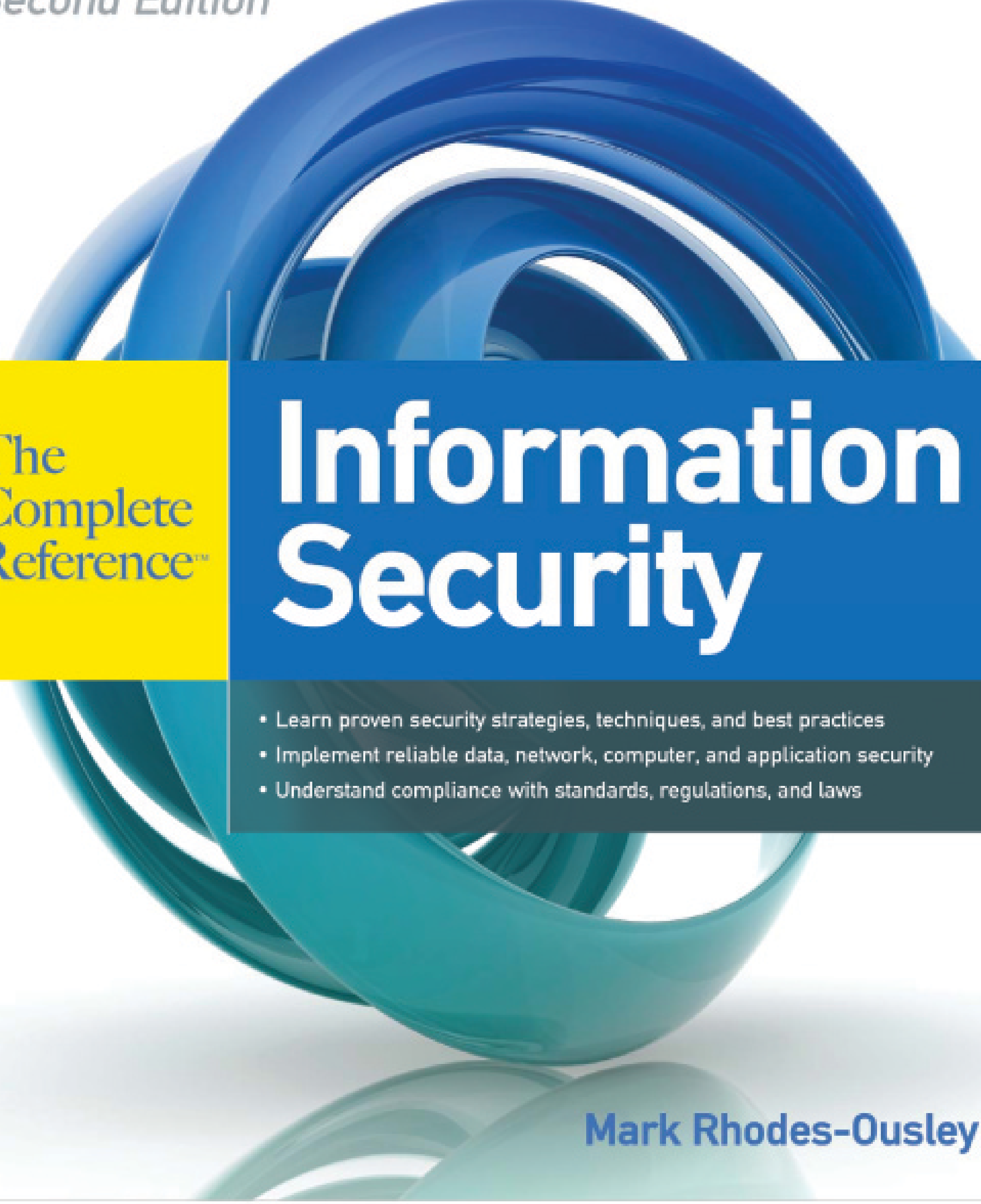
Second Edition



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.komodia.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

Mc Graw Hill Education

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

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.

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 V Application Security

Part VI Security Operations

Part VII Physical Security

Contents

Part II Data Security

Part IV Computer Security

Part V Application Security

Part VII Physical Security

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

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.

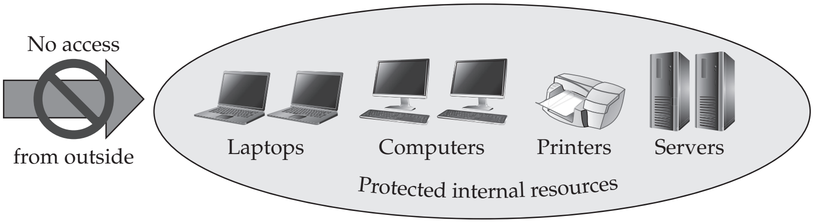


Figure 1-1 Original government perimeter blockade model

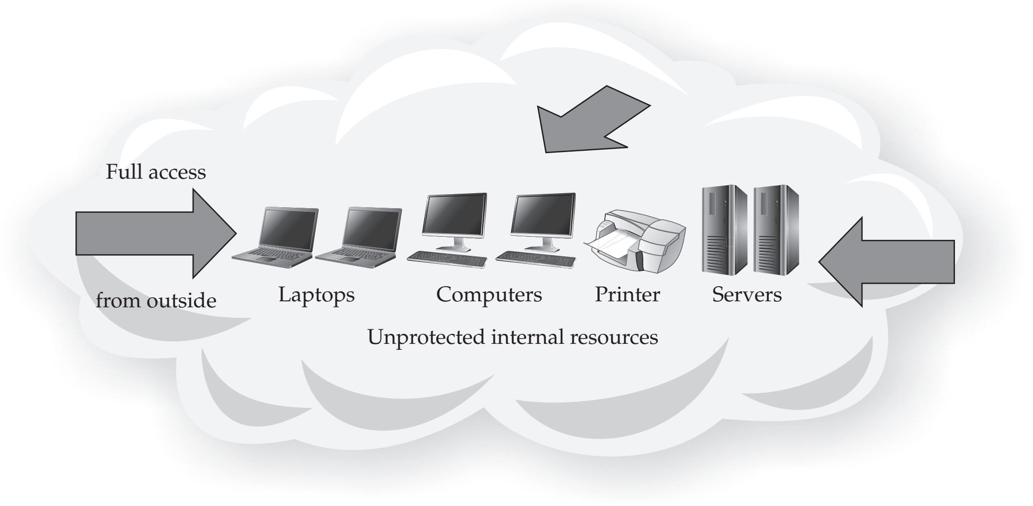


Figure 1-2 Original academic open-access model

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

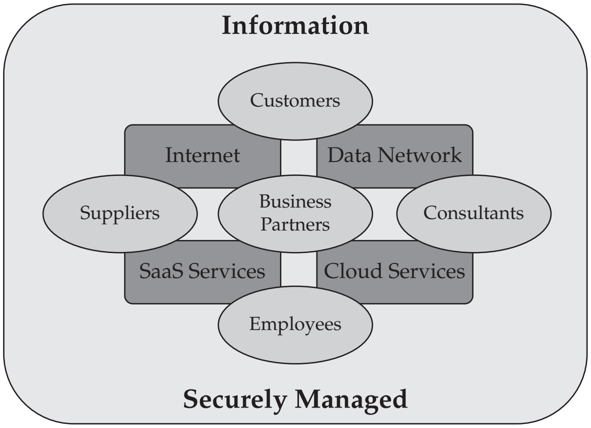


Figure 1-3 Modern information is shared among many consumers, via many channels.

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.