several years before Sarbanes-Oxley. Mason has routinely authored, reviewed, and researched finance control policies and procedures. He has performed audits for governmental agencies and managed a full spectrum of financial, operational, SOX compliance, and data processing audits. He possesses an MBA and numerous certificates, including a CISM, CISA, CFE, CBA, CFSA, and CFSSP and is an Adjunct Professor in Norwich University's Master's of Science in Information Assurance program.

Peter Mell is a senior computer scientist in the Computer Security Division at the National Institute of Standards and Technology. He is the Program Manager for the National Vulnerability Database as well as the Security Content Automation Protocol validation program. These programs are widely adopted within the U.S. government and used for standardizing and automating vulnerability and configuration management, measurement, and policy compliance checking. He has written the NIST publications on patching, malware, intrusion detection, common vulnerability scoring system, and the common vulnerabilities and exposures standard. Mell's research experience includes the areas of intrusion detection systems, vulnerability scoring, and vulnerability databases.

Michael Miora has designed and assessed secure, survivable, highly robust systems for Industry and government over the past 30 years. Miora, one of the original professionals granted the Certified Information Systems Security Professional in the 1990s and the ISSMP in 2004, was accepted as a Fellow of the Business Continuity Institute in 2005. Miora founded and currently serves as President of ContingenZ Corporation. Michael Miora was educated at the University of California, Los Angeles and Berkeley, earning Bachelor's and Master's in Mathematics. He is an Adjunct Professor at Norwich University in the MS Information Assurance program and serves on the editorial boards of the Norwich University *Journal of Information Assurance* and the *Business Continuity Journal*.

Allysa Myers is the Director of Research for West Coast Labs. Her primary responsibilities are researching and analyzing technology and security threat trends as well as reviewing and developing test methodologies. Prior to joining West Coast Labs, Myers spent 10 years working in the Avert group at McAfee Security, Inc. While there, she wrote for the Avert blog and *Sage* magazine, plus several external publications. She also provided training demonstrations to new researchers within McAfee along with other groups such as the Department of Defense and McAfee Technical Support and Anti-Spyware teams. Myers has been a member of various security industry groups, such as the Wildlist and the Drone Armies mailing list.

Scott J. Nathan, Esq. (e-mail: *sjnathan@mindspring.com*) is an attorney whose practice includes litigation concerning intellectual property and technology matters, computer fraud and abuse, and environmental and insurance coverage matters involving the exchange of millions of pages of documents. In addition, he advises clients about, among other things, Internet-related risks and risk avoidance, proprietary and open source software licensing, service-level agreements, and insurance coverage. Nathan has written and spoken extensively about such issues as online privacy, cyberspace jurisdiction, and the legal issues surrounding the use of open source software. He is admitted to practice before the United States Supreme Court, the United States Court of Appeals for the First Circuit, the Federal District Court for the District of Massachusetts, and the Courts of the Commonwealth of Massachusetts. Nathan is a member of the American Bar Association's Litigation and Computer Litigation Committees.

Carl Ness, MS, CISSP, is a Senior Security Analyst for the University of Iowa. Ness has more than 10 years' experience in the information technology and information security fields, mainly in the academic and healthcare sector. He is a speaker, author, and educator on information assurance, including security in the academic environment, messaging security, disaster recovery and business continuity, safe home

computing, and information technology operations. Ness previously served as a systems administrator, network administrator, information technology director, and information security officer. He also provides consulting to several security software development organizations.

Peter G. Neumann has doctorates from Harvard and Darmstadt. He has been in SRI International's Computer Science Lab since September 1971, after spending 10 years at Bell Labs in Murray Hill, New Jersey. His work is concerned with computer systems and networks, trustworthiness and high assurance, security, reliability, survivability, safety, and many risk-related issues, such as voting-system integrity, crypto policy, social implications, and human needs including privacy. He moderates the ACM Risks Forum (risks.org) and created ACM SIGSOFT's Software Engineering Notes in 1976. He has participated in four studies for the National Academies of Science. His 1995 book, *Computer-Related Risks,* is still timely. He is a Fellow of the ACM, IEEE, and AAAS.

Lester E. Nichols earned a BS degree from the University of Phoenix and an MS degree in Information Assurance from Norwich University. He is currently working on his doctoral degree in Information Security at Capella University. He holds the CISSP, MCSA, MCP, and Security+ certifications. Nichols has over 10 years' experience in computer technology in the medical, nonprofit, financial, and local and federal government sectors, in a variety of roles, including application development, network engineering, and information security. Nichols is currently with Knowledge Consulting Group as a Senior Security Engineer, providing security oversight as well as security justification for network and system design implementations, while working with network engineering to integrate security mind-sets to the design stage of projects. Prior to this, he was employed with Prolific Solutions, LLC as a Senior Information Assurance Manager.

Justin Opatrny is currently an information systems manager for a Fortune 500 company, with previous roles specializing in network infrastructure and security. He earned a Master's degree in Information Assurance from Norwich University; holds industry certifications including CISSP, GCFA, and GSNA; and is an active member of ISSA and InfraGard. Opatrny also works as an independent consultant providing technology and information assurance expertise and guidance.

John Orlando, PhD, is the Program Director for the Master of Science in Business Continuity Management at Norwich University. He received his PhD from the University of Wisconsin, and has published articles in a variety of applied ethics fields, including information ethics, business ethics, and medical ethics. He has also published a number of articles on business continuity management and consults with universities on business continuity programs. Orlando helped develop online programs at the University of Vermont and Norwich University, and was the Associate Program Director for the Master of Science in Information Assurance at Norwich University.

Raymond Panko, PhD (e-mail: *Ray@Panko.com*) is a Professor of Information Technology Management in the Shidler College of Business at the University of Hawaii. His interest in security began during lunches with Donn Parker in the 1970s at SRI International and has grown ever since. His textbook on IT security, *Corporate Computer and Network Security,* is published by Prentice-Hall. His current research focuses are

security for end user applications (especially spreadsheets), how to deal with fraud, and human and organizational controls. His main teaching focus, however, remains networking. In his networking classes and textbook, he emphasizes security throughput, pointing out the security implications of network protocols and practices.

Robert A. Parisi, Jr., is the Senior Vice-President and National Technology, Network Risk and Telecommunications Practice Leader for the FINPRO unit of Marsh USA. Parisi has spoken at various businesses, technology, legal, and insurance forums throughout the world and has written on issues affecting professional liability, privacy, technology, telecommunications, media, intellectual property, computer security, and insurance. In 2002, Parisi was honored by *Business Insurance* magazine as one of the Rising Stars of Insurance.

Immediately prior to joining Marsh, Parisi was the Senior Vice-President and Chief Underwriting Officer of eBusiness Risk Solutions (a unit of the property and casualty companies of American International Group, Inc.). Parisi joined the AIG group of companies in 1998 as legal counsel for its Professional Liability group and held several executive and legal positions within AIG, including the position of Chief Underwriting Officer for Professional Liability and Technology. While at AIG, Parisi oversaw the creation and drafting of underwriting guidelines and policies for all lines of professional liability. Prior to joining AIG, Parisi had been in private practice, principally as legal counsel to various Lloyds of London syndicates handling a variety of professional liability lines.

Parisi graduated cum laude from Fordham College with a B.A. in Economics and received his law degree from Fordham University School of Law. He is admitted to practice in New York and the U.S. District Courts for the Eastern and Southern Districts of New York.

Donn B. Parker, CISSP, Fellow of the Association for Computing Machinery (e-mail: *donnlorna@aol.com*) is a retired (1997) senior management consultant who has specialized in information security and computer crime research for 35 of his 50 years in the computer field. He has written numerous books, papers, articles, and reports in his specialty based on interviews with over 200 computer criminals and reviews of the security of many large corporations. He received the 1992 Award for Outstanding Individual Achievement from the Information Systems Security Association, the 1994 National Computer System Security Award from the U.S. NIST/NCSC, the Aerospace Computer Security Associates 1994 Distinguished Lecturer award, and The MIS Training Institute *Infosecurity News* 1996 Lifetime Achievement Award. *Information Security Magazine* identified him as one of the five top Infosecurity Pioneers (1998).

Padgett Peterson, P.E., CISSP, IAM/IEM, has been involved with computer security and encryption for over 40 years. Since 1979 he has been employed by different elements of a major aerospace contractor. Peterson is also an Adjunct Professor in the Master's of Science in Information Assurance program at Norwich University.

Franklin Platt (e-mail: *Fnplatt@aol.com* or telephone: 603 449-2211) is Founder and President of Office Planning Services, a Wall Street consultancy for 20 years headquartered in Stark, New Hampshire since 1990. He has worked extensively in security planning, management, and preparedness in both the private and public sectors. His academic background includes business administration and electrical engineering.

He has received extensive government training in emergency management, including terrorism and weapons of mass destruction, much of which is not available to the public. He holds many security certifications and is currently vetted by the FBI and by several states. Platt's areas of expertise include: security risk management; compliance with the latest Homeland Security procedures and other federal regulations that affect the private sector; risk identification and assessment; vulnerability analysis; cost-value studies; response planning; site security surveys and compliance auditing; briefing and training; second opinion; and due diligence.

Jerrold M. Post, PhD, is Professor of Psychiatry, Political Psychology, and International Affairs and Director of the Political Psychology Program at George Washington University. He has devoted his entire career to the field of political psychology. Post came to George Washington after a 21-year career with the Central Intelligence Agency, where he was the Founding Director of the Center for the Analysis of Personality and Political Behavior. He played the lead role in developing the Camp David profiles of Menachem Begin and Anwar Sadat for President Jimmy Carter and initiated the U.S. government program in understanding the psychology of terrorism. He is a widely published author, whose most recent book is *The Mind of the Terrorist: The Psychology of Terrorists from the IRA to al-Qaeda*. Post is also a frequent commentator on national and international media.

N. Todd Pritsky is the Director of E-learning Courseware at Hill Associates, a telecommunications training company in Colchester, Vermont. He is a Senior Member of the Technical Staff and an instructor of online, lecture, and hands-on classes. His teaching and writing specialties include e-commerce, network security, TCP/IP, and the Internet, and he also leads courses on fast packet and network access technologies. He enjoys writing articles on network security and is a contributing author of *Telecommunications: A Beginner's Guide* (McGraw-Hill/Osborne). Previously he managed a computer center and created multimedia training programs. He holds a BA in Philosophy and Russian/Soviet Studies from Colby College.

Karthik Raman (e-mail: *ramankmail@gmail.com*) is a Research Scientist at McAfee Avert Labs, an internationally renowned research group for fighting malicious software. His work at McAfee focuses on vulnerability research, malware analysis, and security-research automation. His interests include the application of computer and social sciences to computer-security problems and developing security tools. Karthik graduated with BS degrees in Computer Science and Computer Security from Norwich University in 2006, where he studied under Dr. Mich Kabay.

Bridgitt Robertson has been teaching business and technology courses for over six years. Her multidisciplinary approach to security awareness analyzes threats in the global enterprise and investigates how an educated workforce can mitigate risks and enhance corporate competitiveness. Prior to teaching, Robertson worked for global companies in the areas of project management, business analysis, and consulting. She is looking forward to obtaining her doctorate in 2009. She is a member of InfraGard.

Marc Rotenberg is Executive Director of the Electronic Privacy Information Center in Washington, DC. He teaches information privacy law at Georgetown University Law Center. He has published many articles in legal and scientific journals. He is the coauthor of several books, including *Information Privacy Law, Privacy and Human Rights*, *The*

Privacy Law Sourcebook, and *Litigation under the Federal Open Government Laws*. He frequently testifies before the U.S. Congress and the European Parliament on emerging privacy issues. He is a Fellow of the American Bar Foundation and the recipient of several awards, including the World Technology Award in Law.

K. Rudolph, CISSP, is President and Chief Inspiration Officer of Native Intelligence, Inc., a Maryland-based consulting firm focused on providing creative and practical information security awareness solutions. Rudolph develops security awareness products including posters, images, 60-second daily security tips, Web-based and computer-based courses designed in accord with adult-learning principles. She facilitates security awareness peer group meetings and is a frequent speaker at security conferences. In 2006, Rudolph was honored by the Federal Information Security Educators' Association as the Security Educator of the Year. Special areas of interest to Rudolph include storytelling in security awareness and behavior-based messages and metrics.

Eric Salveggio is an information technology security professional who enjoys teaching online courses in CMIS for Liberty University and Auditing for Norwich University. He works as a trained ISO 17799, NSTISSI 4011 and 4013 consultant for Dynetics Corporation of Huntsville, Alabama, in IT Security and Auditing, and as a Private Consultant in networking, network design, and security (wired and wireless) with 10 years experience. He previously worked as the IT Director for the Birmingham, Alabama, campus of Virginia College, where he opened two start-up campuses—on ground and online—and created three accredited programs (two undergrad, one graduate level) at state and federal levels in Network and Cyber Security. While in this position, he was chosen as a nominee for the 2006 Information Security Executive Award, and enjoyed being the only educational facility recognized. He was personally awarded a plaque of recognition by the Stonesoft Corporation for the same. He is a published author and photographer, and enjoys working at times as a Technical Editor for Pearson Education and Thomson Publishing on cyber forensics, cyber security, and operating systems.

Ravi Sandhu is Cofounder and Chief Scientist of SingleSignOn.Net in Reston, Virginia, and Professor of Information Technology and Engineering at George Mason University in Fairfax, Virginia. An ACM and an IEEE Fellow, he is the founding Editor in Chief of *ACM's Transactions on Information and System Security,* Chairman of ACM's Special Interest Group on Security, Audit and Control, and Security Editor for *IEEE Internet Computing*. Sandhu has published over 140 technical papers on information security. He is a popular teacher and has lectured all over the world. He has provided high-level consulting services to numerous private and government organizations.

Sondra Schneider is CEO and Founder of Security University, an Information Security and Information Assurance Training and Certification company. She and SU have challenged security professionals for the past 10 years, delivering hands-on tactical security classes and certifications around the world.

Starting in 2008, SU set up an exam server to meet the demand for tactical security certifications. In 2005, SU refreshed the preexisting AIS security training program to the new "SU Qualified Programs," which meet and exceed security professionals requirements for hands-on tactical security "skills" training. SU delivers the Qualified/Information Security Professional and Qualified/Information Assurance Professional

certifications, which are the first of their kind that measure a candidate's tactical hands-on security skills.

In 2004, Schneider was awarded Entrepreneur of the Year for the First Annual Women of Innovation Award from the Connecticut Technology Council. In 2007, she was Tech Editor for the popular 2007 CEH V5 Study Guide, and a multiple chapter author for the 2007 CHFI Study Guide. She sits on three advisory boards for computer security (start-up) technology companies and is a frequent speaker at computer security and wireless industry events. She is a founding member of the NYC HTCIA and IETF chapters, works closely with $(ISC)^2$, ISSA, and ISACA chapters, and the security and wireless vendor community. She specializes in information security, intrusion detection, information assurance (PKI), wireless security and security awareness training.

William Stallings, PhD (e-mail: *ws@shore.net*) is a consultant, lecturer, and author of over a dozen professional reference books and textbooks on data communications and computer networking. His clients have included major corporations and government agencies in the United States and Europe. He has received numerous awards for the Best Computer Science Textbook of the Year from the Text and Academic Authors Association. He has designed and implemented both TCP/IP-based and OSI-based protocol suites on a variety of computers and operating systems, ranging from microcomputers to mainframes. Stallings created and maintains the Computer Science Student Resource Site at http://WilliamStallings.com/StudentSupport.html.

Peter Stephenson, PhD, is a writer, researcher and lecturer on information assurance and risk, information warfare and counterterrorism, and digital investigation and forensics on large-scale computer networks. He has lectured extensively on digital investigation and security and has written or contributed to 14 books and several hundred articles in major national and international trade, technical and scientific publications.

He is the Associate Program Director in the Master's of Science in Information Assurance program at the Norwich University School of Graduate Studies, where he teaches information assurance, cyber crime and cyber law, and digital investigation on both the graduate and undergraduate levels. He is Senior Research Scientist at the Norwich University Applied Research Institutes, Chair of the Department of Computing, and the Chief Information Security Officer for the university.

He has lectured or delivered consulting engagements for the past 23 years in 11 countries plus the United States and has been a technologist for over 40 years. He operated a successful consulting practice for over 20 years and has worked for such companies as Siemens, Tektronix, and QinetiQ (UK).

Stephenson obtained his PhD in computer science at Oxford Brookes University, Oxford, England, where his research was in the structured investigation of digital incidents in complex computing environments. He holds a Master's of Arts degree in Diplomacy with a concentration in Terrorism from Norwich University.

He is on the editorial advisory boards of *International Journal of Digital Evidence* and the Norwich University *Journal of Information Assurance* among several others. Stephenson is technology editor for *SC Magazine* and the editor in chief for Norwich University Press.

Stephenson is a Fellow of the Institute for Communications, Arbitration and Forensics in the United Kingdom and is a member of Michigan InfraGard and the International Federation of Information Processing Technical Committee 11, Working Group 11.9, Digital Forensics. He serves on the steering Committee of the Michigan Electronic Crime Task Force. His research is focused on information conflict.

Gary L. Tagg is a highly experienced information security professional with over 20 years working in the financial and government sectors. The organizations he has worked with include Deutsche Bank, PA Consulting group, Clearstream, Pearl Assurance, and Lloyds TSB. He has performed a wide range of security roles including risk management, consulting, security architecture, policy and standards, project management, development, testing and auditing. Tagg is currently a risk consultant in Deutsche Bank's IT security Governance Group.

Nicholas Takacs is an information security professional and Business Systems Director for a long-term care insurance company. He is also an Adjunct Professor of Information Assurance at Norwich University. Takacs has expertise in the areas of security policy management, security awareness, business continuity planning, and execution. Prior to moving into the insurance industry, Takacs spent several years in the public utility industry focusing on the areas of regulatory compliance, disaster recovery, and identity management.

James Thomas, MSc CISSP, is a Senior Partner with Norwich Security Associates, a full-spectrum information assurance consultancy headquartered in Scotland. Thomas spends most of his professional time providing policy, process, and governance advice to large banking and financial organizations in the United Kingdom and Europe. He is a 2004 graduate of the Norwich University Master of Science in Information Assurance program. Prior to focusing his efforts in the security space, he had a long career in Information Technology and Broadcast Engineering spanning the United Kingdom and the eastern United States.

Lee Tien, Esq., is a Senior Staff Attorney with the Electronic Frontier Foundation in San Francisco, California. He specializes in free speech and surveillance law and has authored several law review articles. He received his undergraduate degree in psychology from Stanford University and his law degree from Boalt Hall School of Law, UC Berkeley. He is also a former newspaper reporter.

Timothy Virtue is an accomplished information assurance leader with a focus in strategic enterprise technology risk management, information security, data privacy, and regulatory compliance. Virtue has extensive experience with publicly traded corporations, privately held businesses, government agencies, and nonprofit organizations of all sizes. Additionally he holds these professional designations: CISSP, CISA, CCE, CFE, and CIPP/G.

Myles Walsh is an Adjunct Professor at three colleges in New Jersey: Ramapo College, County College of Morris, and Passaic County Community. For the past 12 years, he has taught courses in Microsoft Office and Web Page Design. He also implements small Office applications and Web sites. From 1966 until 1989, he worked his way up from programmer to director in several positions at CBS, CBS Records, and CBS News. His formal education includes an MBA from the Baruch School of Business and a BBA from St. John's University.

Karen F. Worstell, CISM, is Cofounder and Principal of W Risk Group, a consultancy serving clients across multiple sectors to define due diligence to a defensible standard of care for information protection. Her areas of expertise include incident detection and management, compliance, governance, secure data management and risk

management. She is coauthor of *Evaluating the Electronic Discovery Capabilities of Outside Law Firms: A Model Request for Information and Analysis* (BNA, 2006) and is a frequent speaker and contributor in risk management and information security forums internationally. She participates in ISACA, IIA, and the ABA Science and Technology Section, Information Security Committee, and serves as President of the Puget Sound Chapter of the ISSA.

Noel Zakin is President of RANCO Consulting LLC. He has been an information technology/telecommunications industry executive for over 45 years. He has held managerial positions at the Gartner Group, AT&T, the American Institute of CPAs, and Unisys. These positions involved strategic planning, market research, competitive analysis, business analysis, and education and training. His consulting assignments have ranged from the Fortune 500 to small start-ups and have involved data security, strategic planning, conference management, market research, and management of corporate operations. He has been active with ACM, IFIP, and AFIPS and currently with ISSA. He holds an MBA from the Wharton School.

William A. Zucker, Esq., is a partner at McCarter & English, LLP's Boston office. Zucker serves as a senior consultant for the Cutter Consortium on legal issues relating to information technology, outsourcing, and risk management, and is a member of the American Arbitration Association's National Technology Panel and a member of the CPR Institute's working group on technology business alliances and conflict management. He has also served on the faculty of Norwich University, where he taught the intellectual property aspects of computer security. Zucker is a trial lawyer whose practice focuses on negotiation/litigation of business transactions, outsourcing/ebusiness and technology/intellectual property. Among his publications are: "The Legal Framework for Protecting Intellectual Property in the Field of Computing and Computer Software," written for the *Computer Security Handbook*, 4th edition, coauthored with Scott Nathan; and "Intellectual Property and Open Source: Copyright, Copyleft and Other Issues for the Community User."

A NOTE TO INSTRUCTORS

This two-volume text will serve the interests of practitioners and teachers of information assurance. The fourth edition of the *Handbook* was well received in academia; at least one quarter of all copies were bought by university and college bookstores. The design and contents of this fifth edition have been tailored even more closely to meet those needs as well as the needs of other professionals in the field.

University professors looking for texts appropriate for a two-semester sequence of undergraduate courses in information assurance will find the *Handbook* most suitable. In my own work at Norwich University in Vermont, Volume I is the text for our *IS340 Introduction to Information Assurance* and Volume II is the basis for our *IS342 Management of Information Assurance* courses.

The text will also be useful as a resource in graduate courses. In the School of Graduate Studies at Norwich University, we use both volumes as required and supplementary reading for our 18-month, 36-credit Master of Science in Information Assurance program (MSIA).

I will continue to create and post PowerPoint lecture slides based on the chapters of the *Handbook* on my Norwich University Web site for free access by anyone applying them to noncommercial use (e.g., for self-study, for courses in academic institutions, and for unpaid industry training); the materials will be available in the IS340 and IS342 sections:

www2.norwich.edu/mkabay/courses/academic/norwich/is340
www2.norwich.edu/mkabay/courses/academic/norwich/is342

M. E. KABAY
Technical Editor
January 2009

INTRODUCTION TO PART I

FOUNDATIONS OF COMPUTER SECURITY

The foundations of computer security include answers to the superficially simple question "What is this all about?" Our first part establishes a technological and historical context for information assurance so that readers will have a broad understanding of why information assurance matters in the real world. Chapters focus on principles that will underlie the rest of the text: historical perspective on the development of our field; how to conceptualize the goals of information assurance in a well-ordered schema that can be applied universally to all information systems; computer hardware and network elements underlying technical security; history and modern developments in cryptography; and how to discuss breaches of information security using a common technical language so that information can be shared, accumulated, and analyzed.

Readers also learn or review the basics of commonly used mathematical models of information security concepts and how to interpret survey data and, in particular, the pitfalls of self-selection in sampling about crimes. Finally, the first section of the text introduces elements of law (U.S. and international) applying to information assurance. This legal framework from a layman's viewpoint, provides a basis for understanding later chapters; in particular, when examining privacy laws and management's fiduciary responsibilities.

Chapter titles and topics in Part I include:

1. **Brief History and Mission of Information System Security.** An overview focusing primarily on developments in the second half of the twentieth century and the first decade of the twenty-first
2. **History of Computer Crime.** A review of key computer crimes and notorious computer criminals from the 1970s to the mid-2000s
3. **Toward a New Framework for Information Security.** A systematic and thorough conceptual framework and terminology for discussing the nature and goals of securing all aspects of information, not simply the classic triad of confidentiality, integrity, and availability
4. **Hardware Elements of Security.** A review of computer and network hardware underlying discussions of computer and network security

5. **Data Communications and Information Security.** Fundamental principles and terminology of data communications, and their implications for information assurance
6. **Network Topologies, Protocols, and Design.** Information assurance of the communications infrastructure
7. **Encryption.** Historical perspectives on cryptography and steganography from ancient times to today as fundamental tools in securing information
8. **Using a Common Language for Computer Security Incident Information.** An analytic framework for understanding, describing, and discussing security breaches by using a common language of well-defined terms
9. **Mathematical Models of Computer Security.** A review of the most commonly referenced mathematical models used to describe information security functions
10. **Understanding Studies and Surveys of Computer Crime.** Scientific and statistical principles for understanding studies and surveys of computer crime
11. **Fundamentals of Intellectual Property Law.** An introductory review of cyberlaw: laws governing computer-related crime, including contracts, and intellectual property (trade secrets, copyright, patents, open-source-models). Also, violations (piracy, circumvention of technological defenses), computer intrusions, and international frameworks for legal cooperation

CHAPTER 1

BRIEF HISTORY AND MISSION OF INFORMATION SYSTEM SECURITY

Seymour Bosworth and Robert V. Jacobson

1.1 INTRODUCTION TO INFORMATION SYSTEM SECURITY. The growth of computers and of information technology has been explosive. Never before has an entirely new technology been propagated around the world with such speed and with so great a penetration of virtually every human activity. Computers have brought vast benefits to fields as diverse as human genome studies, space exploration, artificial intelligence, and a host of applications from the trivial to the most life-enhancing.

Unfortunately, there is also a dark side to computers: They are used to design and build weapons of mass destruction as well as military aircraft, nuclear submarines,

CHAPTER 2

HISTORY OF COMPUTER CRIME

M. E. Kabay

2.1 WHY STUDY HISTORICAL RECORDS? Every field of study and expertise develops a common body of knowledge that distinguishes professionals from amateurs. One element of that body of knowledge is a shared history of significant events that have shaped the development of the field. Newcomers to the field benefit from learning the names and significant events associated with their field so that they can understand references from more senior people in the profession, and so that they can put new events and patterns into perspective. This chapter provides a brief overview of some of the more famous (or notorious) cases of computer crime (including those targeting computers and those mediated through computers) of the last four decades.[1]

2.2 OVERVIEW. This chapter illustrates several general trends from the 1960s through the decade following 2000:

- In the early decades of modern information technology (IT), computer crimes were largely committed by individual disgruntled and dishonest employees.
- Physical damage to computer systems was a prominent threat until the 1980s.
- Criminals often used authorized access to subvert security systems as they modified data for financial gain or destroyed data for revenge.
- Early attacks on telecommunications systems in the 1960s led to subversion of the long-distance phone systems for amusement and for theft of services.
- As telecommunications technology spread throughout the IT world, hobbyists with criminal tendencies learned to penetrate systems and networks.
- Programmers in the 1980s began writing malicious software, including self-replicating programs, to interfere with personal computers.
- As the Internet increased access to increasing numbers of systems worldwide, criminals used unauthorized access to poorly protected systems for vandalism, political action, and financial gain.
- As the 1990s progressed, financial crime using penetration and subversion of computer systems increased.
- The types of malware shifted during the 1990s, taking advantage of new vulnerabilities and dying out as operating systems were strengthened, only to succumb to new attack vectors.
- Illegitimate applications of e-mail grew rapidly from the mid-1990s onward, generating torrents of unsolicited commercial and fraudulent e-mail.

2.3 1960S AND 1970S: SABOTAGE. Early computer crimes often involved physical damage to computer systems and subversion of the long-distance telephone networks.

CHAPTER 3

TOWARD A NEW FRAMEWORK FOR INFORMATION SECURITY*

Donn B. Parker, CISSP

3.1 PROPOSAL FOR A NEW INFORMATION SECURITY FRAMEWORK.

Information security, historically, has been limited by the lack of a comprehensive, complete, and analytically sound framework for analysis and improvement. The persistence of the classic triad of CIA (confidentiality, integrity, availability) is inadequate to describe what security practitioners include and implement when doing their jobs. We need a new information security framework that is complete, correct, and consistent to express, in practical language, the means for information owners to protect their information from any adversaries and vulnerabilities.

*This chapter is a revised excerpt from Donn B. Parker, *Fighting Computer Crime* (New York: John Wiley & Sons, 1998), Chapter 10, "A New Framework for Information Security," pp. 229–255.

CHAPTER 4

HARDWARE ELEMENTS OF SECURITY

Sy Bosworth and Stephen Cobb

4.1 INTRODUCTION. Computer hardware has always played a major role in computer security. Over the years, that role has increased dramatically, due to both the

CHAPTER 5

DATA COMMUNICATIONS AND INFORMATION SECURITY

Raymond Panko

CHAPTER 6

NETWORK TOPOLOGIES, PROTOCOLS, AND DESIGN

Gary C. Kessler and N. Todd Pritsky

This chapter provides a broad overview of local area network (LAN) concepts, basic terms, standards, and technologies. These topics are important to give the information security professional a better understanding of the terms that might be used to describe a particular network implementation and its products. The chapter also is written with an eye to what information security professionals need to know; for a more complete

CHAPTER 7

ENCRYPTION

Stephen Cobb and Corinne LeFrançois

7.1 INTRODUCTION TO CRYPTOGRAPHY. The ability to transform data so that they are accessible only to authorized persons is just one of the many valuable services performed by the technology commonly referred to as encryption. This technology has appeared in other chapters, but some readers may not be familiar with its principles and origins. The purpose of this chapter is to explain encryption technology in basic terms and to describe its application in areas such as file encryption, message scrambling, authentication, and secure Internet transactions. This is not a theoretical or scientific treatise on encryption, but a practical guide for those who need to employ encryption in a computer security context.

CHAPTER 8

USING A COMMON LANGUAGE FOR COMPUTER SECURITY INCIDENT INFORMATION

John D. Howard

8.1 INTRODUCTION. A computer security *incident* is some set of events that involves an attack or series of attacks at one or more sites. (See Section 8.4.3 for a more formal definition of the term "incident.") Dealing with these incidents is inevitable for individuals and organizations at all levels of computer security. A major part of dealing with these incidents is recording and receiving incident information, which almost always is in the form of relatively unstructured text files. Over time, these files can end up containing a large quantity of very valuable information. Unfortunately, the unstructured form of the information often makes incident information difficult to manage and use.

This chapter presents the results of several efforts over the last few years to develop and propose a method to handle these unstructured, computer security incident records. Specifically, this chapter presents a *tool* designed to help individuals and organizations record, understand, and share computer security incident information. We call the tool the *common language for computer security incident information*. This common language contains two parts:

1. A set of "high-level" incident-related terms
2. A method of classifying incident information (a taxonomy)

CHAPTER 9

MATHEMATICAL MODELS OF COMPUTER SECURITY

Matt Bishop

9.1 WHY MODELS ARE IMPORTANT. When you drive a new car, you look for specific items that will help you control the car: the accelerator, the brake, the shift, and the steering wheel. These exist on all cars and perform the function of speeding the car up, slowing it down, and turning it left and right. This forms a model of the car. With these items properly working, you can make a convincing argument that the model correctly describes what a car must have in order to move and be steered properly.

A model in computer security serves the same purpose. It presents a general description of a computer system (or collection of systems). The model provides a definition of "protect" (e.g., "keep confidential" or "prevent unauthorized change to") and conditions under which the protection is provided. With mathematical models, the conditions can be shown to provide the stated protection. This provides a high degree of assurance that the data and programs are protected, assuming the model is implemented correctly.

CHAPTER 10

UNDERSTANDING STUDIES AND SURVEYS OF COMPUTER CRIME

M. E. Kabay

10.1 INTRODUCTION. This chapter provides guidance for critical reading of research results about computer crime. It will also alert designers of research instruments who may lack formal training in survey design and analysis to the need for professional support in developing questionnaires and analyzing results.

10.1.1 Value of Statistical Knowledge Base. Security specialists are often asked about computer crime; for example, customers want to know who is attacking which systems, how often, using what methods. These questions are perceived as important because they bear on the strategies of risk management; in theory, in order to estimate the appropriate level of investment in security, it would be helpful to have a sound grasp of the probability of different levels of damage. Ideally, one would want to evaluate an organization's level of risk by evaluating the experiences of other organizations with similar system and business characteristics. Such comparisons would be useful in competitive analysis and in litigation over standards of due care and diligence in protecting corporate assets.

10.1.2 Limitations on Our Knowledge of Computer Crime. Unfortunately, in the current state of information security, no one can give reliable answers to such questions. There are two fundamental difficulties preventing us from

CHAPTER 11

FUNDAMENTALS OF INTELLECTUAL PROPERTY LAW

William A. Zucker and Scott J. Nathan

11.1 INTRODUCTION. This chapter is not for lawyers or law students. Rather, it is written for computer professionals who might find it useful to understand how their concerns at work fit into a legal framework, and how that framework shapes strategies that they might employ in their work. It is not intended to be definitive but to help readers spot issues when they arise and to impart an understanding that is the first part of a fully integrated computer security program.

The word "cyberlaw" is really a misnomer. Cyberlaw is a compendium of traditional law that has been updated and applied to new technologies. When gaps have developed or traditional law is inadequate, particular statutes have been enacted. It is a little like the old story of the three blind men and the elephant: One of the blind men touching the elephant's leg believes he is touching a tree; the other touching its ear believes it is a wing, and the third, touching the tail, thinks it is a snake. Issues of cyberspace, electronic data, networks, global transmissions, and positioning have neither simple unitary solutions nor a simple body of law to consult.

INTRODUCTION TO PART II

THREATS AND VULNERABILITIES

What are the practical, technical problems faced by security practitioners? Readers are introduced to what is known about the psychological profiles of computer criminals and employees who commit insider crime. The focus is then widened to look at national security issues involving information assurance—critical infrastructure protection in particular. After a systematic review of how criminals penetrate security perimeters—essential for developing proper defensive mechanisms—readers can study a variety of programmatic attacks (widely used by criminals) and methods of deception, such as social engineering. The section ends with a review of widespread problems such as spam, phishing, Trojans, Web-server security problems, and physical facility vulnerabilities (an important concern for security specialists, but one that is often overlooked by computer-oriented personnel).

The chapter titles and topics in Part II include:

12. **The Psychology of Computer Criminals.** Psychological insights into motivations and behavioral disorders of criminal hackers and virus writers
13. **The Dangerous Technology Insider: Psychological Characteristics and Career Patterns.** Identifying potential risks among employees and other authorized personnel
14. **Information Warfare.** Cyberconflict and protection of national infrastructures
15. **Penetrating Computer Systems and Networks.** Widely used penetration techniques for breaching security perimeters
16. **Malicious Code.** Dangerous computer programs, including viruses and worms
17. **Mobile Code.** Analysis of applets, controls, scripts and other small programs, including those written in activeX, Java, and Javascript
18. **Denial-of-Service Attacks.** Resource saturation and outright sabotage that brings down availability of systems
19. **Social Engineering and Low-Tech Attacks.** Lying, cheating, impersonation, intimidation—and countermeasures to strengthen organizations against such attacks

20. **Spam, Phishing, and Trojans: Attacks Meant to Fool.** Fighting spam, phishing, and Trojans
21. **Web-Based Vulnerabilities.** Web servers, and how to strengthen their defenses
22. **Physical Threats to the Information Infrastructure.** Attacks against the information infrastructure, including buildings and network media

CHAPTER 12

THE PSYCHOLOGY OF COMPUTER CRIMINALS

Q. Campbell and David M. Kennedy

12.1 INTRODUCTION. In modern society, it is virtually impossible to go through the day without using computers to assist us in our various tasks and roles. We use computers extensively in both our professional and personal lives. We rely on them to interact with coworkers and associates, to regulate the climate in our homes, to operate our automobiles, to update our finances, and even to monitor and protect our loved ones. However, this ever-increasing reliance on technology comes at a cost. As we become more dependent on information technology, we are also becoming increasingly vulnerable to attacks and exploitation by computer criminals.

CHAPTER 13

THE DANGEROUS INFORMATION TECHNOLOGY INSIDER: PSYCHOLOGICAL CHARACTERISTICS AND CAREER PATTERNS[1]

Jerrold M. Post

13.1 COMPUTER INFORMATION TECHNOLOGY INSIDERS. In the complex world of information technology, it is people who create the systems and it is people with authorized access, the computer information technology insiders (CITIs), who represent the greatest threat to these systems.

Computer security experts have developed ever more sophisticated technological solutions to protect sensitive information and combat computer fraud. But no matter how sensitive the computer intrusion detection devices, no matter how impenetrable the firewalls, they will be of no avail in countering the malicious insider.

In considering the population of authorized insiders, it is clear just how broad and variegated this category is and that the line between insiders and outsiders is often blurred.

CITIs include:

- Staff employees
- Contractors and consultants
- Partners and customers

CHAPTER 14

INFORMATION WARFARE

Seymour Bosworth

Information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries.

—Dr. Ivan Goldberg, Institute for Advanced Study of Information Warfare

CHAPTER 15

PENETRATING COMPUTER SYSTEMS AND NETWORKS

Chey Cobb, Stephen Cobb, and M. E. Kabay

15.1 MULTIPLE FACTORS INVOLVED IN SYSTEM PENETRATION. Although penetrating computer systems and networks may sound like a technical challenge, most information security professionals are aware that systems security has both technical and nontechnical aspects. Both aspects come into play when people attempt to penetrate systems. Both aspects are addressed in this chapter, which is not a handbook on how to penetrate systems but rather a review of the methods and means by which systems penetrations are accomplished.

15.1.1 System Security: More than a Technical Issue. The primary nontechnical factor in system security and resistance to system penetration is human

CHAPTER 16

MALICIOUS CODE

Robert Guess and Eric Salveggio

16.1 INTRODUCTION. Malicious logic (or code) is "hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose."[1] In this chapter, we enumerate the common types of malicious code, sources of malicious code, methods of malicious code replication, and methods of malicious code detection.

Common types of malicious code include viruses, worms, Trojan horses, spyware, rootkits, and bots. Emerging malicious code threats include kleptographic code, cryptoviruses, and hardware-based rootkits. Present-day malicious code threats do not always fit into neat categories, resulting in confusion when discussing the topic. It is not possible to classify all code as being *good* code or *malicious* code. Absent the *mens rea*, or criminal intent of the author or user, code is neither good nor bad. Authors develop code to achieve some goal or fulfill some purpose just as users run code to

CHAPTER 17

MOBILE CODE

Robert Gezelter

17.1 INTRODUCTION. At its most basic, mobile code is a set of instructions that are delivered to a remote computer for dynamic execution. The problems with mobile code stem from its ability to do more than just display characters on the remote display.

It is this dynamic nature of mobile code that causes policy and implementation difficulties. A blanket prohibition on mobile code is secure, but that prohibition would prevent users of the dynamic Web from performing their tasks. It is this tension between integrity and dynamism that is at the heart of the issue.

The ongoing development of computer-based devices, particularly personal digital assistants (PDAs) and mobile phones, has broadened the spectrum of devices that use mobile code, and therefore are vulnerable to related exploits. The advent of the Apple iPhone in 2007 highlighted this hazard.[1]

Several definitions, as used by United States military forces but applicable to all, are useful in considering the content of this chapter:

> **Enclave.** An information system environment that is end to end under the control of a single authority and has a uniform security policy, including personnel and physical security. Local and remote elements that access resources within an enclave must satisfy the policy of the enclave.

CHAPTER 18

DENIAL-OF-SERVICE ATTACKS

Gary C. Kessler and Diane E. Levine

18.1 INTRODUCTION. This chapter discusses denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. These attacks seek to render target systems and networks unusable or inaccessible by saturating resources or causing catastrophic errors that halt processes or entire systems. Furthermore, they are increasingly easy for even *script kiddies* (persons who follow explicit attack instructions or execute attack programs) to launch. Successful defense against these attacks will come only when there is widespread cooperation among all Internet service providers (ISPs) and other Internet-connected systems worldwide.

Working in a variety of ways, the DoS attacker selects an intended target system and launches a concentrated attack against it. Although initially deemed to be primarily a "nuisance," DoS attacks can incapacitate an entire network, especially those with hosts that rely on Transmission Control Protocol/Internet Protocol (TCP/IP). DoS attacks on corporate networks and ISPs have resulted in significant damage to productivity and revenues. DoS attacks can be launched against any hardware or operating system

CHAPTER 19

SOCIAL ENGINEERING AND LOW-TECH ATTACKS

Karthik Raman, Susan Baumes, Kevin Beets, and Carl Ness

CHAPTER 20

SPAM, PHISHING, AND TROJANS: ATTACKS MEANT TO FOOL

Stephen Cobb

20.1 UNWANTED E-MAIL AND OTHER PESTS: A SECURITY ISSUE.

Three oddly named threats to computer security are addressed in this chapter: spam, phishing, and Trojan code. Spam is unsolicited commercial e-mail. Phishing is the use of deceptive unsolicited e-mail to obtain—to fish electronically for—confidential information. Trojan code, a term derived from the Trojan horse, is software designed to achieve unauthorized access to systems by posing as legitimate applications. In this

CHAPTER 21

WEB-BASED VULNERABILITIES

Anup K. Ghosh, Kurt Baumgarten, Jennifer Hadley, and Steven Lovaas

21.1 INTRODUCTION. This chapter systematically reviews the primary software components that make up Web applications, with a primary focus on e-commerce, and provides an overview of the risks to each of these components.[1] The goal of this chapter is to point out that every system will have risks to its security and privacy that need to be systematically analyzed and ultimately addressed.

21.2 BREAKING E-COMMERCE SYSTEMS. To make a system more secure, it may be advisable to break it. Finding the vulnerabilities in a system is necessary in order to strengthen it, but breaking an e-commerce system requires a different mind-set from that of the programmers who developed it. Instead of thinking about developing within a specification, a criminal or hacker looks outside the specifications.

Hackers believe that rules exist only to be broken, and they always use a system in unexpected ways. In doing so, they usually follow the path of least resistance. Those areas perceived to provide the strongest security, or the most resistance to hacking, will likely be ignored. For example, if a system uses Secure Sockets Layer (SSL) to encrypt Web sessions between Web clients and the Web server, a hacker will not try to

CHAPTER 22

PHYSICAL THREATS TO THE INFORMATION INFRASTRUCTURE

Franklin Platt

INTRODUCTION TO PART III

PREVENTION: TECHNICAL DEFENSES

The threats and vulnerabilities described in Part II can be met in part by effective use of technical countermeasures.

The chapter titles and topics in this part include:

23. **Protecting the Information Infrastructure.** Facilities security and emergency management
24. **Operating System Security.** Fundamentals of operating-systems security, including security kernels, privilege levels, access control lists, and memory partitions
25. **Local Area Networks.** Security for local area networks, including principles and platform-specific tools
26. **Gateway Security Devices.** Effective recommendations for implementing firewalls and proxy servers
27. **Intrusion Detection and Intrusion Prevention Devices.** Critical elements of security management for measuring attack frequencies outside and inside the perimeter and for reducing successful penetrations
28. **Identification and Authentication.** What one knows, what one has, what one is, and what one does
29. **Biometric Authentication.** Special focus on who one is and what one does as markers of identity
30. **E-Commerce and Web Server Safeguards.** Technological and legal measures underlying secure e-commerce and a systematic approach to developing and implementing security services
31. **Web Monitoring and Content Filtering.** Tools for security management within the perimeter
32. **Virtual Private Networks and Secure Remote Access.** Encrypted channels (virtual private networks) for secure communication, and approaches for safe remote access
33. **802.11 Wireless LAN Security.** Protecting increasingly pervasive wireless networks

34. **Securing VoIP.** Security measures for Voice over IP telephony
35. **Securing P2P, IM, SMS, and Collaboration Tools.** Securing collaboration tools such as peer-to-peer networks, instant messaging, text messaging services, and other mechanisms to reduce physical travel, and to facititate communications
36. **Securing Stored Data.** Managing encryption and efficient storage of stored data
37. **PKI and Certificate Authorities.** Concepts, terminology, and applications of the Public Key Infrastructure for asymmetric encryption
38. **Writing Secure Code.** Guidelines for writing robust program code that includes few bugs, and that can successfully resist deliberate attacks
39. **Software Development and Quality Assurance.** Using quality assurance and testing to underpin security in the development phase of programs
40. **Managing Software Patches and Vulnerabilities.** Rational deployment of software patches
41. **Antivirus Technology.** Methods for fighting malicious code
42. **Protecting Digital Rights: Technical Approaches.** Methods for safeguarding intellectual property such as programs, music, and video that must by its nature be shared to be useful

CHAPTER 23

PROTECTING THE INFORMATION INFRASTRUCTURE

Franklin Platt

23.1 INTRODUCTION.

There are three steps necessary to protect the information infrastructure properly. The first step is to establish uniform and comprehensive policies and procedures for security planning, implementation, and management. The second step is to review the facilities design factors and security defenses needed to protect the information infrastructure as well as the people who use it. The third step is a cost-benefit analysis to determine which of the security defenses derived from steps 1 and 2 will be the most cost effective. Once all possible threat situations have been identified and assessed as described in Chapter 22, this chapter covers the remaining steps necessary to implement good security protection.

A uniform and comprehensive process for good security planning and management is no longer optional or accidental. Today, anything less than good security is likely to cost any organization dearly. And even more important today is that good security now requires compliance with many new federal laws, regulations, and directives, if only to ensure good risk management and to circumvent unnecessary and potentially costly allegations of negligence. Once insurance was enough to cover most threat situations.

CHAPTER 24

OPERATING SYSTEM SECURITY

William Stallings

24.1 INFORMATION PROTECTION AND SECURITY. This chapter reviews the principles of security in operating systems. Some general-purpose tools can be built into computers and operating systems (OSs) that support a variety of protection and security mechanisms. In general, the concern is with the problem of controlling access to computer systems and the information stored in them. Four types of overall protection policies, of increasing order of difficulty, have been identified:

1. **No sharing.** In this case, processes are completely isolated from each other, and each process has exclusive control over the resources statically or dynamically assigned to it. With this policy, processes often "share" a program or data file by making a copy of it and transferring the copy into their own virtual memory.
2. **Sharing originals of program or data files.** With the use of reentrant code, a single physical realization of a program can appear in multiple virtual address spaces, as can read-only data files. Special locking mechanisms are required for

CHAPTER 25

LOCAL AREA NETWORKS

Gary C. Kessler and N. Todd Pritsky

25.1 INTRODUCTION. This chapter discusses generic issues surrounding local area network (LAN) security. Securing the LAN is essential to securing the Internet because LANs are where most of the attackers, victims, clients, servers, firewalls, routers, and other devices reside. Compromised LAN systems on the Internet open other nodes on that local network to attack and put other systems at risk on the Internet as a whole. Many of the general issues mentioned herein are described in more specific terms in other chapters of this *Handbook,* such as Chapters 15, 22, 23, and 47 in particular.

25.2 POLICY AND PROCEDURE ISSUES. Twenty years ago, all users had accounts on a shared mainframe or minicomputer. A single system manager was responsible for security, backup, disaster recovery, account management, policies, and all other related issues. Today all users are system managers, and, in many cases, individuals have responsibility for several systems. Since the vulnerability of a single computer can compromise the entire LAN, it is imperative that there be rules in place so that everyone can work together for mutual efficiency and defense. But where polices and procedures can be centralized, they should be, because most users do not take the security procedures seriously enough.

The next list, modified from the Internet Engineering Task Force (IETF) Request for Comment (RFC) 2196, is a rough outline of LAN-related security policies and procedures that should at least be considered.[1]

CHAPTER 26

GATEWAY SECURITY DEVICES

David Brussin and Justin Opatrny

26.1 INTRODUCTION. The firewall has come to represent both the concept and the realization of network and Internet security protections. Due to its rapid acceptance and evolution, the firewall has become the most visible of security technology throughout the enterprise chain of command. In distinct contrast with virtually any other single piece of technology, there is not likely to be a chief executive officer in this country who cannot say a word or two about how firewalls are used to protect enterprise systems and data.

The firewall, as originally devised, was intended to allow certain explicitly authorized communications between networks while denying all others. This approach centralizes much of the responsibility for the security of a protected network at the firewall component while distributing some responsibility to the components handling the authorized communications with outside networks. The centralized responsibility

CHAPTER 27

INTRUSION DETECTION AND INTRUSION PREVENTION DEVICES

Rebecca Gurley Bace

CHAPTER 28

IDENTIFICATION AND AUTHENTICATION

Ravi Sandhu, Jennifer Hadley, Steven Lovaas, and Nicholas Takacs

28.1 INTRODUCTION. *Authorization* is the allocation of permissions for specific types of access to restricted information. In the real world, authorization is conferred on real human beings; in contrast, information technology normally

CHAPTER 29

BIOMETRIC AUTHENTICATION

David R. Lease, Robert Guess, Steven Lovaas, and Eric Salveggio

CHAPTER 30

E-COMMERCE AND WEB SERVER SAFEGUARDS

Robert Gezelter

30.1 INTRODUCTION. Today, electronic commerce involves the entire enterprise. While the most obvious e-commerce applications involve business transactions with outside customers on the World Wide Web (WWW or Web), they are merely the proverbial tip of the iceberg. The presence of e-commerce has become far more pervasive, often involving the entire logistical and financial supply chains that are the foundations of modern commerce. Even the smallest organizations now rely on the Web for access to services and information.

The pervasive desire to improve efficiency often causes a convergence between the systems supporting conventional operations with those supporting the organization's online business. It is thus common for internal systems at bricks-and-mortar stores to utilize the same back-office systems as are used by Web customers. It is also common for kiosks and cash registers to use wireless networks to establish connections back to internal systems. These interconnections have the potential to provide intruders with access directly into the heart of the enterprise.

The TJX case, which came to public attention in the beginning of 2007, was one of a series of large-scale compromises of electronically stored information on back-office and e-commerce systems. Most notably, the TJX case appears to have started with an insufficiently secured corporate network and the associated back-office systems, not a Web site penetration. This breach escalated into a security breach of corporate data systems. It has been reported that at least 94 million credit cards were compromised.[1] On November 30, 2007, it was reported that TJX, the parent organization of stores including TJ Maxx and Marshall's, agreed to settle bank claims related to VISA cards for US$ 40.9M.[2]

E-commerce has now come of age, giving rise to fiduciary risks that are important to senior management and to the board of directors. The security of data networks, both those used by customers and those used internally, now has reached the level where it significantly affects the bottom line. TJX has suffered both monetarily and in public relations, with stories concerning the details of this case appearing in the *Wall Street Journal*, the *New York Times*, *Business Week*, and many industry trade publications. Data security is no longer an abstract issue of concern only to technology personnel. The legal settlements are far in excess of the costs directly associated with curing the technical problem.

Protecting e-commerce information requires a multifaceted approach, involving business policies and strategies as well as the technical issues more familiar to information security professionals.

Throughout the enterprise, people and information are physically safeguarded. Even the smallest organizations have a locked door and a receptionist to keep outsiders from entering the premises. The larger the organization, the more elaborate

CHAPTER 31

WEB MONITORING AND CONTENT FILTERING

Steven Lovaas

31.1 INTRODUCTION. The Internet has been called a cesspool, sometimes in reference to the number of virus-infected and hacker-controlled machines, but more often in reference to the amount of objectionable content available at a click of the mouse. This chapter deals with efforts to monitor and control access to some of this content. Applications that perform this kind of activity are controversial: Privacy and free-speech advocates regularly refer to "censorware," while the writers of such software tend to use the term "content filtering." This chapter uses "content filtering," without meaning to take a side in the argument by so doing. For more on the policy and legal issues surrounding Web monitoring and content filtering, see Chapters 48 and 72 in this *Handbook*.

This chapter briefly discusses the possible motivations leading to the decision to filter content, without debating the legitimacy of these motives. Given the variety of

CHAPTER 32

VIRTUAL PRIVATE NETWORKS AND SECURE REMOTE ACCESS

Justin Opatrny

32.1 INTRODUCTION. The rise of the Internet created a new chapter in human civilization. People are no longer tied to static information sources such as libraries. The seemingly exponential growth of people looking to access wide varieties of content also spurred the desire for mobility. If a person can search for information residing halfway around the world from home, why not be able to do the same from the local coffee shop or while sitting at an airport during a business trip? This information revolution offered an opportunity to provide information and services to consumers, businesses, and employees at virtually any point on the globe.

32.1.1 Borders Dissolving. Prolific Internet access redefined the dynamics of network and perimeter protections. Previously, companies needed to focus on protecting the internal network as well as systems exposed to the Internet. A perimeter firewall was sufficient to keep the digital predators at bay. The greater challenge then became how to maintain the security of the internal network when employees use mobile technologies from home or while traveling. Further complicating the issue is how to allow other business partners to access the systems and information that require protection.

CHAPTER 33

802.11 WIRELESS LAN SECURITY

Gary L. Tagg

33.1 INTRODUCTION. Corporations and home users have mass adopted IEEE 802.11 as the protocol for wireless local area networks. These networks have benefits over traditional wired networks, such as mobility, flexibility, rapid deployment, and cost reduction. However, as with any networking technology, it creates new opportunities for unauthorized individuals to access the networks and the information carried over them.

The purpose of this chapter is to introduce wireless LAN technologies, the issues, and ways to address them. Reasons driving the adoption of wireless LANs derive from:

- The 802.11 architecture and product types
- The threats to information presented by wireless LAN technology, and how they compare to other networking threats, such as the Internet
- The security functionality provided by the original 802.11 standard, the security weaknesses, and how to mitigate them
- The security functionality provided by the 802.11i security standard, which was developed to address issues with the original standards

CHAPTER 34

SECURING VOIP

Christopher Dantos and John Mason

34.1 INTRODUCTION. Whether it is referred to as Voice over Internet Protocol (VoIP) or Internet Protocol Telephony (IPT), the digitization of voice messaging has had and will continue to have an impact on society. Voice messaging is part of a shift that some are calling the Unified Messaging System (UMS).[1] The future does not include separate applications for instant messaging, text messaging, voice communications, video conferencing, e-mail, and network presence. These are expected to become one application that will be shared by both the home user and large corporations. New technologies promise to empower users as never before by freeing our communications from geographically stationary limits. For example, users can decide to work from home and have their office telephones ring into their laptops. Aside from convenience and

CHAPTER 35

SECURING P2P, IM, SMS, AND COLLABORATION TOOLS

Carl Ness

35.1 INTRODUCTION. Peer-to-peer (P2P) communications, instant messaging (IM), short message services (SMS), and collaboration tools must be directly addressed in any comprehensive security plan. The dangers are very real, as is the probability that at least one of these technologies is in use on almost every information system.

35.2 GENERAL CONCEPTS AND DEFINITIONS. This chapter is designed to present enough information and resources to aid in integrating the defense of each function into the organization's security plan. A list of resources is provided at the end of the chapter to aid in further research.

CHAPTER 36

SECURING STORED DATA

David J. Johnson, Nicholas Takacs, and Jennifer Hadley

36.1 INTRODUCTION TO SECURING STORED DATA. This chapter reviews methods of securing data stored on nonvolatile media. Nonvolatile media include magnetic disks and their (hard) drives, compact discs (CDs), and digital video disks (DVDs) with their optical drives, and flash drives (also known as USB drives, flash disks, and memory keys). Volatile storage devices, which are not covered in this

CHAPTER 37

PKI AND CERTIFICATE AUTHORITIES

Santosh Chokhani, Padgett Peterson, and Steven Lovaas

CHAPTER 38

WRITING SECURE CODE

Lester E. Nichols, M. E. Kabay, and Timothy Braithwaite

38.1 INTRODUCTION. The topic of secure coding cannot be adequately addressed in a single chapter. Unfortunately, programs are inherently difficult to secure because of the large number of ways that execution can traverse the code as a result of different input sequences and data values.

This chapter provides a starting point and additional resources for security professionals, system architects, and developers to build a successful and secure development methodology. Writing secure code takes coordination and cooperation of various functional areas within an organization, and may require fundamental changes in the way software development currently is designed, written, tested, and implemented.

38.2 POLICY AND MANAGEMENT ISSUES. There are countless security hurdles facing those writing code and developing software. Today dependence on the reliability and security of the automated system is nearly total. For an increasing number of organizations, distributed information processes, implemented via networked environments, have become the critical operating element of their business. Not only must the processing system work when needed, but the information processed must

CHAPTER 39

SOFTWARE DEVELOPMENT AND QUALITY ASSURANCE

Diane E. Levine, John Mason, and Jennifer Hadley

CHAPTER 40

MANAGING SOFTWARE PATCHES AND VULNERABILITIES

Peter Mell and Karen Kent

40.1 INTRODUCTION. *Vulnerabilities* are flaws that can be exploited by a malicious entity to gain greater access or privileges than it is authorized to have on a computer system. *Patches* are additional pieces of code developed to address problems (commonly called "bugs") in software. Patches enable additional functionality, or they address security flaws such as vulnerabilities within a program. Not all vulnerabilities have related patches, especially when new vulnerabilities are first announced, so system administrators must be aware not only of applicable vulnerabilities and

CHAPTER 41

ANTIVIRUS TECHNOLOGY

Chey Cobb and Allysa Myers

41.1 INTRODUCTION. For over two decades, computer viruses have been a persistent, annoying, and costly threat, and there is no end in sight to the problem. There are many vendors offering to provide a cure for viruses and malware, but the mere existence of these software pests is understandably vexing to those charged with system security.

Initially, most viruses were not designed to cause harm but were created more to gain notoriety for the creator or as a prank. Because these early viruses were designed to subvert legitimate program operations across multiple systems, they were more likely to cause unexpected problems. These viruses, and later some Trojans, often damaged data and caused system downtime. The cleanup required to recover from even a minor virus infection was expensive in terms of lost productivity and unbudgeted labor costs.

Viruses and Trojan behavior have merged, and now both are considered as part of the larger family referred to as malware. No longer is malware just written for a virus writer's 15 minutes of fame; today, malware is created primarily for financial gain. Malware can still cause damage, but now it is more likely to have been created to

CHAPTER 42

PROTECTING DIGITAL RIGHTS: TECHNICAL APPROACHES

Robert Guess, Jennifer Hadley, Steven Lovaas, and Diane E. Levine

42.1 INTRODUCTION. Ever since publishing and commerce were introduced to the digital world, the risks to intellectual property and to personal privacy in cyberspace have steadily escalated on comparable but separate paths. These paths have now converged. Unfortunately, many times, antipiracy efforts lead to possible breaches in personal privacy.

Efforts to stem the flow of pirated software worldwide remain mediocre in efficacy; piracy is still proving to be big business in the new millennium. According to the Business Software Alliance (BSA), a 2006 study shows that "thirty-five percent of the packaged software installed on personal computers (PC) worldwide in 2005 was illegal, amounting to $34 billion in global losses due to software piracy."[1] This single-year loss equals 57 percent of the total for years 1995 to 2000 combined. Although the methods

INTRODUCTION TO PART IV

PREVENTION: HUMAN FACTORS

Human factors underlie all the mechanisms invented by technical experts. Without human awareness, training, education, and motivation, technical defenses inevitably fail. This part details a number of valuable areas of knowledge for security practitioners, including these chapters and topics:

43. **Ethical Decision Making and High Technology.** A strategy for setting a high priority on ethical behavior and a framework for making ethical decisions
44. **Security Policy Guidelines.** Guidelines for how to express security policies effectively
45. **Employment Practices and Policies.** Policy guidelines on hiring, managing, and firing employees
46. **Vulnerability Assessment.** Methods for smoothly integrating vulnerability assessments into the corporate culture
47. **Operations Security and Production Controls.** Running computer operations securely, and controlling production for service levels and quality
48. **E-Mail and Internet Use Policies.** Guidelines for setting expectations about employee use of the Web and e-mail at work
49. **Implementing a Security Awareness Program.** Methods for ensuring that all employees are aware of security requirements and policies
50. **Using Social Psychology to Implement Security Policies.** Drawing on the science of social psychology for effective implementation of security policies
51. **Security Standards for Products.** Established standards for evaluating the trustworthiness and effectiveness of security products

CHAPTER 43

ETHICAL DECISION MAKING AND HIGH TECHNOLOGY

James Landon Linderman

43.1 INTRODUCTION: THE ABCs OF COMPUTER ETHICS

43.1.1 Why an Ethics Chapter in a Computer Security Handbook?

In an information age, many potential misuses and abuses of information create privacy and security problems. In addition to possible legal issues, ethical issues affect many groups and individuals—including employees and customers, vendors, consultants, bankers, and stockholders—who have enough at stake in the matter to confront and even destroy an organization over ethical lapses. As is so often the case, consciousness raising is at the heart of maintaining control.

CHAPTER 44

SECURITY POLICY GUIDELINES

M. E. Kabay and Bridgitt Robertson

44.1 INTRODUCTION. This chapter reviews principles, topics, and resources for creating effective security policies. It does not propose specific guidelines except as examples. Many of the chapters in this *Handbook* discuss policy; a few examples are listed next:

Chapter 23 provides an extensive overview of physical security policies.

Chapter 25 discusses local area network security issues and policies.

Chapter 38 reviews software development policies.

Chapter 39 surveys quality assurance policies.

Chapter 45 provides guidance on employment policies from a security standpoint.

CHAPTER 45

EMPLOYMENT PRACTICES AND POLICIES

M. E. Kabay and Bridgitt Robertson

45.1 INTRODUCTION. Crime is a human issue, not merely a technological one. True, technology can reduce the incidence of computer crimes, but the fundamental problem is that people can be tempted to take advantage of flaws in our information systems. The most spectacular biometric access control in the world will not stop someone from getting into the computer room if the janitor believes it is "just to pick up a listing."

People are the key to effective information security, and disaffected employees and angry ex-employees are important threats according to many current studies. For example, the 2007 CSI Computer Crime and Security Survey, published by the Computer Security Institute, reported on responses from 494 participants in a wide range of industries, nonprofits and government agencies; the authors stated:

> Insider abuse of network access or e-mail (such as trafficking in pornography or pirated software) edged out virus incidents as the most prevalent security problem, with 59 and 52 percent of respondents reporting each respectively.[1]

The same report indicated that about 64 percent of the respondents believed that insiders accounted for at least some of their cybercrime losses:

CHAPTER 46

VULNERABILITY ASSESSMENT

Rebecca Gurley Bace

46.1 SCOREKEEPER OF SECURITY MANAGEMENT. Information security has, over time, evolved from a collection of esoteric security issues and technical remedies to its current state, in which it is more tightly integrated with the area of enterprise risk management. One effect of this move from technology to management discipline is the growth in the deployment and use of vulnerability management (and its primary technical constituent, vulnerability assessment [VA]) systems. These systems are considered fundamental to modern information security practice and have matured in architecture, features, and interfaces to accommodate the changing landscape of modern enterprises.

46.1.1 What Is Vulnerability Management? Vulnerability management is a process of assessing deployed IT systems in order to determine the security state of the system. It includes the determination of corrective measures to mitigate issues identified that represent exposures for the enterprise, and managing the application of those measures. Vulnerability assessment is the key technology component of vulnerability management. However, there is a synergy between VA and the other elements of

CHAPTER 47

OPERATIONS SECURITY AND PRODUCTION CONTROLS

M. E. Kabay, Don Holden, and Myles Walsh

47.1 INTRODUCTION. Despite the enormous increase in individual computing on personal computers and workstations in the years since the first edition of this *Handbook* was published in 1975, many mainframe computers and their networks are

CHAPTER 48

E-MAIL AND INTERNET USE POLICIES

M. E. Kabay and Nicholas Takacs

CHAPTER 49

IMPLEMENTING A SECURITY AWARENESS PROGRAM

K. Rudolph

49.1 INTRODUCTION. Even the best security process will fail when implemented by the uninformed. Information technology security awareness is achieved when people know what is going on around them, can recognize potential security violations or suspicious circumstances, and know what initial actions to take. Security awareness is the result of activities, tools, and techniques intended to attract people's attention and to help them focus on security. Because people play an integral role in protecting an organization's assets, security awareness among staff, contractors, partners, and customers is a necessary and cost-effective countermeasure against security breaches. Effective awareness programs motivate people and provide measurable benefits. Prerequisites for implementing a security awareness program successfully include senior-level management support, an in-place security policy, measurable goals, and a plan for reaching those goals. Attention-getting awareness materials tailored to the audience and to the technology yield maximum program impact. This chapter contains practical information on design approaches for an awareness program, including its content, techniques, principles, tools, measurement approaches, and evaluation techniques.

49.2 AWARENESS AS A SURVIVAL TECHNIQUE. In recent years, awareness of security concerns worldwide has increased. Business, government organizations, and individuals are conducting a significant part of their activities electronically. Electronic information (corporate and personal data) often can be easily accessed,

CHAPTER 50

USING SOCIAL PSYCHOLOGY TO IMPLEMENT SECURITY POLICIES

M. E. Kabay, Bridgitt Robertson, Mani Akella, and D. T. Lang

50.1 INTRODUCTION[1]. Most security personnel have commiserated with colleagues about the difficulty of getting people to pay attention to security policies—to comply with what seems like good common sense. They shake their heads in disbelief as they recount tales of employees who hold secured doors open for their workmates—or for total strangers, thereby rendering million-dollar card-access systems useless. In large organizations, upper managers who decline to wear their identification badges discover that soon no one else will either. In trying to implement security policies, practitioners sometimes feel that they are involved in turf wars and personal vendettas rather than rational discourse.

CHAPTER 51

SECURITY STANDARDS FOR PRODUCTS

Paul Brusil and Noel Zakin

51.1 INTRODUCTION. Standards provide for uniformity of essential characteristics of products and product-related procedures. Standards allow consumers to have a better understanding of what they purchase. This section provides a general introduction to standards: who creates standards, what types of features and capabilities are standardized, why standards are important, and what types of standards apply to products.

In later sections, attention turns to standards associated with testing and evaluation of products. The nonstandard approaches confronting and befuddling consumers, as well as the issues arising from nonstandard approaches, are contrasted with the confidence obtained by using a universal, internationally accepted standard for product testing and evaluation. The common standard allows the consumer to understand with greater certainty the security and assurance features offered by a product. Increased software quality assurance became of top concern to U.S. Government agency chief information security officers (CISOs) as attention turned to the Federal Information Security Management (FISMA) Act.[1]

51.1.1 Value of Standards. Many parties benefit from standards: customers, vendors, testing houses, and more.

Customers find standards helpful in several ways. Standards help specify their needs for various security functionalities and the degrees of assurance they require in the products they buy. Standards help customers understand what security functionality and assurances that a product builder claims to provide. Standards help consumers select commercial off-the-shelf products that they can trust will conform to their security and assurance requirements and that, as needed, interoperate with comparable products. Customers under the mandates of the security-relevant regulations imposed by the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act (SOX) often look to establishing due diligence by leveraging products that have established trust in their security and assurance functionality in a standard way.

Vendors find standards helpful in several ways. Use of standards provides evidence that vendors have migrated their product development to a paradigm wherein security is built-in from the start. Use of standards provides evidence that security is not some

INTRODUCTION TO PART V

DETECTING SECURITY BREACHES

No matter how well we implement security mechanisms, we are facing human opponents who may counter our best efforts until we can respond appropriately. How do security and network administrators find out if there has been a breach of security? How can they evaluate their own defenses before they are penetrated? This part includes chapters on:

52. **Application Controls.** Application-software security and logging
53. **Monitoring and Control Systems.** System logging and data reduction methods
54. **Security Audits, Standards, and Inspections.** Measuring compliance with explicit policies and with industry standards
55. **Cyber Investigation.** Organizing effective digital forensic studies of observed or suspected security breaches, for internal use, and for cooperation with law enforcement

CHAPTER 52

APPLICATION CONTROLS

Myles Walsh

52.1 PROTECTION IN APPLICATION DEVELOPMENT. In computer installations where systems development takes place, there are technologies that tend to enhance security. These technologies, together with mandatory organizational procedures and standards, force analysts and programmers to adhere to guidelines when they are developing in-house applications or systems to be marketed. This chapter reviews some of the methods programmers use to prevent and identify problems involving data corruption or unavailability.

One of the underpinnings of modern programming is the technology known as the database management system (DBMS). Many applications are developed using this technology. A contemporary RDBMS supports relational databases. Relational databases themselves are based on an underlying technology developed in the 1960s and implemented through the remainder of the twentieth century. It seems certain that the technology will continue to be used for the foreseeable future.

RDBMSs are sets of programs that provide users with the tools to perform these tasks:

- Create database structures (file or table layouts, and screens or forms).
- Enter information into the structures.
- Establish cross-references among the files or tables.

CHAPTER 53

MONITORING AND CONTROL SYSTEMS

Caleb S. Coggins and Diane E. Levine

CHAPTER 54

SECURITY AUDITS, STANDARDS, AND INSPECTIONS

Donald Glass, Chris Davis, John Mason, David Gursky, James Thomas, Wendy Carr, and Diane Levine

CHAPTER 55

CYBER INVESTIGATION[1]

Peter Stephenson

55.1 INTRODUCTION. Cyber investigation (also widely known as *digital investigation*) as a discipline has changed markedly since publication of the fourth edition of this *Handbook* in 2002. In 1999, when *Investigating Computer Related Crime*[2] was published, practitioners in the field were just beginning to speculate as to how cyber investigations would be carried out. At that time, the idea of cyber investigation was almost completely congruent with the practice of computer forensics. Today (as this is being written in April 2008), we know that such a view is too confining for investigations in the current digital environment.

INTRODUCTION TO PART VI

RESPONSE AND REMEDIATION

What are the options when security breaches or accidents occur? How do we prepare for trouble so that we can minimize the consequences and respond quickly and effectively? This part includes these chapters and topics:

56. **Computer Security Incident Response Teams.** Planning and rehearsing responses to a wide variety of security problems—in advance instead of on the fly
57. **Data Backups and Archives.** The essential tool for all forms of recovery
58. **Business Continuity Planning.** Systematic approach to analyzing the priorities for orderly recovery when anything interrupts the smooth operation of the organization
59. **Disaster Recovery.** Planning for rapid, cost-effective return to normal after a crisis is over
60. **Insurance Relief.** Using modern insurance services to reduce the consequences of disasters
61. **Working with Law Enforcement.** Establishing relations with all levels of law enforcement before there is a crisis, and coordinating efficiently and effectively to support investigation and prosecution of criminals

CHAPTER 56

COMPUTER SECURITY INCIDENT RESPONSE TEAMS[1]

Michael Miora, M. E. Kabay, and Bernie Cowens

56.1 OVERVIEW. No matter how good one's security, at some point a security measure will fail. Knowing that helps organizations to plan for security in depth, so that a single point of failure does not necessarily result in catastrophe. Furthermore, instead of trying to invent a response when every second counts, it makes sense to have a competent team in place, trained, and ready to act. The value of time is not constant. Spending an hour or a day planning, so that an emergency response is shortened by a few seconds, may save a life or prevent a business disaster.

An essential element of any effective information security program today is the ability to respond to computer emergencies. Although many organizations have some form of intrusion detection in place, far too few take full advantage of the capabilities those systems offer. Fewer still consistently monitor the data available to them from automated intrusion detection systems, let alone respond to what they see.

The key is to make beneficial use of the knowledge that something has happened, that something is about to happen, or that something is perhaps amiss. Intrusion detection systems can be costly to implement and maintain. It therefore makes little business sense to go to the trouble of implementing an intrusion detection capability if there is not, at the same time, a way to make use of the data produced by these systems.

Computer emergency quick-response teams are generally called *computer security incident response teams* (CSIRTs, the abbreviation used in this chapter) or *computer incident response team*s (CIRTs). Sometimes one sees the term "computer emergency response team" (CERT), but that term and acronym are increasingly reserved for the Computer Emergency Response Team Coordination Center (CERT/CC®) at the Software Engineering Institute of Carnegie Mellon University, as explained in Section 56.1.3 of this chapter.

CSIRTs can provide organizations with a measurable return on their investment in computer security mechanisms and intrusion detection systems. Intrusion detection can indicate that something occurred; CSIRTs can do something about that occurrence. Often their value to an organization can be felt in more subtle ways as well. Many times computer emergencies and incidents cast an organization in an unfavorable light, and they can erode confidence in that organization. Efficient handling of computer emergencies can lessen the erosion of confidence, can help speed the organization's recovery, and in some cases can help restore its image. In addition, CSIRT postmortems (see Section 56.7) can provide information for process improvement (as discussed in Section 56.7.2).

When an incident occurs, the intrusion detection system makes us aware of the incident in one manner or another. We make use of this knowledge by responding to the situation appropriately. "Appropriately" can mean something different in different situations. Therefore, a well-trained, confident, authoritative CSIRT is essential.

Intrusion detection systems are not the only means by which we learn about incidents. In a sense, every component of a system and every person who interacts with the system forms a part of the overall defense and detection system. End users are often the first to notice that something is different. They may not recognize a particular

CHAPTER 57

DATA BACKUPS AND ARCHIVES

M. E. Kabay and Don Holden

57.1 INTRODUCTION. Nothing is perfect. Equipment breaks, people make mistakes, and data files become corrupted or disappear. Everyone, and every system, needs a well-thought-out backup and retrieval policy. In addition to making backups, data processing personnel also must consider requirements for archival storage and for retrieval of data copies. Backups also apply to personnel, equipment, and electrical power; for other applications of redundancy, see Chapters 23 and 45 in this *Handbook*.

57.1.1 Definitions. *Backups* are copies of data files or records, made at a moment in time, and primarily used in the event of failure of the active files. Normally,

CHAPTER 58

BUSINESS CONTINUITY PLANNING

Michael Miora

58.1 INTRODUCTION. We are in an age where businesses and governments are turning in increasing numbers to high-technology systems, and to the Internet, to gain and maintain their competitive advantage. Businesses of all types are relying on high-technology products to build, promote, sell, and deliver their wares and services—as are government, educational, and nonprofit enterprises. All of these are dependent on technology to maintain their income, image, and profitability. business continuity planning (BCP) is the process of protecting organizations from the deleterious effects on their missions that can result from outages in information systems.

The goal of BCP is to protect the operations of the enterprise, not just the computing systems. Prudent planning is not restricted to computer or telecommunications systems

CHAPTER 59

DISASTER RECOVERY

Michael Miora

59.1 INTRODUCTION. In Chapter 58 in this *Handbook*, the importance of a business impact analysis (BIA) and the method of preparing one were described. Once the preliminary groundwork is finished and the BIA analysis is complete, the next step is to design specific strategies for recovery and the tasks for applying those strategies. In this chapter, we discuss the specific strategies to recover the Category I functions, the most time-critical functions identified during the BIA, as well as the remaining lower-priority functions. We examine the traditional strategies of hot sites, warm sites, and cold sites as well as a more modern technique we call reserve systems. We describe how to make good use of Internet and client/server technologies, and of high-speed connections for data backup, for making electronic journals and for data vaulting. We develop the recovery tasks representing the specific activities that must take place to continue functioning, and to resume full operations. These tasks begin with the realization that there is, or may be, a disaster in progress, continue through to full business resumption, and end with normalization, which is the return to normal operations. We examine a set of tasks taken from a real-world disaster recovery plan to illustrate how each task fits into an overall plan, accounting for anticipated contingencies while providing flexibility to handle unforeseen circumstances.

59.2 IDENTIFYING THREATS AND DISASTER SCENARIOS. Threat assessment is the foundation for discovery of threats and their possible levels of impact.

CHAPTER 60

INSURANCE RELIEF

Robert A. Parisi, Jr. and Nancy Callahan

60.1 INTRODUCTION. This chapter presents an overview of traditional insurance products and discusses how they may or may not provide coverage for the risks associated with intellectual property and with computer and network security. It also addresses the new types of coverage that have been developed expressly for those risks.

60.1.1 Historical Background. Historically, people have responded to the risks associated with commerce by finding ways to lessen their impact or severity.

- Around 3000 BCE, Chinese merchants cooperated by distributing cargo among several ships prior to navigating dangerous waterways, so that the loss of one ship would not cause a total loss to any individual.

CHAPTER 61

WORKING WITH LAW ENFORCEMENT

David A. Land

61.1 INTRODUCTION. Today, working with law enforcement is likely one of the most important aspects of computer security, and of our collective need to protect our sites and our sites' information. The entire paradigm has shifted to one where you will need law enforcement, and they will most certainly need you. In times past, however, this was not the case. Understanding their needs before, during, and after the commission of a crime significantly enhances your organization's opportunity to come back online quickly, with, it is hoped, little or no disturbance to your users or customers. Likewise, conveying your needs to law enforcement prior to an incident will serve you well later on. Working with law enforcement is, however, not your opportunity to assume the role of law enforcement. You must know your limitations and at what point to engage your law enforcement contacts.

INTRODUCTION TO PART VII

MANAGEMENT'S ROLE IN SECURITY

Management responsibilities include judgements of which resources can rationally be expended in defending against which threats. Managers must understand how to cope with the lack of quantitative risk estimates while using what information is available to guide investment decisions in personnel and technology. Their decisions are affected by regulatory and legal requirements and by the practical constraints of their relationships with other leaders within their organizations. This part includes chapters and topics that bear on information assurance managers' roles:

62. **Risk Assessment and Risk Management.** Which vulnerabilities warrant repair? Which threats must be taken seriously? How much expense is justified on specific security measures?
63. **Management Responsibilities and Liabilities.** Roles, responsibilities, due diligence, staffing security functions, and the value of accreditation and education
64. **U.S. Legal and Regulatory Security Issues.** For U.S. practitioners especially, this chapter reviews the Gramm-Leach-Bliley Act and the Sarbanes-Oxley legislation
65. **The Role of the CISO.** The chief information security officer as an agent of change and as a strategist working to ensure that security fits into the strategic mission of the organization, and that it is communicated effectively to other C-level executives
66. **Developing Security Policies.** Approaches to creating a culture of security where policies grow organically from the commitment of all sectors of the organization, instead of being imposed unilaterally by security staff
67. **Developing Classification Policies for Data.** The essential role of data classification and how to implement systems that conform to regulatory and legal requirements
68. **Outsourcing and Security.** Security of outsourcing and outsourcing of security

CHAPTER 62

RISK ASSESSMENT AND RISK MANAGEMENT

Robert V. Jacobson

62.1 INTRODUCTION TO RISK MANAGEMENT

62.1.1 What Is Risk? There is general agreement in the computer security community with the common dictionary definition: "the possibility of suffering harm or loss." The definition shows that there are two parts to risk: the *possibility* that

CHAPTER 63

MANAGEMENT RESPONSIBILITIES AND LIABILITIES

Carl Hallberg, M. E. Kabay, Bridgitt Robertson, and Arthur E. Hutt

63.1 INTRODUCTION. This chapter reviews the critical roles of management in establishing, implementing, and maintaining information security policies in the modern enterprise. It also reviews some of the risks to management personnel in failing to ensure adequate standards of information security.[1]

CHAPTER 64

U.S. LEGAL AND REGULATORY SECURITY ISSUES

Timothy Virtue

64.1 INTRODUCTION. The regulatory requirements facing today's business leaders can strengthen the overall business environment while offering increased safeguards to stakeholders such as consumers, suppliers, shareholders, employees, and other interested parties transacting with today's businesses. Although regulatory requirements vary from institution to institution and across different industries, the recurring theme is that management must be proactively involved and fully accountable for the actions of its organization.

Compliance is an ongoing process that can be achieved successfully only when the organization's senior leaders support compliance from both a cultural and operational perspective. In other words, the right attitudes (integrity, honesty, transparency, etc.), also known as *tone at the top*, must be exemplified in all facets of the organization while working in tandem with operational processes to create a comprehensive compliance environment. A culture of compliance must be integrated throughout the organization and must be seamlessly built into all operational facets of the business.

Many organizations are restructuring independent and isolated operational units (sometimes described as *silos*) and focusing on coordinated strategic risk management

CHAPTER 65

ROLE OF THE CISO

Karen F. Worstell

65.1 CISO AS CHANGE AGENT. The title of chief information security officer (CISO) has evolved because of the realization that the function of the chief information officer (CIO) is so broad as to require another person to focus specifically on the *security* elements of information. Another motivation derives from the fact that the CISO can perform functions that are not usually associated with the CIO. Our approach to information security needs to change in response to the disruptive events affecting the network and the boardroom. CISOs should be the change agents to make this happen. This is a shift from the majority of CISOs' emphasis today as senior managers of information technology (IT) security.

Today, CISOs are in the trust business due to the need to create and maintain a network of trust among all the people, business processes, and technology of an enterprise and its partners. The interconnected ecosystem that developed since the commercialization of the Internet has seen dramatic shifts of trust: Consumers are thinking twice

CHAPTER 66

DEVELOPING SECURITY POLICIES

M. E. Kabay and Sean Kelley

66.1 INTRODUCTION. This chapter reviews methods for developing security policies in specific organizations. Some of the other chapters of this *Handbook* that bear on policy content, development, and implementation are listed next:

- Chapter 23 provides an extensive overview of physical security policies.
- Chapter 25 discusses local area network security issues and policies.
- Chapter 39 reviews software development policies and quality assurance policies.

CHAPTER 67

DEVELOPING CLASSIFICATION POLICIES FOR DATA

Karthik Raman and Kevin Beets

67.1 INTRODUCTION. A figure appears from the bushes on a dark and stormy night and silently slips past two guards. Inside the building, a flashlight flickers to life and begins a slow dance around a cluttered office. The beam freezes. It illuminates an envelope that is stamped with large red letters: "TOP SECRET."

The top secret label is likely the most popularly recognized part of an example of a data classification (DC) scheme. DC labels information so that its custodians and users can comply with established data protection policies when organizing, viewing, editing, valuing, protecting, and storing data.

Historically, DC has been used by the government and military. Today, however, it has increasingly become a necessity for businesses because of the competitive value of information, because of the legal requirements for maintenance of sound financial and operational records, and because of the demands of privacy-protection laws.

This chapter explains why DC is necessary, how it relates to information security, common laws and standards associated with DC, its design and implementation in an enterprise, hardware and software solutions that can assist in performing DC, and some practical recommendations to consider when implementing DC.

CHAPTER 68

OUTSOURCING AND SECURITY

Kip Boyle, Michael Buglewicz, and Steven Lovaas

68.1 INTRODUCTION. The term "outsourcing" has come to identify several distinct concepts, each requiring a different risk management strategy. In this chapter,

INTRODUCTION TO PART VIII

PUBLIC POLICY AND OTHER CONSIDERATIONS

This edition of the *Handbook* ends with compelling issues in information security. Part VIII provides a basis for vigorous discussion about important and controversial topics such as:

69. **Privacy in Cyberspace: U.S. and European Perspectives.** With increasingly frequent losses of control over personally identifiable information, the public is ever more concerned about privacy
70. **Anonymity and Identity in Cyberspace.** How individuals are representing themselves in Internet-mediated communications; the social and legal consequences of completely anonymous interactions, and of untraceable but stable identifiers
71. **Medical Records Protection.** How the special requirements of high availability coupled with extreme sensitivity of medical information poses complex problems for security specialists in medical environments
72. **Legal and Policy Issues of Censorship and Content Filtering.** How corporations and governments around the world regulate access to information that violates social norms, or is perceived as a potential threat to state power
73. **Expert Witnesses and the *Daubert* Challenge.** How security specialists should prepare for their day in court
74. **Professional Certification and Training in Information Assurance.** Benefits and costs of education, professional certifications, examinations, and commercial training
75. **U.S. Undergraduate and Graduate Education in Information Assurance.** Initiatives in the United States have added information assurance to the curriculum of many programs at institutions of higher learning
76. **Undergraduate and Graduate Education in Information Assurance.** Perspectives on information assurance education at the baccalaureate and advanced levels in Europe and the United States
77. **The Future of Information Assurance.** A giant in the field of information assurance reviews the foundations of IA, best practices, and risk reduction and applies his expertise to computer-aided voting as a case study in applied security

CHAPTER 69

PRIVACY IN CYBERSPACE: U.S. AND EUROPEAN PERSPECTIVES

Henry L. Judy, Scott L. David, Benjamin S. Hayes, Jeffrey B. Ritter, and Marc Rotenberg

CHAPTER 70

ANONYMITY AND IDENTITY IN CYBERSPACE

M. E. Kabay, Eric Salveggio, and Robert Guess

70.1 INTRODUCTION. As electronic communications technology becomes widespread among increasingly international populations of computer users, one of the most hotly debated questions is how to maintain the benefits of free discourse while simultaneously restricting antisocial communications and behavior on the Net. The debate is complicated by the international and intercultural dimensions of

CHAPTER 71

MEDICAL RECORDS PROTECTION

Paul J. Brusil

71.1 INTRODUCTION. U.S. regulatory compliance forces increased attention on information protection. Regulations such as SOX 404 (Sarbanes-Oxley), FISMA (Federal Information System Management Act), GLB (Gramm-Leach Bliley), HIPAA (Health Insurance Portability and Accountability Act), and others are establishing

CHAPTER 72

LEGAL AND POLICY ISSUES OF CENSORSHIP AND CONTENT FILTERING

Lee Tien, Seth Finkelstein, and Steven Lovaas

72.1 INTRODUCTION

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers.[1]

One might think that the Internet will make this ringing proclamation a reality. Like no other technology, the Internet transcends national borders and eliminates barriers to the free flow of information. Governments, however, are trying to control speech on the Internet.

CHAPTER 73

EXPERT WITNESSES AND THE *DAUBERT* CHALLENGE

Chey Cobb

73.1 INTRODUCTION. Whenever science or technology enters the courtroom, there must surely be an expert who can give clear and proper explanations of the subject matter to the judge and jury. As new sciences and technologies have emerged, the courts have had to decide if a person is, indeed, an expert and whether or not the science is real and admissible.[1]

In 1923, the United States courts began accepting scientific evidence based on a new rule. That rule used the "general acceptance" test to determine if evidence was legitimate. This test was based on the rulings in *Frye v. United States*, which declared that if a scientific practice was generally accepted among the scientific community in which it was practiced, it could be admitted in court. This has become generally referred to as the *Frye test*.[2]

In 1975, the federal government made the scientific assertions a bit stronger by issuing the Federal Rules of Evidence No. 702 (FRE 702), which states in part:

CHAPTER 74

PROFESSIONAL CERTIFICATION AND TRAINING IN INFORMATION ASSURANCE

Christopher Christian, M. E. Kabay, Kevin Henry, and Sondra Schneider

74.1 BUILDING SKILLS THROUGH PROFESSIONAL EDUCATION. Perhaps one of the most critical decisions an organization has to make today is how to invest in its staff. Technology, policies, and well-defined processes are all important

CHAPTER 75

UNDERGRADUATE AND GRADUATE EDUCATION IN INFORMATION ASSURANCE

Vic Maconachy and Seymour Bosworth

75.1 INTRODUCTION. Information assurance has come to the forefront of the consciousness of the modern world. Recent events such as high-publicity breaches of security, as well as pervasive small-scale abuses of the technologies available at work and at home, have highlighted the need for trained professionals able to operate in the complex world of information assurance. Toward this end, recent initiatives in the United States and Europe have added information assurance into the undergraduate and graduate curriculum of more common degrees such as computer science, and have also identified information assurance as its own discipline worthy of its own curriculum. This chapter outlines some of the initiatives that have taken place in the United States and speculates about the future of the discipline.

75.2 U.S. INITIATIVES IN TRAINING AND EDUCATION OF INFORMATION ASSURANCE

75.2.1 TIE System. Any approach to information assurance (IA) education must be presented in a conceptual context. The Trusted Information Environment

CHAPTER 76

EUROPEAN GRADUATE WORK IN INFORMATION ASSURANCE AND THE BOLOGNA DECLARATION[1]

Urs E. Gattiker

A fundamental fact in computer, information, and network security[2] is the impossibility of 100 percent assurance that a computer system is trusted.[3] How education can help in achieving the required level of trust considering various stakeholders (e.g.,

CHAPTER 77

THE FUTURE OF INFORMATION ASSURANCE[1]

Peter G. Neumann

77.1 INTRODUCTION

Assurance is in the eye of the beholder.

Although this chapter is at the end of the *Handbook*, we are still only at the beginning of the quest for meaningfully trustworthy systems. We begin by asserting that there

INDEX