Managing Information Security

Editor

John R. Vacca

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Syngress is an imprint of Elsevier

SYNGRESS

Syngress is an imprint of Elsevier.
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
This book is printed on acid-free paper.

Material in this work originally appeared in *Computer and Information Security Handbook*, edited by John R. Vacca (Elsevier Inc., 2009).

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.
To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
Application submitted

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

ISBN: 978-1-59749-533-2

Printed in the United States of America
10 11 12 13 5 4 3 2 1

This book is dedicated to my wife, Bee

Contents

Foreword

Improving security of IT, network, and telecom assets has become absolutely essential. The growth of distributed computing, combined with the widespread use of off-the-shelf software products and Internet connectivity, has created security nightmares for many organizations. During the last decade, a great deal of attention has been focused on the cyber aspects of information systems security. In an effort to address an array of cyber security problems, many organizations have hired or trained new IT security personnel and dramatically increased spending on computer security products. It appears that the struggle to improve cyber security will continue well into the future.

However, the obsessive concern over information cyber security has far too often overshadowed the need for understanding the basics of information systems. The purpose of this book is to show organizations how to effectively and efficiently organize and maintain their defenses on all fronts, not just protect against the cyber threat. This includes risk analysis, mitigation design, deployment of defenses, and the maintenance of security efforts. The book starts with basic concepts and takes readers through the steps to help them to effectively secure computer networks and information systems.

Michael Erbschloe
Computer & Network Security Consultant

Acknowledgments

There are many people whose efforts on this book have contributed to its successful completion. I owe each a debt of gratitude and want to take this opportunity to offer my sincere thanks.

A very special thanks to my Senior Acquisitions Editor, Rick Adams, without whose continued interest and support, this book would not have been possible. Associate Editor, David Bevans, who provided staunch support and encouragement when it was most needed. Thanks to my Project Manager, Julie Ochs, and Copyeditor, Chuck Hutchinson, whose fine editorial work has been invaluable. Thanks also to my Marketing Manager, Andrea Dierna, whose efforts on this book have been greatly appreciated. Finally, thanks to all the other people at Syngress (an imprint of Morgan Kaufmann Publishers/Elsevier Science & Technology Books) whose many talents and skills are essential to a finished book.

Thanks to my wife, Bee Vacca, for her love, her help, and her understanding of my long work hours. Also, a very very special thanks to Michael Erbschloe for writing the foreword. Finally, I wish to thank all the following authors who contributed chapters that were necessary for the completion of this book: Albert Caballero, James T. Harmening, Joe Wright, Rahul Bhaskar, Bhushan Kapoor, Tewfiq El Maliki, Jean-Marc Seigneur, Christopher Day, Scott R. Ellis, Yong Guan, Linfeng Zhang, Errin W. Fulp, Jay Bavisi, and Almantas Kakareka.

About the Editor

John R. Vacca is an information technology consultant and best-selling author based in Pomeroy, Ohio. Since 1982, John has authored 65 books. Some of his most recent books include *Computer and Information Security Handbook* (Morgan Kaufman 2009); *Biometric Technologies and Verification Systems* (Elsevier 2007); *Practical Internet Security* (Springer 2006); *Optical Networking Best Practices Handbook* (Wiley-Interscience 2006); *Guide to Wireless Network Security* (Springer 2006); *Computer Forensics: Computer Crime Scene Investigation, 2nd Edition* (Charles River Media 2005); *Firewalls: Jumpstart for Network and Systems Administrators* (Elsevier 2004); *Public Key Infrastructure: Building Trusted Applications and Web Services (*Auerbach 2004); *Identity Theft* (Prentice Hall\PTR 2002); *The World's 20 Greatest Unsolved Problems* (Pearson Education 2004); and more than 600 articles in the areas of advanced storage, computer security, and aerospace technology. John was also a configuration management specialist, computer specialist, and the computer security official (CSO) for NASA's space station program (Freedom) and the International Space Station Program, from 1988 until his early retirement from NASA in 1995.

Contributors

Michael Erbschloe (Foreword), Teaches Information Security courses at Webster University in St. Louis, MO

Albert Caballero, CISSP, GSEC (Chapter 1), Security Operations Center Manager, Terremark Worldwide, Inc., Bay Harbor Islands, FL 33154

James T. Harmening and Joe Wright (Chapter 2), Computer Bits, Inc., Chicago, IL 60602

Rahul Bhaskar (Chapter 3), Department of Information Systems and Decision Sciences, California State University, Fullerton, CA 92834

Bhushan Kapoor (Chapter 3), Department of Information Systems and Decision Sciences, California State University, Fullerton, CA 92834

Tewfiq El Maliki (Chapter 4), Telecommunications Labs, University of Applied Sciences of Geneva, Geneva, Switzerland

Jean-Marc Seigneur (Chapter 4), Department of Social and Economic Sciences, University of Geneva, Switzerland

Christopher Day, CISSP, NSA:IEM (Chapter 5), Senior Vice President, Secure Information Systems, Terremark Worldwide, Inc., Miami, FL 33131

Scott R. Ellis, EnCE (Chapter 6), RGL—Forensic Accountants & Consultants, Chicago, IL 60602

Yong Guan (Chapter 7), Litton Assistant Professor, Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011

Linfeng Zhang (Chapter 7), Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011

Errin W. Fulp (Chapter 8), Department of Computer Science, Wake Forest University, Winston-Salem, NC, 27109

Jay Bavisi (Chapter 9), President, EC-Council, Albuquerque, NM 87109

Almantas Kakareka (Chapter 10), Terremark Worldwide Inc., Security Operations Center, Miami, FL 33132

Introduction

This *Managing Information Security* book provides a broad overview of information security program elements to assist practitioners and IT professionals in enhancing their skills and knowledge on how to establish and implement an information security program. The material in this book can be referenced for general information on a particular topic or can be used in the decision-making process for managing an information security program. The purpose of this book is to inform information security management practitioners and IT professionals about various aspects of information security that they will be expected to implement and oversee in their respective organizations. In addition, the book provides guidance for facilitating a more consistent approach to information security programs.

Furthermore, this comprehensive book serves as a professional reference to provide the most complete and concise view of how to manage computer security and privacy available. It offers in-depth coverage of computer security theory, technology, and practice as it relates to established technologies, as well as recent advancements. It explores practical solutions to a wide range of security issues. Individual chapters are authored by leading experts in the field and address the immediate and long-term challenges in the contributors' respective areas of expertise.

The book provides information that practitioners and IT professionals can use in building their information security program strategy. In addition, new security vendors are building Ethernet switches that offer full security on every single port at very affordable prices, driving prices down and making competition fiercer for all integrated security products.

The book is therefore useful to any manager who requires a broad overview of information security practices. In addition, in this book, you will also learn how to

1. Configure tools and utilities to minimize exposure and detect intrusions
2. Create, document, and test continuity arrangements for your organization
3. Perform a risk assessment and business impact assessment (BIA) to identify vulnerabilities
4. Select and deploy an alternate site for continuity of mission-critical activities

5. Identify appropriate strategies to recover the infrastructure and processes
6. Organize and manage recovery teams
7. Test and maintain an effective recovery plan in a rapidly changing technology environment
8. Detect and respond to vulnerabilities that put your organization at risk using scanners
9. Employ real-world exploits and evaluate their effect on your systems
10. Configure vulnerability scanners
11. Analyze the results of vulnerability scans
12. Assess vulnerability alerts and advisories
13. Establish a strategy for vulnerability management
14. Build a firewall to protect your network
15. Install and configure proxy-based and stateful-filtering firewalls
16. Provide access to HTTP and FTP services on the Internet
17. Implement publicly accessible servers without compromising security
18. Protect internal IP addresses with NAT and deploy a secure DNS architecture
19. Manage information security risks within your organization
20. Identify security threats to your data and IT infrastructure
21. Recognize appropriate technology to deploy against these threats
22. Adapt your organization's information security policy to operational requirements and assess compliance
23. Effectively communicate information security issues
24. Oversee your organization's ongoing information security

You will also learn to identify vulnerabilities and implement appropriate countermeasures to prevent and mitigate threats to your mission-critical processes. You will learn techniques for creating a business continuity plan (BCP) and the methodology for building an infrastructure that supports its effective implementation.

Knowledge of vulnerability assessment and hacking techniques allows you to detect vulnerabilities before your networks are attacked. In this book, you will learn to configure and use vulnerability scanners to detect weaknesses and prevent network exploitation.

You will also acquire the knowledge to assess the risk to your enterprise from an array of vulnerabilities and to minimize your exposure to costly threats.

The firewall has emerged as a primary tool to prevent unauthorized access to valuable data. In this book, you will gain experience installing and configuring a firewall. You will also learn how to allow access to key services while maintaining your organization's security.

Securing information is vital to the success of every organization and is the link to maximizing the benefits of information technology. This book will empower managers with an understanding of the threats and risks to information resources. You will also gain the knowledge of what needs to be done to protect information infrastructures, develop an action plan, and monitor threats. You will learn to identify best practices and deploy a security program throughout your organization.

Finally, throughout this book, you will gain practical skills through a series of interactive small-group workshops and evolving case studies. You will also learn how to design and develop a disaster recovery plan, which includes the following:

1. Assessing threats
2. Avoiding disasters
3. Identifying the impact on critical business functions
4. Recognizing alternatives for continuing business functions
5. Planning your continuity project
6. Organizing team structures for use in an emergency
7. Creating a recovery plan from the response to a disaster

In addition, this book is valuable for those involved in selecting, implementing or auditing secure solutions for access into the enterprise. And, it is also valuable for anyone responsible for ensuring the continuity of an organization's critical systems or processes. For example, you should have general familiarity with and knowledge equivalent to the following:

- Project management: skills for success
- Internet and intranet firewall deployment
- Web security implementation
- Management skills
- Influence skills
- Project risk management

- Intrusion detection and analysis
- Vulnerability assessment
- Disaster recovery planning

Organization of This Book

The book is composed of 10 contributed chapters by leading experts in their fields.

Contributor Albert Caballero (Chapter 1, "Information Security Essentials for IT Managers: Protecting Mission-Critical Systems") begins by discussing how security goes beyond technical controls and encompasses people, technology, policy, and operations in a way that few other business objectives do. Information security involves the protection of organizational assets from the disruption of business operations, modification of sensitive data, or disclosure of proprietary information. The protection of such data is usually described as maintaining the confidentiality, integrity, and availability (CIA) of the organization's assets, operations, and information.

The evolution of a risk-based paradigm, as opposed to a technical solution paradigm for security, has made it clear that a secure organization does not result from securing technical infrastructure alone.

Next, contributors Joe Wright and James T. Harmening (Chapter 2, "Security Management Systems") examine documentation requirements and the maintenance of an effective security system, as well as assessments. Today, when most companies and government agencies rely on computer networks to store and manage their organizations' data, it is essential that measures are put in place to secure those networks and keep them functioning optimally. Network administrators need to define their security management systems to cover all parts of their computer and network resources.

A security management system starts as a set of policies that dictate the way in which computer resources can be used. The policies are then implemented by the organization's technical departments and enforced. This can be easy for smaller organizations but can require a team for larger international organizations that have thousands of business processes. Either way, measures need to be put in place to prevent, respond to, and fix security issues that arise in an organization.

Contributors Rahul Bhasker and Bhushan Kapoor (Chapter 3, "Information Technology Security Management") discuss the processes that are supported with enabling organizational structure and technology to protect an organization's information technology operations and information technology assets against internal and external threats, intentional or otherwise. Information technology security management can be defined as processes that support

enabling organizational structure and technology to protect an organization's IT operations and assets against internal and external threats, intentional or otherwise. The principal purpose of IT security management is to ensure confidentiality, integrity, and availability of IT systems. Fundamentally, security management is a part of the risk management process and business continuity strategy in an organization.

These processes are developed to ensure confidentiality, integrity, and availability of IT systems. There are various aspects to the IT security in an organization that need to be considered. They include security policies and procedures, security organization structure, IT security processes, and rules and regulations.

Contributors Dr. Jean-Marc Seigneur and Tewfiq El Maliki (Chapter 4, "Identity Management") continue by presenting the evolution of identity management requirements. Recent technological advances in user identity management have highlighted the paradigm of federated identity management and user-centric identity management as improved alternatives. The first empowers the management of identity; the second allows users to actively manage their identity information and profiles. It also allows providers to easily deal with privacy aspects regarding user expectations. This problem has been tackled with some trends and emerging solutions, as described in this chapter.

First, Seigneur and El Maliki provide an overview of identity management from Identity 1.0 to 2.0, with emphasis on user-centric approaches. They survey how the requirements for user-centric identity management and their associated technologies have evolved, with emphasis on federated approaches and user-centricity. Second, they focus on related standards XRI and LID, issued from the Yadis project, as well as platforms, mainly ID-WSF, OpenID, InfoCard, Sxip, and Higgins. Finally, they treat identity management in the field of mobility and focus on the future of mobile identity management.

Seigneur and El Maliki then survey how the most advanced identity management technologies fulfill present-day requirements. Then they discusses how mobility can be achieved in the field of identity management in an ambient intelligent/ubiquitous computing world.

Identity has become a burden in the online world. When it is stolen, it engenders a massive fraud, principally in online services, which generates a lack of confidence in doing business with providers and frustration for users. Therefore, the whole of society would suffer from the demise of privacy, which is a real human need. Because people have hectic lives and cannot spend their time administering their digital identities, we need consistent identity management platforms and technologies enabling usability and scalability, among other things. In this chapter, Seigneur and El Maliki survey how the requirements have evolved for mobile user-centric identity management and its associated technologies.

The Internet is increasingly used, but the fact that the Internet has not been developed with an adequate identity layer is a major security risk. Password fatigue and online fraud are a growing problem and are damaging user confidence.

This chapter underlines the necessity of mobility and the importance of identity in future ambient intelligent environments. Mobile identity management will have to support a wide range of information technologies and devices with critical requirements such usability on the move, privacy, scalability, and energy-friendliness.

Next, contributor Christopher Day (Chapter 5, "Intrusion Prevention and Detection Systems") discusses the nature of computer system intrusions, those who commit these attacks, and the various technologies that can be utilized to detect and prevent them. With the increasing importance of information systems in today's complex and global economy, it has become mission and business critical to defend those information systems from attack and compromise by any number of adversaries. Intrusion prevention and detection systems are critical components in the defender's arsenal and take on a number of different forms. Formally, intrusion detection systems (IDSs) can be defined as "software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems." Intrusion prevention systems (IPSs) are systems that attempt to actually stop an active attack or security problem. Though there are many IDS and IPS products on the market today, often sold as self-contained, network-attached computer appliances, truly effective intrusion detection and prevention are achieved when viewed as a process coupled with layers of appropriate technologies and products.

It should now be clear that intrusion detection and prevention are not a single tool or product, but a series of layered technologies coupled with the appropriate methodologies and skill sets. Each of the technologies surveyed in this chapter has its own specific strengths and weaknesses, and a truly effective intrusion detection and prevention program must be designed to play to those strengths and minimize the weaknesses. Combining NIDS and NIPS with network session analysis and a comprehensive SIM, for example, helps offset the inherent weakness of each technology and provides the information security team greater flexibility to bring the right tools to bear for an ever-shifting threat environment.

Contributor Scott R. Ellis (Chapter 6, "Computer Forensics") provides an in-depth familiarization with computer forensics as a career, a job, and a science. This chapter helps you avoid mistakes and find your way through the many aspects of this diverse and rewarding field.

Again and again throughout this chapter, a single recurring theme emerges: Data that have been overwritten cannot, by any conventionally known means, be recovered. If it could be,

then Kroll Ontrack and every other giant in the forensics business would be shouting this service from the rooftops and charging a premium price for it.

Contributors Yong Guan and Linfeng Zhang (Chapter 7, "Network Forensics,") continue by helping you determine the path from a victimized network or system through any intermediate systems and communication pathways, back to the point of attack origination or the person who should be accountable. Today's cyber criminal investigator faces a formidable challenge: tracing network-based cyber criminals. The possibility of becoming a victim of cyber crime is the number-one fear of billions of people. This concern is well founded. The findings in the annual *CSI/FBI Computer Crime and Security Surveys* confirm that cyber crime is real and continues to be a significant threat. Traceback and attribution are performed during or after cyber violations and attacks, to identify where an attack originated, how it propagated, and what computer(s) and person(s) are responsible and should be held accountable. The goal of network forensics capabilities is to determine the path from a victimized network or system through any intermediate systems and communication pathways, back to the point of attack origination or the person who is accountable. In some cases, the computers launching an attack may themselves be compromised hosts or be controlled remotely. *Attribution* is the process of determining the identity of the source of a cyber attack. Types of attribution can include both digital identity (computer, user account, IP address, or enabling software) and physical identity (the actual person using the computer from which an attack originated).

Finally, in this chapter, Guan and Linfeng Zhang discuss the current network forensic techniques in cyber attack traceback. They focus on the current schemes in IP spoofing traceback and stepping-stone attack attribution. Furthermore, they introduce the traceback issues in Voice over IP, Botmaster, and online fraudsters.

Next, contributor Errin W. Fulp (Chapter 8, "Firewalls," provides an overview of firewalls: policies, designs, features, and configurations. Of course, technology is always changing, and network firewalls are no exception. However, the intent of this chapter is to describe aspects of network firewalls that tend to endure over time.

Providing a secure computing environment continues to be an important and challenging goal of any computer administrator. The difficulty is in part due to the increasing interconnectivity of computers via networks, which includes the Internet. Such interconnectivity brings great economies of scale in terms of resources, services, and knowledge, but it has also introduced new security risks. For example, interconnectivity gives illegitimate users much easier access to vital data and resources from almost anywhere in the world.

Network firewalls are a key component in providing a secure environment. These systems are responsible for controlling access between two networks, which is done by applying a

security policy to arriving packets. The policy describes which packets should be accepted and which should be dropped. The firewall inspects the packet header and/or the payload (data portion).

There are several different types of firewalls, each briefly described in this chapter. Firewalls can be categorized based on what they inspect (packet filter, stateful, or application), their implementation (hardware or software), or their location (host or network). Combinations of the categories are possible, and each type has specific advantages and disadvantages.

Improving the performance of the firewall can be achieved by minimizing the rules in the policy (primarily for software firewalls). Moving more popular rules near the beginning of the policy can also reduce the number of rule comparisons that are required. However, the order of certain rules must be maintained (any rules that can match the same packet).

Regardless of the firewall implementation, placement, or design, deployment requires constant vigilance. Developing the appropriate policy (set of rules) requires a detailed understanding of the network topology and the necessary services. If either of these items change (and they certainly will), the policy will require updating. Finally, it is important to remember that a firewall is not a complete security solution but is a key part of a security solution.

Contributor Jay Bavisi (Chapter 9, "Penetration Testing,") shows how penetration testing differs from an actual "hacker attack," some of the ways penetration tests are conducted, how they're controlled, and what organizations might look for when choosing a company to conduct a penetration test for them. Thus, penetration testing is the exploitation of vulnerabilities present in an organization's network. It helps determine which vulnerabilities are exploitable and the degree of information exposure or network control that the organization could expect an attacker to achieve after successfully exploiting a vulnerability. No penetration test is or ever can be "just like a hacker would do it," due to necessary limitations placed on penetration tests conducted by "white hats." Hackers don't have to follow the same rules as the "good guys," and they couldn't care less whether your systems crash during one of their "tests." Bavisi also writes about various types of vulnerabilities and how they might be discovered.

Vulnerabilities can be thought of in two broad categories: logical and physical. We normally think of logical vulnerabilities as those associated with the organization's computers, infrastructure devices, software, or applications. Physical vulnerabilities, on the other hand, are normally thought of as those having to do with either the actual physical security of an organization (such as a door that doesn't always lock properly), the sensitive information that "accidentally" ends up in the dumpster, or the vulnerability of the organization's employees to social engineering (a vendor asking to use a computer to send a "quick email" to the boss).

Logical vulnerabilities can be discovered using any number of manual or automated tools and even by browsing the Internet. For those of you who are familiar with Johnny Long's *Google Hacking* books, you might appreciate this statement: "*Passwords*, for the *love of God!!!* Google found *passwords!*" The discovery of logical vulnerabilities is usually called *security scanning, vulnerability scanning*, or just *scanning*. Unfortunately, there are a number of "security consultants" who run a scan, put a fancy report cover on the output of the tool, and pass off these scans as a penetration test.

Physical vulnerabilities can be discovered as part of a physical security inspection, a "midnight raid" on the organization's dumpsters, getting information from employees, or via unaccompanied access to a usually nonpublic area. Thus, vulnerabilities might also exist due to a lack of company policies or procedures or an employee's failure to follow the policy or procedure. Regardless of the cause of the vulnerability, it might have the potential to compromise the organization's security. So, of all the vulnerabilities that have been discovered, how do we know which ones pose the greatest danger to the organization's network? We test them! We test them to see which ones we can exploit and exactly what could happen if a "real" attacker exploited that vulnerability.

Because few organizations have enough money, time, or resources to eliminate every vulnerability discovered, they have to prioritize their efforts; this is one of the best reasons for an organization to conduct a penetration test. At the conclusion of the penetration test, they will know which vulnerabilities can be exploited and what can happen if they are exploited. They can then plan to correct the vulnerabilities based on the amount of critical information exposed or network control gained by exploiting the vulnerability. In other words, a penetration test helps organizations strike a balance between security and business functionality. Sounds like a perfect solution, right? If only it were so!

Finally, contributor Almantas Kakareka (Chapter 10, "What Is Vulnerability Assessment?") covers the fundamentals: defining vulnerability, exploit, threat, and risk; analyzing vulnerabilities and exploits; configuring scanners; and showing you how to generate reports, assess risks in a changing environment, and manage vulnerabilities. In computer security, the term *vulnerability* is applied to a weakness in a system that allows an attacker to violate the integrity of that system. Vulnerabilities may result from weak passwords, software bugs, a computer virus, or other malware (malicious software), a script code injection, or an SQL injection, just to name a few.

Vulnerabilities always existed, but when the Internet was in its early stage they were not as often used and exploited. The media did not report news of hackers who were getting put in jail for hacking into servers and stealing vital information.

Finally, vulnerability assessment may be performed on many objects, not only computer systems/networks. For example, a physical building can be assessed so it will be clear what

parts of the building have what kinds of flaws. If an attacker can bypass a security guard at the front door and get into the building via a back door, that is definitely a vulnerability. Actually, going through the back door and using that vulnerability is called an *exploit*. The physical security is one of the most important aspects to be taken into account. If the attackers have physical access to the server, the server is not yours anymore! Just stating "Your system or network is vulnerable" doesn't provide any useful information. Vulnerability assessment without a comprehensive report is pretty much useless. A vulnerability assessment report should include

- Identification of vulnerabilities
- Quantity of vulnerabilities

John R. Vacca
Editor-in-Chief
jvacca@frognet.net
http://www.johnvacca.com