

Second Edition

The
Complete
Reference™

Information Security

- Learn proven security strategies, techniques, and best practices
- Implement reliable data, network, computer, and application security
- Understand compliance with standards, regulations, and laws

Mark Rhodes-Ousley

The
Complete
Reference™

Information Security
Second Edition

About the Author

Mark Rhodes-Ousley is experienced with every aspect of security, from program management to technology. That experience includes risk management, security policies, security management, technology implementation and operations, physical security, disaster recovery, and business continuity planning. A resident of Silicon Valley, he has been fortunate to live through the early years, boom times, and mainstreaming of computers and the Internet, practicing information security even before Windows existed. Mark holds a CISSP certification from the International Information Systems Security Certification Consortium (ISC)², a CISM certification from the Information Systems Audit and Control Association (ISACA), and certifications from ITIL, Microsoft (MCSE: Security 2003), Cisco, Security Dynamics, Raptor Systems, Hewlett-Packard, and Digital Equipment Corporation, along with a bachelor's degree in applied mathematics and electrical engineering from the University of California, San Diego (UCSD).

Specializing in information security since 1994 when he built the first Internet firewall for Santa Clara County, California, Mark has built quality-focused security programs, processes, and technologies at Robert Half International (RHI), Merrill-Lynch, National City Bank, Fremont Bank, Sun Microsystems, PG&E, Clorox, The Gap, Aspect Communications, Hitachi Data Systems (HDS), SunPower, and the original Napster. He holds two core beliefs: that business processes are just as important as technology because security relies on people; and that security should be a business enabler, with a goal of enhancing the customer experience. Believing that maturity of a security program should be improved one step at a time, measured on a five-point maturity scale, with targets agreed upon by business stakeholders, Mark is also a proponent of “management by measurement”—performance measured with metrics (raw data) to manage down and key performance indicators (KPI dashboards) to manage up. His experience has shown that building bridges and fostering cross-departmental collaboration, along with executive sponsorship and engagement, enhances the success of the security program.

Mark can be reached at mro@engineer.com or www.facebook.com/pages/Information-Security-The-Complete-Reference-2nd-Ed on Facebook.

About the Contributors and Technical Reviewers

Andrew Abbate, contributor, enjoys the position of principal consultant and partner at Convergent Computing. With nearly 20 years of experience in IT, Andrew's area of expertise is understanding a business's needs and translating that to processes and technologies to solve real problems. Having worked with companies from the Fortune 10 to companies of ten employees, Andrew has a unique perspective on IT and a grasp on “big picture” consulting. Andrew has also written nine industry books on varying technologies ranging from Windows to security to unified communications and has contributed to several others. Andrew can be reached via e-mail at andrew@abbate.org.

After being battered about for 20 years in the construction industry, **Barrington Allen**, technical reviewer, packed up his transferable skills and began a career in information technology 16 years ago. Working in a Fortune 100 company has provided Barrington the opportunity to work on interesting and complex enterprise systems, while also providing the continual learning support which is essential to any IT career. Barrington is often seen walking his border collies, or seeking to ride on a velodrome near you.

Brian Baker, contributor, has been an IT professional for nearly three decades. Brian has supported environments consisting of large, multi-mainframe data centers, international corporations, and smaller, single-site e-commerce infrastructures. He has worked for EDS, ACS, Merrill Lynch, Ross Dress for Less, and others over the course of his career. His roles have included systems, network, messaging, and security, and for the past ten years he has been supporting and managing storage infrastructures. Brian initially began his storage career while he worked as part of a small team to select and design a SAN implementation. From there he managed the backup and storage infrastructure for a division of Merrill Lynch. As his experience grew, Brian accepted a position with a large hosting provider, joining a small team that managed over 3 petabytes of storage consisting of various SAN array vendors and SAN fabrics within 16 data centers. Brian is an EMC Storage Specialist (EMCSA) and holds a bachelor's degree in information technology from National University. He may be contacted at bmbaker@gmail.com.

As a security researcher at McAfee, contributor **Zheng Bu**'s every day work is on host and network security. He likes to innovate and address security problems. His recent research includes application and mobile. He is a runner, badminton player, and photographer. Feel free to contact him at zheng.bu.sec@gmail.com.

Brian Buege, contributor, is the Director of Engineering at Spirent Communications. He has more than ten years of software development experience and has been developing large-scale, enterprise Java applications since 1998. He lives in McKinney, Texas, with his wife and son.

Anil Desai (MCSE, MCSA, MCSD, MCDBA), contributor, is an independent consultant based in Austin, Texas. He specializes in evaluating, developing, implementing, and managing solutions based on Microsoft technologies. He has worked extensively with Microsoft's server products and the .NET platform. Anil is the author of several other technical books, including *MCSE/MCSA Managing and Maintaining a Windows Server 2003 Environment Study Guide Exam 70-290* (McGraw-Hill/Osborne, 2003), *Windows 2000 Directory Services Administration Study Guide* (McGraw-Hill/Osborne, 2001), *Windows NT Network Management: Reducing Total Cost of Ownership* (New Riders, 1999), and *SQL Server 2000 Backup and Recovery* (McGraw-Hill/Osborne, 2001). He has made dozens of conference presentations at national events and is also a contributor to magazines. When he's not busy doing techie-type things, Anil enjoys cycling in and around Austin, playing electric guitar and drums, and playing video games. For more information, you can contact him at anil@austin.rr.com.

Leo Dregier, contributor, got his start in networking when he took the MCSE 4.0 Microsoft track. After a few short months, he was recognized as a very knowledgeable subject matter expert, so much so that the corporate school he attended offered him a job to teach other aspiring Microsoft engineers. Leo has the ability to learn very quickly and is highly adaptable, analytical, and an overachiever (as demonstrated by having expertise in over 40 of the popular computer certifications, including CISSP, ISSEP, CISM, CISA, CRISC, PMP, CEH, CHFI, and several others). Leo has been a principal at the computer security firm The Security Matrix, LLC, since 1995. He has provided consulting services to many U.S. federal clients, including the Department of State, the Department of Labor, the Internal Revenue Service, and the Centers for Medicaid and Medicare Services. Additionally, Leo has helped thousands of IT professionals achieve their certifications online at TheCodeOfLearning.com and maintains an evaluation level above 90+%. When Leo is not working as a consultant or in the classroom, you can find him working on his other personal projects. TheProfitCycle.com is geared toward people who need help learning how to adapt to technology and want to

make money using technology as a solution. Leo has also created FindRealEstateHelp.com, which is a real estate problem-solving and investment company. In his spare time, he sleeps and spends time with his beautiful wife. Leo can be contacted for consulting, public speaking, TV appearances, and more at www.leodregier.com.

Dr. Nick Efford, contributor, is a senior teaching fellow in the School of Computing at the University of Leeds in the United Kingdom, where he currently teaches object-oriented software engineering, distributed systems, and computer security. His previous published work includes a book on digital image processing using Java.

Aaron Estes, technical reviewer, has over twelve years of experience in software development and security engineering. His expertise includes secure coding and code review, penetration-testing, security architecture review, and network security. Aaron has had key security engineering roles on several of Lockheed Martin's largest contracts. In addition to Lockheed Martin, Aaron has worked with a number of Fortune 500 companies as a security consultant. He has over four years of teaching experience at Southern Methodist University at the undergraduate and graduate level, and expects to complete his doctorate degree this year in Software Engineering with a focus on security software at Southern Methodist University in Dallas.

Thaddeus Fortenberry (MCSE, MCT), contributor, is a senior member technical staff and the remote access architect for employee access at HP. For the past year, he has been working on the consolidation of the remote access solutions for the merged Compaq and HP environments. Thaddeus specializes in complete security plans for remote deployments that address real-world issues and protection.

Christian Genetski, contributor, is a Senior Vice President and General Counsel at the Entertainment Software Association. Christian is a former prosecutor in the Department of Justice Computer Crime Section, where he coordinated the investigations of several prominent computer crime cases, including the widely publicized denial of service attacks that hit e-commerce sites eBay, Amazon.com, and others in February 2000. In private practice, he counsels clients on compliance with information security regulations, conducts investigations into computer security breaches or other hostile network activity, and represents clients in civil litigation or criminal referrals arising from network incidents. Christian graduated from the Vanderbilt University School of Law, Order of the Coif. He regularly lectures to a wide variety of audiences on computer crime and information security issues, and he serves as an adjunct professor at the Georgetown University Law Center. Christian would like to thank David Tonisson for his thoughtful contributions to Chapter 3 on legal issues.

Christine Grayban, technical reviewer, is the Enterprise Security practice lead for Stach & Liu, where she oversees all projects related to information security compliance and controls, risk management, governance, and security strategy. She has helped several organizations reach compliance with PCI DSS, HIPAA, ISO 27001/2, and other information security frameworks. Prior to joining Stach & Liu, Christie spent several years in the security consulting practices at Accenture and Ernst & Young for clients in the Global 500, with verticals including financial services, telecommunications, health care, and resources. She is currently based in New York City and has worked and lived internationally in San Francisco, London, and Mumbai.

Roger A. Grimes (CPA, MCSE NT/2000, CNE 3/4, A+), contributor, is the author of *Malicious Mobile Code: Virus Protection for Windows* (O'Reilly, 2001), *Honeypots for Windows* (Apress, 2004), and *Professional Windows Desktop and Server Hardening* (Wrox, 2006) and

has been fighting malware since 1987. He has consulted for some of the world's largest companies, universities, and the U.S. Navy. Roger has written dozens of articles for national computer magazines, such as *Windows & .NET Magazine*, *Microsoft Certified Professional Magazine*, and *Network Magazine*, and *Newsweek* covered his work fighting computer viruses. You can contact him at rogerg@cox.net.

Gregory Hoban, technical reviewer, is a Senior Systems Engineer currently in Emeryville, California. He has over 17 years of experience dealing with a wide range of servers and storage, specializing in systems and database installation and configuration. Gregory has deployed highly available Oracle and SQL server databases on a number of SANs. He has been responsible for implementing security restrictions and business IT process controls at both FDA- and SOX-compliant facilities. Gregory holds an NCDA certification for NetApp and an Advanced CXE certification for Xiotech.

Michael Howard, contributor, is a Principal CyberSecurity Architect at Microsoft Corp., a founding member of the Secure Windows Initiative group at Microsoft, and a coauthor of *Writing Secure Code* (Microsoft Press, 2001). He focuses on the short- and long-term goals of designing, building, testing, and deploying applications to withstand attack and yet to still be usable by millions of nontechnical users.

Ayush Jain, technical reviewer, is a Senior IT Infrastructure Manager in Emeryville, California. Ayush's professional experiences cover all facets of information security, including, but not limited to, designing and deploying secure infrastructures, BYOD, VDI, implementing intrusion detection and data leak prevention systems, and developing policies and procedures for IT Governance. He holds a bachelor's degree in information technology from Rochester Institute of Technology (R.I.T.) and Advanced CXE certification for Xiotech.

Michael Judd (a.k.a. Judd), contributor, is a Senior Application Engineer at FTEN (a NASDAQ OMX company). He has taught and developed technical courseware on subjects ranging from Java syntax, object-oriented analysis and design, patterns, and distributed programming, to Java security and J2EE. He lives in Denver, Colorado.

Dr. Bryan Kissinger, contributor, is a seasoned security professional with over 18 years of experience advising government and various private sector organizations on enhancing their security posture. He is currently responsible for assessing risk, recommending infrastructure enhancements, and managing compliance for a major healthcare provider. Bryan was previously a Director in PricewaterhouseCoopers' Security practice with leadership responsibilities in the Pacific Northwest and Bay Area markets. He is considered a healthcare and technology sector specialist and is a published author and frequent public speaker on the topics of security and information technology strategy.

Thomas Knox, contributor, has done Unix administration for more years than he wants to admit. He is currently a Streaming Media Engineer at Comcast and previously worked as a network and system engineer for National Geographic and Amazon.com. His thanks go to his wife Gisela for all her love and support.

Brenda Larcom, technical reviewer, is a Senior Security Consultant throughout the United States and occasionally beyond. She has over 17 years of experience securing software and the odd bit of hardware throughout the development and deployment lifecycle, particularly for Agile organizations. Brenda cofounded an open source threat modeling methodology that analyzes security requirements as well as architecture. Brenda holds a bachelor's degree in computer science from the University of Washington. She may be contacted at blarcom@stachliu.com.

Eric Milam, contributor, is a Principal Security Assessor with over 14 years of experience in information technology. Eric has performed innumerable consultative engagements, including enterprise security and risk assessments, perimeter penetration testing, vulnerability assessments, social engineering, physical security testing, and wireless assessments, and has extensive experience in PCI compliance controls and assessments. Eric is a project steward for the Ettercap project as well as creator and developer of the easy-creds and smbexec open source software projects. He can be reached at emilam@accuvant.com and jbrav.hax@gmail.com.

Michael T. Raggo (CISSP, NSA-IAM, CCSI, ACE, CSI), contributor, applies over 20 years of security technology experience and evangelism to the technical delivery of security research and solutions. Michael's technology experience includes penetration testing, wireless security assessments, compliance assessments, firewall and IDS/IPS deployments, mobile device security, incident response and forensics, and security research, and he is also a former security trainer. As a Product Manager at AirDefense, he co-designed a new and innovative product (Wireless Vulnerability Assessment; U.S. patent #7,577,424), a wireless "hacker-in-a-box" add-on module for AirDefense's Wireless IPS solution. In addition, Michael conducts ongoing independent research on various wireless and mobile hacking techniques, as well as data hiding. He has presented on various security topics at numerous conferences around the world (including BlackHat, DefCon, SANS, DoD Cyber Crime, OWASP, InfoSec, etc.) and has even briefed the Pentagon. You can find out more on his security research website at www.spyhunter.org.

Eric Reither, technical reviewer, is the Vice President and a Senior Security Consultant at Security by Design Inc. Since 2001, he has been involved with numerous projects, and his project management skills have proven invaluable for keeping projects on time and on budget. Eric's project involvement also extends to engineering, drafting, and database management. This deep level of project involvement combined with Eric's experience helps to guarantee client expectations are exceeded on a regular basis. Eric also has over ten years of experience in the fire suppression and facilities communication systems industries. During that period, his responsibilities included systems installation, all facets of project management, systems engineering and design, and training program development. He can be reached at eric_reither@sbd.us.

Ben Rothke (CISSP), technical reviewer, is a Corporate Services Information Security Manager at Wyndham Worldwide, and he has more than 15 years of industry experience in the area of information systems security. His areas of expertise are in PKI, HIPAA, 21 CFR Part 11, design and implementation of systems security, encryption, firewall configuration and review, cryptography, and security policy development. Prior to joining ThruPoint, Inc., Ben was with Baltimore Technologies, Ernst & Young, and Citicorp, and he has provided security solutions to many Fortune 500 companies. Ben is also the lead mentor in the ThruPoint CISSP preparation program, preparing security professionals to take the rigorous CISSP examination. Ben has written numerous articles for such computer periodicals as the *Journal of Information Systems Security*, *PC Week*, *Network World*, *Information Security*, *SC*, *Windows NT Magazine*, *InfoWorld*, and the *Computer Security Journal*. Ben writes for *Unix Review* and *Security Management* and is a former columnist for *Information Security* and *Solutions Integrator* magazine; he is also a frequent speaker at industry conferences. Ben is a Certified Information Systems Security Professional (CISSP) and Certified Confidentiality Officer (CCO), and a member of HTCIA, ISSA, ICSA, IEEE, ASIS, and CSI. While not busy making corporate America a more secure place, Ben enjoys spending time with his family.

Zeke (Ezekiel) Rutman-Allen, technical reviewer and contributor, is first and foremost a fanatical technologist. Zeke carries an active interest in all disciplines of technology application, from tradecrafts to supercomputing, with expertise in many different areas of telecommunications, networking, and data centers. Originally a network engineer, he has held a variety of technical and management positions in enterprise and government organizations in network engineering, data center, and voice/VoIP architecture, design, and operation. Currently, Zeke holds the position of Senior Manager, Global Network Services for a multibillion dollar green energy company. His responsibilities include several key technology stacks, including data center spec/design/operation, LAN/WAN, global voice and VoIP platforms, and all remote access. These duties have allowed Zeke to satiate his hunger for knowledge while maintaining a wide variety of expertise across a multitude of disciplines. Zeke can be reached at zekera@gmail.com.

Stephen Singam, technical reviewer, has extensive experience in information security architecture and management, stakeholder management, strategic planning, and security project management and delivery. He is currently a CTO at Hewlett-Packard, and has held security leadership positions at Commonwealth Bank of Australia (Sydney), 20th Century Fox/News Corporation (Los Angeles), Salesforce.com (San Francisco), IBM (New York), and Nokia (Helsinki). His accomplishments include developing a Cyber Security Operation Center (SOC) encompassing the provisioning of security monitoring via IDaaS, threat and vulnerability intelligence using Big Data technologies and managed security infrastructure, and creating a cloud security reference architecture for a large telecommunication SaaS market offering. At 20th Century Fox, Stephen developed Intellectual Property Security Architecture, Standards, and Policies that cover all release platforms from Script Development to Home Entertainment worldwide. This was accomplished with a focus on the most successful movie of all time—James Cameron's *Avatar*. As a result, Fox became the first Media & Entertainment firm to successfully attain a zero pre-release IP leak of major DVD releases in Russia. Stephen has an MS in management of technology from the University of Pennsylvania, a joint program of Wharton Business School and the School of Applied Science & Engineering. He is a Moore Fellow in Management of Technology at University of Pennsylvania. He also has an MS in international management from University of Reading (United Kingdom). Stephen has been an Invited Panelist at: Tech ROI; New York Times Business-Innovation; and Silicon Valley's ISACA Annual Meeting and United Kingdom's Knowledge Transfer Network. In 2011, he was invited by the Chinese government in Chongqing to advise on non-monitored cloud services for MNCs such as Microsoft, JP Morgan and IBM Corp. He can be reached at stephen@ssingam.com.

Keith Strassberg (CPA, CISSP), technical reviewer, contributor, and first edition coauthor, is now CEO/CTO of Universal Survey, one of the world's largest independent market research data collection companies. Keith oversees Universal's operations and pushes the company to be a highly competitive and efficient partner. Universal's clients benefit from Keith's insight and extensive technical abilities, and he is known for developing and executing solutions in dynamic and fast-moving technology environments. Keith has been in the information security field for over 15 years and has worked at firms such as The Guardian Life Insurance Company of America and Arthur Andersen. Keith holds a BS in accounting from Binghamton University, and he can be reached at kstrassberg@yahoo.com.

Simon Thorpe, contributor, has been working with information security technologies since 1999. He was the first employee of SealedMedia after the founder received the first round of funding. He was involved in the development, support, QA, sales, consulting, product management, and marketing of the SealedMedia product. In 2006, when the technology was acquired by Oracle, Simon continued his involvement by working on IRM solutions with companies around the globe as well as deploying the technology internally, protecting Oracle's most valuable information. Simon has written for the Oracle IRM blog, *Oracle Profit Magazine*, and other online publications, and has extensive knowledge of many of the unstructured data security solutions in the market today. Simon then moved from Oracle to Microsoft, where he continues to apply his IRM knowledge with the Microsoft AD RMS technology. Simon is often looking for feedback on how people implement document and file security technologies, so feel free to contact him at simon@securitypedant.com.

Dr. Andrew A. Vladimirov (CISSP, CCNP, CCDP, CWNA, TIA Linux+), contributor, currently holds the position of Chief Security Manager for Arhont Information Security Ltd. (www.arhont.com), a fast-growing information security company based in Bristol, UK. Andrew is a graduate of King's College London and University of Bristol. He is a researcher with wide interests, ranging from cryptography and network security to bioinformatics and neuroscience. He published his first scientific paper at the age of 13 and dates his computing experience back to the release of Z80. Andrew was one of the cofounders of Arhont, which was established in 2000 as a pro-open-source information security company with attitude. Over the years, Andrew has participated in Arhont's contributions to the security community via publications at BugTraq and other security-related public e-mail lists, network security articles for various IT magazines, and statistical research. Andrew's wireless networking and security background predates the emergence of the 802.11 standard and includes hands-on experience designing, installing, configuring, penetrating, securing, and troubleshooting wireless LANs, Bluetooth PANs, and infrared links implemented using a wide variety of operating systems and hardware architectures. Andrew was one of the first UK IT professionals to obtain the CWNA certification, and he is currently in charge of the wireless consultancy service provided by Arhont. He participates in wireless security equipment beta testing for major wireless hardware and firmware vendors, such as Proxim, Belkin, and Netgear.

Barak Weichselbaum, contributor and technical reviewer, is a network and security consultant who started his career in the Israeli Defense Forces and served in the intelligence corps. He spearheaded the development of numerous network security products and solutions, including B2B, P2P, IPS, and IDS, from the ground up to the deployment and integration stage. He is the founder and CEO of B.W. Komodia Ltd. You can contact him at www.komodiam.com.

Marcia Wilson, contributor, is an information technology veteran who has focused on information security for the last decade. She holds the CISSP and CISM designations. She received her master's degree from the University of San Francisco and is finishing up her doctoral studies in information assurance at Capella University. Marcia has worked in a number of capacities in information security, including managing and directing security teams in a global environment, as an individual contributor, and as a consultant for small, medium, and large organizations. She is experienced in healthcare, financial, and high tech organizations in both the private and public sectors. Marcia's passion is protecting the privacy of individual personal and healthcare information.

The
Complete
Reference™

Information Security

Second Edition

Mark Rhodes-Ousley



New York Chicago San Francisco
Lisbon London Madrid Mexico City
Milan New Delhi San Juan
Seoul Singapore Sydney Toronto

Copyright © 2013 by The McGraw-Hill Companies. All rights reserved. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

ISBN: 978-0-07-178436-8

MHID: 0-07-178436-5

The material in this e-Book also appears in the print version of this title: ISBN: 978-0-07-178435-1,
MHID: 0-07-178435-7

McGraw-Hill e-Books are available at special quantity discounts to use as premiums and sales promotions, or for use in corporate training programs. To contact a representative please e-mail us at bulksales@mcgraw-hill.com.

All trademarks are trademarks of their respective owners. Rather than put a trademark symbol after every occurrence of a trademarked name, we use names in an editorial fashion only, and to the benefit of the trademark owner, with no intention of infringement of the trademark. Where such designations appear in this book, they have been printed with initial caps.

Information has been obtained by McGraw-Hill from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw-Hill or others, McGraw-Hill does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

TERMS OF USE

This is a copyrighted work and McGraw-Hill and its licensors reserve all rights in and to the work. Use of this work is subject to these terms. Except as permitted under the Copyright Act of 1976 and the right to store and retrieve one copy of the work, you may not decompile, disassemble, reverse engineer, reproduce, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish or sublicense the work or any part of it without McGraw-Hill prior consent. You may use the work for your own noncommercial and personal use; any other use of the work is strictly prohibited. Your right to use the work may be terminated if you fail to comply with these terms.

THE WORK IS PROVIDED "AS IS." THE MCGRAW-HILL COMPANIES AND ITS LICENSORS MAKE NO GUARANTEES OR WARRANTIES AS TO THE ACCURACY, ADEQUACY OR COMPLETENESS OF OR RESULTS TO BE OBTAINED FROM USING THE WORK, INCLUDING ANY INFORMATION THAT CAN BE ACCESSED THROUGH THE WORK VIA HYPERLINK OR OTHERWISE, AND EXPRESSLY DISCLAIM ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. McGraw-Hill and its licensors do not warrant or guarantee that the functions contained in the work will meet your requirements or that its operation will be uninterrupted or error free. Neither McGraw-Hill nor its licensors shall be liable to you or anyone else for any inaccuracy, error or omission, regardless of cause, in the work or for any damages resulting therefrom. McGraw-Hill has no responsibility for the content of any information accessed through the work. Under no circumstances shall McGraw-Hill and/or its licensors be liable for any indirect, incidental, special, punitive, consequential or similar damages that result from the use of or inability to use the work, even if any of them has been advised of the possibility of such damages. This limitation of liability shall apply to any claim or cause whatsoever whether such claim or cause arises in contract, tort or otherwise.

*For those who toil in the thankless and invisible labor of defending
infrastructure against thieves, vandals, and fools who cause damage for
fun and profit. Stay true.*

—MRO

This page intentionally left blank

Contents at a Glance

Part I	Foundations	
1	Information Security Overview	3
2	Risk Analysis	25
3	Compliance with Standards, Regulations, and Laws	55
4	Secure Design Principles	85
5	Security Policies, Standards, Procedures, and Guidelines	107
6	Security Organization	149
7	Authentication and Authorization	167
Part II	Data Security	
8	Securing Unstructured Data	191
9	Information Rights Management	211
10	Encryption	241
11	Storage Security	253
12	Database Security	273
Part III	Network Security	
13	Secure Network Design	299
14	Network Device Security	321
15	Firewalls	343
16	Virtual Private Networks	355
17	Wireless Network Security	371
18	Intrusion Detection and Prevention Systems	399
19	Voice over IP (VoIP) and PBX Security	427
Part IV	Computer Security	
20	Operating System Security Models	463
21	Unix Security	477
22	Windows Security	499
23	Securing Infrastructure Services	543
24	Virtual Machines and Cloud Computing	575
25	Securing Mobile Devices	597

Part V	Application Security	
26	Secure Application Design	611
27	Writing Secure Software	635
28	J2EE Security	655
29	Windows .NET Security	679
30	Controlling Application Behavior	713
Part VI	Security Operations	
31	Security Operations Management	727
32	Disaster Recovery, Business Continuity, Backups, and High Availability	745
33	Incident Response and Forensic Analysis	767
Part VII	Physical Security	
34	Physical Security	789
	Glossary	803
	Index	833

Contents

Prefacexxxiii
Acknowledgments	xxxv
Introduction	xxxvii

Part I Foundations

Chapter 1	Information Security Overview	3
	The Importance of Information Protection	3
	The Evolution of Information Security	5
	Justifying Security Investment	8
	Business Agility	9
	Cost Reduction	10
	Portability	10
	Security Methodology	11
	How to Build a Security Program	14
	Authority	14
	Framework	15
	Assessment	16
	Planning	16
	Action	17
	Maintenance	17
	The Impossible Job	17
	The Weakest Link	18
	Strategy and Tactics	20
	Business Processes vs. Technical Controls	21
	Summary	22
	References	23
Chapter 2	Risk Analysis	25
	Threat Definition	25
	Threat Vectors	26
	Threat Sources and Targets	29
	Types of Attacks	30
	Malicious Mobile Code	31
	Advanced Persistent Threats (APTs)	41
	Manual Attacks	42

	Risk Analysis	51
	Summary	53
	References	53
Chapter 3	Compliance with Standards, Regulations, and Laws	55
	Information Security Standards	55
	COBIT	56
	ISO 27000 Series	57
	NIST	60
	Regulations Affecting Information Security Professionals	62
	The Duty of Care	63
	Gramm-Leach-Bliley Act (GLBA)	63
	Sarbanes-Oxley Act	66
	HIPAA Privacy and Security Rules	66
	NERC CIP	68
	PCI DSS: Payment Card Industry Data Security Standard	69
	Laws Affecting Information Security Professionals	70
	Hacking Laws	71
	Electronic Communication Laws	76
	Other Substantive Laws	79
	Summary	82
	References	83
Chapter 4	Secure Design Principles	85
	The CIA Triad and Other Models	85
	Confidentiality	85
	Integrity	86
	Availability	86
	Additional Concepts	86
	Defense Models	87
	The Lollipop Model	87
	The Onion Model	88
	Zones of Trust	90
	Best Practices for Network Defense	93
	Secure the Physical Environment	93
	Harden the Operating System	94
	Keep Patches Updated	94
	Use an Antivirus Scanner (with Real-Time Scanning)	95
	Use Firewall Software	95
	Secure Network Share Permissions	95
	Use Encryption	96
	Secure Applications	96

	Back Up the System	101
	Implement ARP Poisoning Defenses	102
	Create a Computer Security Defense Plan	102
	Summary	104
	References	105
Chapter 5	Security Policies, Standards, Procedures, and Guidelines	107
	Security Policies	108
	Security Policy Development	109
	Security Policy Contributors	110
	Security Policy Audience	111
	Policy Categories	112
	Frameworks	113
	Security Awareness	114
	Importance of Security Awareness	114
	Objectives of an Awareness Program	115
	Increasing Effectiveness	117
	Implementing the Awareness Program	118
	Enforcement	119
	Policy Enforcement for Vendors	120
	Policy Enforcement for Employees	120
	Software-Based Enforcement	120
	Example Security Policy Topics	121
	Acceptable Use Policies	122
	Computer Policies	124
	Network Policies	127
	Data Privacy Policies	128
	Data Integrity Policies	130
	Personnel Management Policies	132
	Security Management Policies	135
	Physical Security Policies	138
	Security Standards	142
	Security Standard Example	142
	Security Procedures	144
	Security Procedure Example	144
	Security Guidelines	145
	Security Guideline Example	145
	Ongoing Maintenance	147
	Summary	147
	References	148

Chapter 6	Security Organization	149
	Roles and Responsibilities	149
	Security Positions	151
	Security Incident Response Team	158
	Managed Security Services	160
	Services Performed by MSSPs	162
	Services That Can Be Monitored by MSSPs	163
	Security Council, Steering Committee, or Board of Directors	164
	Interaction with Human Resources	164
	Summary	165
	References	166
Chapter 7	Authentication and Authorization	167
	Authentication	167
	Usernames and Passwords	168
	Certificate-Based Authentication	175
	Extensible Authentication Protocol (EAP)	180
	Biometrics	180
	Additional Uses for Authentication	181
	Authorization	182
	User Rights	182
	Role-Based Authorization (RBAC)	182
	Access Control Lists (ACLs)	183
	Rule-Based Authorization	186
	Compliance with Standards	186
	NIST	186
	ISO 27002	186
	COBIT	187
	Summary	187
	References	188

Part II Data Security

Chapter 8	Securing Unstructured Data	191
	Structured Data vs. Unstructured Data	191
	At Rest, in Transit, and in Use	193
	Approaches to Securing Unstructured Data	194
	Databases	195
	Applications	198
	Networks	201
	Computers	202
	Storage (Local, Removable, or Networked)	203
	Data Printed into the Physical World	205

	Newer Approaches to Securing Unstructured Data	207
	Data Loss Prevention (DLP)	207
	Information Rights Management (IRM)	208
	Summary	209
	References	210
Chapter 9	Information Rights Management	211
	Overview	212
	The Difference Between DRM and IRM	212
	What's in a Name? EDRM, ERM, RMS, IRM	215
	Evolution from Encryption to IRM	216
	IRM Technology Details	217
	What Constitutes an IRM Technology?	217
	Architecture	218
	Going Offline	230
	Unstructured Data Formats	231
	Getting Started with IRM	232
	Classification Creation	232
	User Provisioning	233
	Rights Assignment	234
	Securing Content	235
	Distributing Content	236
	Installing and Configuring the IRM Client	236
	Authentication	236
	Authorization	237
	Rights Retrieval and Storage	237
	Content Access and Rights Invocation	237
	Access Auditing and Reporting	238
	Rights Revocation	238
	Summary	238
	References	239
Chapter 10	Encryption	241
	A Brief History of Encryption	241
	Early Codes	242
	More Modern Codes	243
	Symmetric-Key Cryptography	243
	Key Exchange	245
	Public Key Cryptography	245
	Key Exchange	246
	Public Key Infrastructure	247
	Structure and Function	247
	CA Hierarchy	247

	Certificate Templates and Enrollment	248
	Revocation	248
	Role Separation	249
	Cross-Certification	249
	Compliance with Standards	249
	NIST	250
	ISO 27002	250
	COBIT	250
	Summary	251
	References	251
Chapter 11	Storage Security	253
	Storage Security Evolution	253
	Modern Storage Security	255
	Storage Infrastructure	255
	Administration Channel	260
	Risks to Data	260
	Risk Remediation	261
	Confidentiality Risks	262
	Integrity Risks	266
	Availability Risks	267
	Best Practices	270
	Zoning	270
	Arrays	270
	Servers	270
	Staff	271
	Offsite Data Storage	271
	Summary	271
	References	271
Chapter 12	Database Security	273
	General Database Security Concepts	273
	Understanding Database Security Layers	275
	Server-Level Security	275
	Network-Level Security	275
	Operating System Security	277
	Understanding Database-Level Security	278
	Database Administration Security	279
	Database Roles and Permissions	279
	Object-Level Security	281
	Using Other Database Objects for Security	283
	Using Application Security	285
	Limitations of Application-Level Security	286
	Supporting Internet Applications	287

Database Backup and Recovery	289
Determining Backup Constraints	290
Determining Recovery Requirements	290
Types of Database Backups	291
Keeping Your Servers Up to Date	292
Database Auditing and Monitoring	292
Reviewing Audit Logs	293
Database Monitoring	293
Summary	294
References	295

Part III Network Security

Chapter 13	Secure Network Design	299
	Introduction to Secure Network Design	300
	Acceptable Risk	300
	Designing Security into a Network	301
	Designing an Appropriate Network	302
	The Cost of Security	302
	Performance	303
	Availability	306
	Security	308
	Wireless Impact on the Perimeter	309
	Remote Access Considerations	311
	Internal Security Practices	311
	Intranets, Extranets, and DMZs	313
	Outbound Filtering	315
	Compliance with Standards	317
	NIST	317
	ISO 27002	318
	COBIT	319
	Summary	319
	References	319
Chapter 14	Network Device Security	321
	Switch and Router Basics	321
	MAC Addresses, IP Addresses, and ARP	322
	TCP/IP	323
	Hubs	325
	Switches	326
	Routers	327
	Network Hardening	330
	Patching	330
	Switch Security Practices	330
	Access Control Lists	331
	Disabling Unused Services	331

	Administrative Practices	333
	Internet Control Message Protocol (ICMP)	337
	Anti-Spoofing and Source Routing.	339
	Logging	340
	Summary.	340
	References	340
Chapter 15	Firewalls	343
	Overview	343
	The Evolution of Firewalls.	344
	Application Control.	345
	Must-Have Firewall Features	346
	Core Firewall Functions.	347
	Network Address Translation (NAT)	347
	Auditing and Logging	350
	Additional Firewall Capabilities	350
	Application and Website Malware Execution Blocking.	350
	Antivirus	351
	Intrusion Detection and Intrusion Prevention	351
	Web Content (URL) Filtering and Caching	351
	E-Mail (Spam) Filtering.	351
	Enhance Network Performance	351
	Firewall Design	351
	Firewall Strengths and Weaknesses.	352
	Firewall Placement.	353
	Firewall Configuration.	353
	Summary.	353
	References	354
Chapter 16	Virtual Private Networks	355
	How a VPN Works	355
	VPN Protocols.	356
	IPSec.	357
	PPTP	359
	L2TP over IPSec.	359
	SSL VPNs	359
	Remote Access VPN Security.	360
	Authentication Process	361
	Client Configuration	362
	Client Networking Environment	364
	Offline Client Activity	368
	Site-to-Site VPN Security	368
	Summary.	370
	References	370
Chapter 17	Wireless Network Security	371
	Radio Frequency Security Basics.	372
	Security Benefits of RF Knowledge.	372
	Layer One Security Solutions	373

Data-Link Layer Wireless Security Features, Flaws, and Threats	383
802.11 and 802.15 Data-Link Layer in a Nutshell	383
802.11 and 802.15 Data-Link Layer Vulnerabilities and Threats	385
Closed-System SSIDs, MAC Filtering, and Protocol Filtering	386
Built-in Bluetooth Network Data-Link Security and Threats	386
Wireless Vulnerabilities and Mitigations	387
Wired Side Leakage	387
Rogue Access Points	388
Misconfigured Access Points	389
Wireless Phishing	389
Client Isolation	390
Wireless Network Hardening Practices and Recommendations	390
Wireless Security Standards	390
Temporal Key Integrity Protocol and Counter Mode with CBC-MAC Protocol	391
802.1x-Based Authentication and EAP Methods	391
Wireless Intrusion Detection and Prevention	393
Wireless IPS and IDS	394
Bluetooth IPS	395
Wireless Network Positioning and Secure Gateways	396
Summary	397
References	397
Chapter 18 Intrusion Detection and Prevention Systems	399
IDS Concepts	399
Threat Types	400
First-Generation IDS	404
Second-Generation IDS	405
IDS Types and Detection Models	406
Host-Based IDS	406
Network-Based IDS (NIDS)	407
Anomaly-Detection (AD) Model	409
Signature-Detection Model	410
What Type of IDS Should You Use?	413
IDS Features	413
IDS End-User Interfaces	413
Intrusion-Prevention Systems (IPS)	414
IDS Management	415
IDS Logging and Alerting	417
IDS Deployment Considerations	418
IDS Fine-Tuning	418
IPS Deployment Plan	419

	Security Information and Event Management (SIEM)	420
	Data Aggregation	421
	Analysis	423
	Operational Interface	424
	Additional SIEM Features	424
	Summary	425
	References	426
Chapter 19	Voice over IP (VoIP) and PBX Security	427
	Background	428
	VoIP Components	430
	Call Control	430
	Voice and Media Gateways and Gatekeepers	431
	MCUs	432
	Hardware Endpoints	433
	Software Endpoints	434
	Call and Contact Center Components	434
	Voicemail Systems	435
	VoIP Vulnerabilities and Countermeasures	436
	Old Dogs, Old Tricks: The Original Hacks	437
	Vulnerabilities and Exploits	438
	The Protocols	441
	Security Posture: System Integrators and Hosted VoIP	450
	PBX	456
	Hacking a PBX	456
	Securing a PBX	457
	TEM: Telecom Expense Management	457
	Summary	458
	References	459
Part IV	<u>Computer Security</u>	
Chapter 20	Operating System Security Models	463
	Operating System Models	463
	The Underlying Protocols Are Insecure	464
	Access Control Lists	465
	MAC vs. DAC	466
	Classic Security Models	467
	Bell-LaPadula	467
	Biba	468
	Clark-Wilson	468
	TCSEC	468
	Labels	470
	Reference Monitor	471
	The Reference Monitor Concept	471
	Windows Security Reference Monitor	472

	Trustworthy Computing	472
	International Standards for Operating System Security	473
	Common Criteria	473
	Summary	476
	References	476
Chapter 21	Unix Security	477
	Start with a Fresh Install	477
	Securing a Unix System	478
	Reducing the Attack Surface	479
	Install Secure Software	481
	Configure Secure Settings	486
	Keep Software Up to Date	493
	Place Servers into Network Zones	493
	Strengthen Authentication Processes	493
	Require Strong Passwords	494
	Use Alternatives to Passwords	495
	Limit Physical Access to Systems	495
	Limit the Number of Administrators and Limit the Privileges of Administrators	495
	Use sudo	495
	Back Up Your System	496
	Subscribe to Security Lists	496
	Compliance with Standards	496
	ISO 27002	496
	COBIT	497
	Summary	498
	References	498
Chapter 22	Windows Security	499
	Securing Windows Systems	499
	Disable Windows Services and Remove Software	500
	Securely Configure Remaining Software	501
	Use Group Policy to Manage Settings	508
	Computer Policies	508
	User Policies	510
	Security Configuration and Analysis	512
	Group Policy	514
	Install Security Software	517
	Application Whitelisting	518
	Patch Systems Regularly	518
	Segment the Network into Zones of Trust	519
	Blocking and Filtering Access to Services	519
	Mitigating the Effect of Spoofed Ports	519

	Strengthen Authentication Processes	520
	Require, Promote, and Train Users in Using Strong Passwords . . .	520
	Use Alternatives to Passwords	522
	Apply Technology and Physical Controls	
	to Protect Access Points	523
	Modify Defaults for Windows Authentication Systems	524
	Limit the Number of Administrators	
	and Limit the Privileges of Administrators	525
	Applications that Require Admin Access to Files	
	and the Registry	525
	Elevated Privileges Are Required	526
	Programmers as Administrators	526
	Requiring Administrators to Use runas	526
	Active Directory Domain Architecture	527
	Logical Security Boundaries	527
	Role-Based Administration	534
	A Role-Based Approach to Security Configuration	535
	Compliance with Standards	537
	NIST	537
	ISO 27002	538
	COBIT	539
	Summary	540
	References	540
Chapter 23	Securing Infrastructure Services	543
	E-Mail	543
	Protocols, Their Vulnerabilities, and Countermeasures	544
	Spam and Spam Control	558
	Malware and Malware Control	561
	Web Servers	562
	Types of Attacks	562
	Web Server Protection	565
	DNS Servers	567
	Install Patches	568
	Prevent Unauthorized Zone Transfers	568
	DNS Cache Poisoning	569
	Proxy Servers	569
	HTTP Proxy	570
	FTP Proxy	570
	Direct Mapping	570
	POP3 Proxy	570
	HTTP Connect	571
	Reverse Proxy	571
	Summary	572
	References	573

Chapter 24	Virtual Machines and Cloud Computing	575
	Virtual Machines	575
	Protecting the Hypervisor	576
	Protecting the Guest OS	576
	Protecting Virtual Storage	577
	Protecting Virtual Networks	577
	NIST Special Publication 800-125	577
	Cloud Computing	578
	Types of Cloud Services	579
	Cloud Computing Security Benefits	579
	Security Considerations	580
	Cloud Computing Risks and Remediations	582
	Summary	595
	References	595
Chapter 25	Securing Mobile Devices	597
	Mobile Device Risks	597
	Device Risks	598
	Application Risks	599
	Mobile Device Security	600
	Built-in Security Features	600
	Mobile Device Management (MDM)	603
	Data Loss Prevention (DLP)	606
	Summary	606
	References	607
Part V	Application Security	
Chapter 26	Secure Application Design	611
	Secure Development Lifecycle	611
	Application Security Practices	613
	Security Training	613
	Secure Development Infrastructure	613
	Security Requirements	613
	Secure Design	613
	Threat Modeling	613
	Secure Coding	614
	Security Code Review	614
	Security Testing	614
	Security Documentation	614
	Secure Release Management	614
	Dependency Patch Monitoring	614
	Product Security Incident Response	615
	Decisions to Proceed	615

	Web Application Security	615
	SQL Injection	615
	Forms and Scripts	620
	Cookies and Session Management	623
	General Attacks	624
	Web Application Security Conclusions	625
	Client Application Security	625
	Running Privileges	626
	Application Administration	626
	Integration with OS Security	627
	Application Updates	628
	Remote Administration Security	629
	Reasons for Remote Administration	629
	Remote Administration Using a Web Interface	630
	Authenticating Web-Based Remote Administration	630
	Custom Remote Administration	631
	Summary	632
	References	633
Chapter 27	Writing Secure Software	635
	Security Vulnerabilities: Causes and Prevention	635
	Buffer Overflows	636
	Integer Overflows	639
	Cross-Site Scripting	643
	SQL Injection	649
	Whitelisting vs. Blacklisting	652
	Summary	653
	References	653
Chapter 28	J2EE Security	655
	Java and J2EE Overview	655
	The Java Language	655
	Attacks on the JVM	657
	The J2EE Architecture	658
	Servlets	658
	JavaServer Pages (JSP)	660
	Enterprise JavaBeans (EJB)	661
	Containers	662
	Authentication and Authorization	664
	J2EE Authentication	664
	J2EE Authorization	666

	Protocols	667
	HTTP	668
	HTTPS	670
	Web Services Protocols	671
	IIOP	672
	JRMP	674
	Proprietary Communication Protocols	675
	JMS	675
	JDBC	676
	Summary	676
	References	677
Chapter 29	Windows .NET Security	679
	Core Security Features of .NET	679
	Managed Code	679
	Role-Based Security	684
	Code Access Security	687
	AppDomains and Isolated Storage	696
	Application-Level Security in .NET	699
	Using Cryptography	699
	.NET Remoting Security	708
	Securing Web Services and Web Applications	708
	Summary	712
	References	712
Chapter 30	Controlling Application Behavior	713
	Controlling Applications on the Network	713
	Access Control Challenges	714
	Application Visibility	716
	Controlling Application Communications	716
	Restricting Applications Running on Computers	718
	Application Whitelisting Software	718
	Application Security Settings	720
	Summary	722
	References	723
	<u>Part VI</u> Security Operations	
Chapter 31	Security Operations Management	727
	Communication and Reporting	727
	Change Management	730
	Acceptable Use Enforcement	732
	Examples of Acceptable Use Enforcement	732
	Proactive Enforcement	733
	Administrative Security	733
	Preventing Administrative Abuse of Power	734

	Management Practices	734
	Accountability Controls	735
	Security Monitoring and Auditing	736
	Keeping Up with Current Events	741
	Incident Response	741
	Summary	743
	References	744
Chapter 32	Disaster Recovery, Business Continuity, Backups, and High Availability	745
	Disaster Recovery	746
	Business Continuity Planning	746
	The Four Components of Business Continuity Planning	747
	Third-Party Vendor Issues	750
	Awareness and Training Programs	750
	Backups	752
	Traditional Backup Methods	752
	Backup Alternatives and Newer Methodologies	756
	Backup Policy	757
	High Availability	758
	Automated Redundancy Methods	759
	Operational Redundancy Methods	761
	Compliance with Standards	762
	ISO 27002	762
	COBIT	762
	Summary	764
	References	765
Chapter 33	Incident Response and Forensic Analysis	767
	Incident Response	767
	Incident Detection	768
	Response and Containment	768
	Recovery and Resumption	770
	Review and Improvement	770
	Forensics	771
	Legal Requirements	771
	Evidence Acquisition	772
	Evidence Analysis	776
	Compliance with Laws During Incident Response	781
	Law Enforcement Referrals—Yes or No?	781
	Preservation of Evidence	782
	Confidentiality and Privilege Issues	784
	Summary	785
	References	786

Part VII Physical Security

Chapter 34	Physical Security	789
	Classification of Assets	789
	Physical Vulnerability Assessment	790
	Buildings	790
	Computing Devices and Peripherals	790
	Documents	791
	Records and Equipment	791
	Choosing Site Location for Security	791
	Accessibility	792
	Lighting	792
	Proximity to Other Buildings	793
	Proximity to Law Enforcement and Emergency Response	793
	RF and Wireless Transmission Interception	793
	Utilities Reliability	793
	Construction and Excavation	794
	Securing Assets: Locks and Entry Controls	794
	Locks	794
	Entry Controls	795
	Physical Intrusion Detection	796
	Closed-Circuit Television	796
	Alarms	797
	Compliance with Standards	797
	ISO 27002	797
	COBIT	798
	Summary	801
	References	801
	Glossary	803
	Index	833

This page intentionally left blank

Preface

Dear Reader, You hold in your hands a vast and thorough repository of knowledge and experience. Information security is an incredibly complicated and ever-changing subject, and this book tackles the entire subject. The original concept for this book was to provide a security blueprint or cookbook—a comprehensive guide for building a complete, effective security program. This second edition stays true to that idea. The book was written for people who, like myself once upon a time, find themselves in a position of having to secure an organization’s network, and start to realize there’s more to security than a firewall. The technologies are important, and they are complex and varied. But the nontechnical aspects of security are equally if not more important. Bruce Schneier famously said “Security is a process, not a product,” and I completely agree. I’d say the same thing about any business process. Technology can help an organization enforce its business goals and policies, but it is not, in and of itself, a magic solution to all problems. That’s why this book covers both technology and practice.

I envisioned the first edition of this book a decade ago and participated in writing it because I wanted to share with other IT professionals what I had learned in my first ten years in the field of information security, and the philosophies I developed along the way. After 20 years of practice, I’ve found that those lessons and philosophies still hold true: an organization needs security policies, a technology strategy that’s based on risk assessment, and the right technologies to plug all the holes inherent in the network. But it doesn’t end there—as a security professional, you need to change and manage the behaviors of the people who handle data. When you begin to contemplate that, you soon realize that what you’re really protecting are information assets—which may be electronic, or may take other forms such as paper and voice. A comprehensive approach is the only way to be successful. You have to look at the complete picture in order to really be effective. How do you get your arms around all that? Breaking it down into individual topics, and ensuring that every aspect is covered, from philosophy to strategy to technology to behaviors, is the approach I’ve taken. Everything is manageable when you carve it into bite-sized chunks that can be dealt with one at a time. This book covers everything you need to know in order to build a comprehensive, effective security program.

The first edition was written at the beginning of the millennium—when the Internet was transitioning from a business resource to a business necessity—to provide a comprehensive resource for IT administrators (which was not available anywhere else) by offering guidance on how to create, deploy, and monitor a security solution on a budget. This second edition remains true to that vision, with every aspect of information security represented and updated. This book was, and remains, the only cradle-to-grave network security reference that brings security strategies and tactics together in one resource. The holistic approach to security theory, combined with logical, concise, hands-on information, arms IT professionals with the knowledge they need to secure their infrastructure.

I hope this book provides you with valuable insight, perspective, and knowledge. I believe we are at our best when we share what we know.

Regards,
Mark Rhodes-Ousley

Acknowledgments

Profound thanks are offered to Zeke Rutman-Allen for going way above and beyond expectations to improve and modernize the entire networking section, and for delivering on commitments despite insane day-job requirements; Brenda Larcom for drastically reorganizing everything into a greatly improved and more intuitive table of contents (trust me, you'd thank her too if you could see the improvement); Marcia Wilson for providing excellent and admirable contributions on several chapters while juggling work, school, and family; Ayush Jain for last-minute reviews that saved the day; Barrington Allen for timely and quality reviews; Greg Hoban for last-minute reviews; Judy Gottlieb for helping organize the original outline; Eric Reither for giving Physical Security the once-over; Amy Jollymore for being the best editor I've ever had and for being a patient leader; Ms. Ryan Willard for over-and-above shepherding; Margie and Trent for being patient and supporting me throughout the entire endeavor while I immersed myself in writing, making them a "book widow" and "book orphan" for much of the two-year span this book required.

This page intentionally left blank

Introduction

Whether you are a security professional, an IT professional who wants to learn more about security, someone who has been thrust into a security role without preparation, an executive who wants to increase your organization's knowledge assets, a member of a sales force in a company that sells security products or services, or a technology, law, or business student or professor in a college or university, this book was written for you.

Students and professionals alike need a comprehensive guide to all aspects of security, and this second edition fulfills corporate and academic needs with updated material. Colleges now offer dedicated information security programs, yet they don't have access to a comprehensive security textbook. Organized with academic institutions in mind, this book is an important resource for the security professionals of the future, and it is still the only comprehensive book on security. This book takes a vendor-neutral approach in order to improve the lifespan and applicability of the material without "favoritism" to particular products.

A typical reader of this book would be a networking or technology professional put in charge of deploying and managing network security within their company. Due to cuts in IT budgets, many IT professionals are being tasked with assessing and deploying network security solutions for their company. Millions of IT professionals in small, midsize, and large companies are finding themselves in charge of network security but are ill-equipped to handle these responsibilities. Many of these IT professionals do not possess enough training to successfully secure their networks from both internal and external attacks. This book contains everything they need to know about information security.

What This Book Covers

This book covers all aspects of information security, from concept to details. It includes methodology, analysis, and technical details to fit the reader's needs. Equally applicable to the beginner and the seasoned professional, this book provides a one-stop reference that replaces and obsoletes other books.

The practice of information security has grown in depth and breadth since the first edition. New standards and regulations have appeared, as have new technologies. Most security practitioners find themselves in the position of needing to comply with these new standards and regulations and secure new technologies. This book covers information security standards, including COBIT, ISO 27000, and NIST, regulations such as Gramm-Leach-Bliley (GLBA), Sarbanes-Oxley (SOX), HIPAA, NERC CIP, and PCI DSS, and a variety of state, federal, and international laws. Organizing around these standards and

regulations improves this book's practicality and usefulness as a professional reference. In addition, many organizations use IT Infrastructure Library (ITIL) practices to improve the quality of their processes, and this book shows how ITIL can be integrated with security to produce successful results.

How to Use This Book

Start with Chapter 1 to understand the philosophy and methodology that inform the core principles and practices of a successful and effective security program, and then skim the rest of Part I to learn more about the subjects that are important to you. Then, jump to the chapters that are particularly relevant to your situation for a deeper dive. This book is meant to be a desk reference that you can pick up at any time to find the guidance you need.

For instructors, the publisher has created Instructor Teaching Materials, which you can download from this book's McGraw-Hill web page at www.mhprofessional.com/InfoSecurity2e.

How This Book Is Organized

The seven parts of this book are organized into conceptually related subject groups, beginning with the most basic, comprehensive material that every security practitioner should know, and proceeding through the layers of infrastructure that are found in IT—data, network, computers, applications, people, and facilities—with techniques to secure the components found in each layer.

Part I: Foundations starts with the fundamentals of security. I encourage you to read at least the first four chapters, regardless of which particular subjects interest you. To see the whole picture, you need to understand the rationale and philosophy behind the best practices. The overview given in Chapter 1 expresses the importance of security and the best way to go about it. Risk analysis follows in Chapter 2, because it should be the first step before you do anything else. The discussion of compliance with standards, regulations, and laws in Chapter 3 provides guidance to those who need to avoid legal risk. Chapter 4 offers secure design principles, which describe how to plan for security. Security policies (Chapter 5) form the core set of requirements needed for a security program. Chapter 6 provides insights into how to staff, resource, and support the security function. Authentication and authorization (Chapter 7) form the basis for restricting access based on need.

Part II: Data Security provides guidance on protecting the most valuable assets on the network: data. Chapter 8 describes techniques to protect data on its own outside of a structured environment. Information rights management, covered in Chapter 9, gives a new option for protecting data in the wild. Encryption (Chapter 10) is the tried-and-true approach to protecting the confidentiality of data, and storage security (Chapter 11) and database security (Chapter 12) provide best practices for protecting data within their borders.

Part III: Network Security (Chapters 13–19) covers the security of the network infrastructure itself, including secure network design, network device security, firewalls, virtual private networks, wireless networks, intrusion detection and prevention, and voice security.

Part IV: Computer Security (Chapters 20–25) dives into operating system security models, Unix security, Windows security, securing infrastructure services, virtual machines and cloud computing, and securing mobile devices.

Part V: Application Security (Chapters 26–30) takes on secure application design, writing secure software, J2EE security, Windows .NET security, and controlling application behavior.

Part VI: Security Operations (Chapters 31–33) addresses security operations management, disaster recovery, business continuity, backups, high availability, incident response, and forensic analysis.

Part VII: Physical Security (Chapter 34) describes how to protect the premises in which computers and people reside.

The end of the book includes a comprehensive security glossary, for easy lookup of any acronym or term you may be unfamiliar with.

This page intentionally left blank

PART

I

Foundations

CHAPTER 1

Information Security
Overview

CHAPTER 2

Risk Analysis

CHAPTER 3

Compliance with Standards,
Regulations, and Laws

CHAPTER 4

Secure Design Principles

CHAPTER 5

Security Policies, Standards,
Procedures, and Guidelines

CHAPTER 6

Security Organization

CHAPTER 7

Authentication and
Authorization

This page intentionally left blank

CHAPTER

1

Information Security Overview

There are a few key questions that you need to ask before embarking on any security endeavor. What are you trying to protect? Why are you trying to protect it? How will you protect it? This chapter helps you to address those questions by covering some background information and axioms, ideologies, reasoning, values, and viewpoints you should keep in mind whenever you are considering security tools and techniques. The following sections explain why information is important, the historical context of information protection, methodologies that are used to maximize the effectiveness of security implementations, and how to define and describe the value of the security investment. By keeping these concepts in mind when you refer to this book and when you put this book's practices into operation, you will enhance your success and be able to defend your decisions and choices.

NOTE Words in italics are specialized terms that are defined at the end of this book, in the Security Dictionary. Check the Dictionary for clarification on what these italicized terms mean.

The Importance of Information Protection

Information is an important asset. The more information you have at your command, the better you can adapt to the world around you. In business, information is often one of the most important assets a company possesses. Information differentiates companies and provides leverage that helps one company become more successful than another.

Information can be classified into different categories, as described in Chapter 5. This is typically done in order to control access to the information in different ways, depending on its importance, its sensitivity, and its vulnerability to theft or misuse. Organizations typically choose to deploy more resources to control information that has higher sensitivity. The U.S. government, for example, uses a five-level classification system that progresses from Unclassified information (which everyone can see) to Top Secret information (to which only the most trusted people have access).

Organizations classify information in different ways in order to differently manage aspects of its handling, such as labeling (whether headers, footers, and watermarks specify how it should be handled), distribution (who gets to see it), duplication (how copies are made and handled), release (how it is provided to outsiders), storage (where it is kept), encryption (if required), disposal (whether it is shredded or strongly wiped), and methods of transmission (such as e-mail, fax, print, and mail). The specifics are spelled out in an organization's information classification and handling policy, which represents a very important component of an organization's overall security policy.

Information intended for internal use only is usually meant to be seen by employees, contractors, and service providers, but not by the general public. Examples include internal memos, correspondence, general e-mail and instant message discussions, company announcements, meeting requests, and general presentation materials. This type of information is typically the least restricted—because spending a lot of time and money on protecting it doesn't outweigh the value of the information or the risk of its disclosure.

Companies may have *confidential information*, such as research and development plans, manufacturing processes, strategic corporate information, product roadmaps, process descriptions, customer lists and contact information, financial forecasts, and earnings announcements, that is intended for internal use on a need-to-know basis. Loss or theft of confidential information could violate the privacy of individuals, reduce the company's competitive advantage, or cause damage to the company. This type of information is available to external audiences only for business-related purposes and only after entering a nondisclosure agreement (NDA) or equivalent obligation of confidentiality.

Specialized information or *secret information* may include trade secrets, such as formulas, production details, and other intellectual property, proprietary methodologies and practices that describe how services are provided, research plans, electronic codes, passwords, and encryption keys. If disclosed, this type of information may severely damage the company's competitive advantage. It is usually restricted to only a few people or departments within a company and is rarely disclosed outside the company.

Egg on Their Faces: A Case Study

Egghead Software was a well-known software retailer who discovered in 2000 that Internet attackers might have stolen as many as 3.7 million credit card numbers from its web site, housed offsite at an e-commerce service provider that lacked good security.

This information quickly made the news, and as a result, Egghead's corporate identity was more than just tarnished—it was destroyed. Customers fled in droves. The media coverage ruined the company's reputation. Egghead's stock price dropped dramatically, along with its sales. Cost-cutting measures, including layoffs, followed. The chain reaction finally concluded with Egghead's bankruptcy and subsequent acquisition by Amazon.com.

Were the consequences of inattention to security too extreme? You be the judge. But could those consequences have been avoided with good security practices? Absolutely.

In some business sectors, the protection of information is not just desirable, it's mandatory. For example, health care organizations are heavily regulated and must comply with the security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). They are required by HIPAA to ensure robust security over *protected health information (PHI)* that consists of medical data and *personally identifiable information (PII)*. Financial institutions are also required by regulations to protect customer information, PII, and financial records. These regulations include security rules defined by the Federal Financial Institutions Examination Council (FFIEC), and the Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999. Regulations such as the Sarbanes-Oxley Act of 2002 (also known as SOX or Sarbox) also apply to many companies that are publicly traded, to protect shareholders against the dissemination of false financial information. Other legal regulations include SB 1386 and SB 24, which are California laws requiring companies to protect personal information. All of these regulations carry penalties, some of which are strong, for failure to properly protect information. (Chapter 3 covers these and other regulatory requirements in more detail.) The proliferation of information security regulations around the world is an indicator of the importance of protecting data.

The better your security controls are that protect all these different types of data, the greater the level of access that you can safely provide to authorized parties who need to use that data. Likewise, third parties can give you more access to their data if it's secure. The higher the mutual trust, the more access you can safely provide to external parties such as your customers, suppliers, business partners, vendors, consultants, employees, and contractors. In this global and increasingly digital age, the ability to provide this secure and trusted access is no longer a differentiator, but a business necessity.

The Evolution of Information Security

In the early days of networking, individual computers were connected together only in academic and government environments. Thus, at that time, the networking technologies that were developed were specific to academic and government environments. Originally, the academic security model was “wide open” and the government security model was “closed and locked.” There wasn't much in between. The government was mainly concerned with blocking access to computers, restricting internal access to confidential data, and preventing interception of data (for example, by shielding equipment to prevent electromagnetic radiation from being intercepted). This method of protecting assets provided a hard-to-penetrate perimeter, as depicted in Figure 1-1.

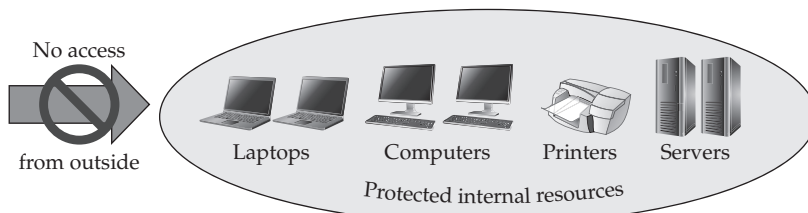


Figure 1-1 Original government perimeter blockade model

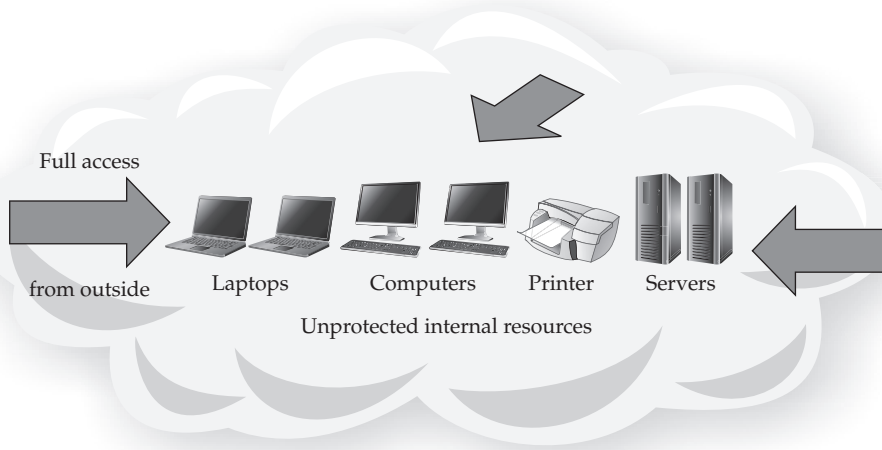


Figure 1-2 Original academic open-access model

In the academic world, the goal was to share information openly, so security controls were limited to accounting functions in order to charge money for the use of computer time. Figure 1-2 shows the original security model for academic institutions. Compare this model with the government model shown in Figure 1-1. Note that these two models are diametrically opposite—the government model blocks everything, while the academic model allows everything. There is plenty of room in between these two extremes.

In the field of computer security, the practices established by the academic and government institutions persisted until the early 1990s, and some of those practices are still around today. Those practices that have endured continue to have their place in a comprehensive security strategy, but they are no longer sufficient to meet the needs of the modern computer network.

Dangers of the Academic Open-Access Model: A Case Study

InterNex was an Internet service provider (ISP) headquartered in Palo Alto, California. The only security control it employed was basic username and password authentication. It had designed its network intentionally to allow unrestricted access. This was a philosophical decision. The ideology of InterNex was that the Internet should be open to everyone.

Unfortunately for InterNex, the open-access philosophy had consequences. Many of its systems were compromised by attackers who were able to guess the passwords of various user accounts. One of the most famous attackers in history, Kevin Mitnick, used InterNex's compromised systems to disguise his identity while attacking other networks, including during the 1994 *IP spoofing attack* against computers in San Diego. Mitnick was eventually captured and served five years in jail.

When businesses started to widely embrace the Internet as a sales channel and business tool in the early-to-mid 1990s, a new security model was required. A closed-door approach doesn't work when you need to allow thousands or millions of people to have access to the services on your network. Likewise, an open-door approach doesn't work when you need to protect the privacy of each individual who interacts with the services on your network. E-commerce and business required a more blended approach of providing limited access to data in a controlled fashion, which is a more sophisticated and complex approach than that used by the earlier security models. To use the analogy of a house, consider the complexity of allowing certain authorized parties (like utility companies, cleaning staff, or caterers) to get into your house while still keeping out burglars and vandals. Isn't it easier just to keep all your doors locked (as in the old government model) or to leave them all unlocked (as in the academic model)? Partial controlled access requires authentication, authorization, and privacy—and more complexity. How would you design the security of a house to provide multilevel, complex, granular access, visibility, and control?

As the use of information technologies evolved, the original all-or-nothing approaches to security no longer met the needs of information consumers. So, the practice of network security evolved. The concepts of intranets and extranets were developed to accommodate internal and external customers, respectively, with secured boundaries that resembled miniature versions of the firewall perimeter. Virtual private networks (VPNs) were developed to provide a secure channel (or tunnel) from one network to another. These approaches continued through the end of the 1990s to the early part of the 2000s, after which the first edition of this book was published in late 2003.

Throughout the first decade of the 21st century, the Internet continued to become an increasingly critical business platform, and the network became more of a key business component. As more companies started doing business on the Internet, concepts such as *Software-as-a-Service (SaaS)* were developed to provide business services over the Internet. And the threats found on the Internet evolved as well. Basic *viruses* and *worms* along with the simple *exploits* and *man-in-the-middle* attacks found in the decade of the 1990s became more sophisticated, effective, and ubiquitous.

Which brings us to today. Business partners need to share information with your company, and often with each other as well. Employees, consultants, contractors, service providers, system integrators, and other entities that augment a company's resources all need to collaborate with a pool of information. The better the distribution vehicle for that information, the more business opportunities that can be accessed by the company. Customers require secure access to the information that they need. A secure data network allows a company to distribute information quickly and effectively throughout the organization, to business partners, and to customers. Figure 1-3 characterizes the interconnectedness among data, computers, networks, and information consumers.

SaaS offerings have become just as prevalent as in-house services—in fact, they are increasingly more prevalent. Companies are choosing to leverage existing service offerings on the Internet rather than build their own. *Social networking* is becoming a powerful marketing force. And *cloud computing* is moving the boundaries of the network even further away from the data center. This global interconnectedness requires a different perspective on security—we can no longer build virtual walls around our networks. Instead, security must be pervasive, built into every aspect of information processing. And the security

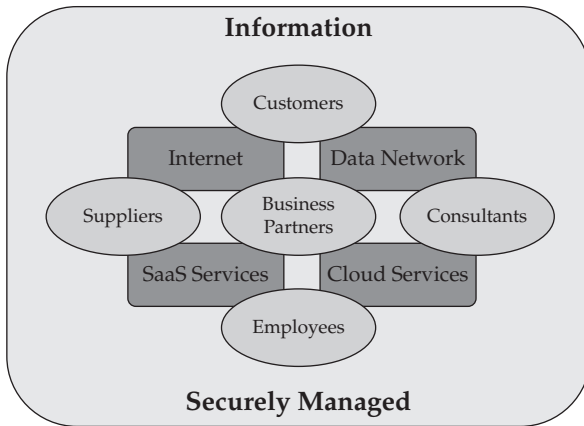


Figure 1-3 Modern information is shared among many consumers, via many channels.

threats to all these information resources have evolved at a rate equal to or greater than the technologies themselves. (Chapter 2 covers modern threats in detail.)

Modern security products are now designed to balance the needs of business on the Internet while protecting against today's sophisticated threats. Modern information security practices have evolved into a blended approach to managing access to information. Technology and information are blended into everyday life, and they can no longer be kept in a locked box or left unprotected.

Justifying Security Investment

How do you justify spending money on security? That is perhaps the most challenging, and debated, topic in the field of information security. First there was FUD—fear, uncertainty, and doubt. Without really measuring anything or delivering specific results, executives were simply frightened into spending money. That didn't last long. Soon thereafter, *return on investment (ROI)* was used as an attempt to market security as an investment that “pays for itself.” This was the standard approach to justifying information technology budgets, but it never translated well to security. There is really no good way to demonstrate a monetary amount gained by spending money on security. So, ROI was combined with annualized loss expectancy (ALE), a risk measurement strategy that combines the frequency (or probability) of a loss with the cost of that loss, to produce a yearly expected monetary value. The problem was that too much guesswork went into ALE, and losses don't distribute themselves evenly from year to year, so ALE estimates were really not defensible.

The “insurance analogy” was developed as an alternative to value-based security justifications. People and businesses spend money on insurance—often as much as 10 percent of the value of the asset per year—even though they may never have a claim to file. They spend this money for peace of mind, knowing that they will be covered in the event of a problem. Likewise, businesses spend money on security because it's insurance against

misuse of their assets. How do you measure the value of that insurance? It certainly has value, but it's hard to quantify. The Egghead Software case study presented earlier in this chapter is a good example of how failure to focus on security can cause a major business loss that greatly exceeds the value of the assets themselves.

So, where does that leave us? The business benefits of security are hard to express in terms of a simple monetary value. Instead, consider this justification for security spending: good security practices *enable* business. They allow the business to prosper. They help provide a solid foundation upon which the business can expand and grow. Robust information security practices not only reduce risks and costs, but also provide new opportunities for revenue. In the past, security was thought of only in the context of *protection* (blocking access, closing holes, segmenting and separating systems and networks, and denying connections). Today that view has evolved to focus on enabling business on a global scale, using new methods of communication. By improving access to the information that drives its business, every company can expand its business influence on a global scale, regardless of the company's size or location. Information, one of the important assets a company possesses, is even more valuable when shared with those authorized to have it. Modern security practices provide information to those who need it without exposing it to those who should not have it.

Good security practices allow companies to perform their operations in a more integrated manner, especially with their customers. By carefully controlling the level of access provided to each individual customer, a company can expand its customer base and the level of service it can provide to each individual customer, without compromising the safety and integrity of its business interests, its reputation, and its customers' assets. Specific benefits of a strong security program are business agility, cost reduction, and portability.

Business Agility

Today, every company wants to open up its business operations to its customers, suppliers, and business partners, in order to reach more people and facilitate the expansion of revenue opportunities. For example, manufacturers want to reach individual customers and increase sales through e-commerce web sites. Web sites require connections to back-end resources like inventory systems, customer databases, and material and resource planning (MRP) applications. Extranets need to allow partners and contractors to connect to development systems, source code, and product development resources. And SaaS applications deliver business process tools over the Internet to customers.

Knowledge is power—in business, the more you know, the better you can adapt. Strong security provides insight into what is happening on the network and, consequently, in the enterprise. Weak security leaves many companies blind to the daily flow of information to and from their infrastructure. If a company's competitors have better control of their information, they have an advantage. The protection of a company's information facilitates new business opportunities, and business processes require fewer resources when managed efficiently and securely. Contemporary security technologies and practices make life easier, not harder.

Security allows information to be used more effectively in advancing the goals of organization because that organization can safely allow more outside groups of people to utilize the information when it is secure. The more access you provide, the more people you

can reach—and that means you can do more with less. Automation of business processes, made *trustworthy* by appropriate security techniques, allows companies to focus on their core business. Interconnecting productivity tools opens up new levels of operational effectiveness, and a responsible security program enables that effectiveness without exposure to undue risk.

When all levels of company management strongly support security, have a fundamental knowledge of security principles, and place a high value on security practices, the greatest gain is realized.

Cost Reduction

Modern security practices do reduce some costs, such as those resulting from loss of data or equipment. Data loss due to mishandling, misuse, or mistakes can be expensive. A rampant virus outbreak, a web site outage, or a denial of service (DoS) attack can result in service outages during which customers cannot make purchases and the company cannot transact business. Perhaps even worse, the service outage may attract unwelcome press coverage. The consequences of a security compromise can be significant. A publicized security incident can severely damage the credibility of a company, and thus its ability to acquire and retain customers.

An increasing number of attacks are categorized as *advanced persistent threats (APTs)*. These attacks are designed to deploy malware into a network and remain undetected until triggered for some malicious purpose. Often, the goal of the attacks is theft of financial information or intellectual property. Loss of service or leakage of sensitive data can result in fines, increased fees, and an overall decrease in corporate reputation and stock price. Strong security reduces loss of information and increases service availability and confidentiality.

Portability

Portability means that software and data can be used on multiple platforms or can be transferred/transmitted within an organization, to a customer, or to a business partner. The “consumerization” of information has placed demands on companies to be able to provide meaningful and accurate information at a moment’s notice.

A survey of CIOs and CISOs in 2011 concluded that the single biggest driver of information security spending over the preceding three years was client requirement, meaning that customers want to buy products and services from companies that have good security, and will in fact sometimes require evidence of security practices before completing a purchase.

To meet the demands of today’s businesses and consumers, architectures and networks need to be designed with security controls baked in as part of the development process. Clearly, this level of broad access to information resources requires a well-thought-out and properly deployed security program. With sound security built in from the ground up, portability of data as a key benefit can be realized.

Portability also enables business and creates value. For example, Apple’s ability to both host music and allow personal music libraries to be synchronized to a tablet, mobile phone, and MP3 player has greatly increased Apple’s bottom line. Security for mobile platforms affords users the opportunity to take their music everywhere while protecting the interests of the business by preventing unauthorized downloading of copyrighted material.