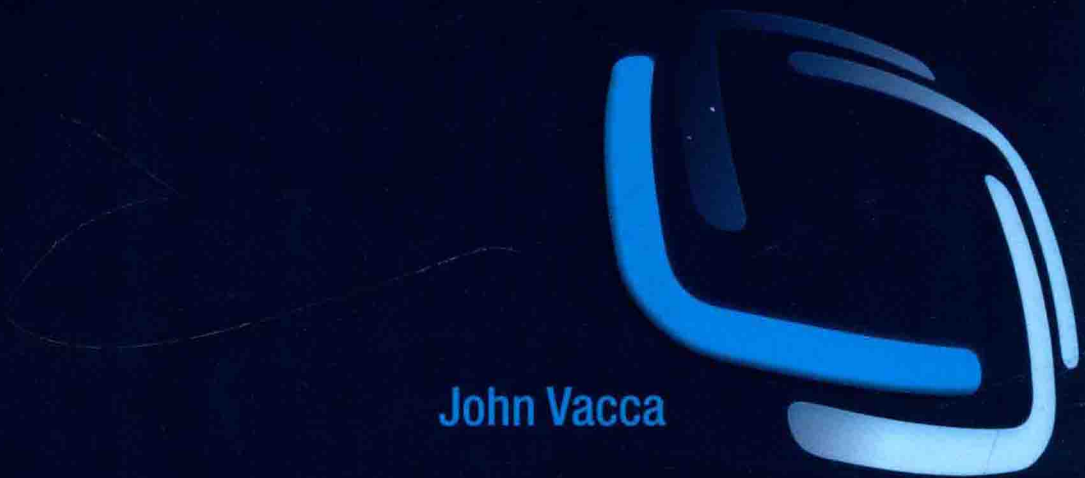
SYNGRESS

MANAGING INFORMATION SECURITY

Second Edition



John Vacca

MANAGING INFORMATION SECURITY

SECOND EDITION

Edited by

JOHN R. VACCA

ELSEVIER

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

Syngress is an imprint of Elsevier

SYNGRESS.

Publisher: Steven Elliot
Senior Developmental Editor: Nathaniel McFadden
Editorial Project Manager: Lindsay Lawrence
Project Manager: Mohanambal Natarajan
Designer: Matthew Limbert

Syngress is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA

Second edition 2014

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

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

For information on all **Syngress** publications,
visit our website at store.elsevier.com/Syngress

ISBN: 978-0-12-416688-2

Printed and bound in USA

14 15 16 17 18 10 9 8 7 6 5 4 3 2 1

MANAGING INFORMATION SECURITY

SECOND EDITION

This book is dedicated to my wife Bee.

Acknowledgements

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 publisher, Steve Elliot, without whose continued interest and support this book would not have been possible. Senior development editor Nate McFadden provided staunch support and encouragement when it was most needed. Thanks to my production project manager, Mohanambal Natarajan, whose fine work and attention to detail has been invaluable. Thanks also to my marketing manager, Todd Conly, whose efforts on this book have been greatly appreciated. Finally, thanks to all the other people at 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. Finally, I wish to thank all the following authors who contributed chapters that were necessary for the completion of this book: Sanjay Bavisi, Rahul Bhaskar, Albert Caballero, Christopher Day, Scott R. Ellis, Errin W. Fulp, Yong Guan, Cem Gurkok, James T. Harmening, Almantas Kakareka, Bhushan Kapoor, Jean-Marc Seigneur.

About the Editor

John Vacca is an information technology consultant, professional writer, editor, reviewer and internationally-known, best-selling author based in Pomeroy, Ohio. Since 1982, John has authored 73 books (some of his most recent books include):

- **Computer and Information Security Handbook, 2E** (*Publisher:* Morgan Kaufmann (an imprint of Elsevier Inc.) (May 31, 2013))
- **Identity Theft (Cybersafety)** (*Publisher:* Chelsea House Pub (April 1, 2012)
- **System Forensics, Investigation, And Response** (*Publisher:* Jones & Bartlett Learning (September 24, 2010)
- **Managing Information Security** (*Publisher:* Syngress (an imprint of Elsevier Inc.) (March 29, 2010))
- **Network and Systems Security** (*Publisher:* Syngress (an imprint of Elsevier Inc.) (March 29, 2010))
- **Computer and Information Security Handbook, 1E** (*Publisher:* Morgan Kaufmann (an imprint of Elsevier Inc.) (June 2, 2009))
- **Biometric Technologies and Verification Systems** (*Publisher:* Elsevier Science & Technology Books (March 16, 2007))
- **Practical Internet Security** (Hardcover): (*Publisher:* Springer (October 18, 2006))
- **Optical Networking Best Practices Handbook** (Hardcover): (*Publisher:* Wiley-Interscience (November 28, 2006))
- **Guide to Wireless Network Security** (*Publisher:* Springer (August 19, 2006)
- **Computer Forensics: Computer Crime Scene Investigation (With CD-ROM), 2nd Edition** (*Publisher:* Charles River Media (May 26, 2005)

and, more than 600 articles in the areas of advanced storage, computer security and aerospace technology (copies of articles and books are available upon request). 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 retirement from NASA in 1995. In addition, John is also an independent online book reviewer. Finally, John was one of the security consultants for the MGM movie titled: "AntiTrust," which was released on January 12, 2001. A detailed copy of my author bio can be viewed at URL: http://www.johnvacca.com. John can be reached at: john2164@windstream.net.

Contributors

Sanjay Bavisi (Chapter 7), President, EC-Council, Selangor, Malaysia

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

Albert Caballero, CISSP, GSEC (Chapter 1), Chief Technology Officer_CTO, Digital Era Group, LLC, Surfside, Fl. 33154

Christopher Day, CISSP, NSA: IEM (Chapter 5), Senior Vice President, Secure Information Systems, Terremark Worldwide, Inc., 2 South Biscayne Blvd., Suite 2900, Miami, FL 33131

Scott R. Ellis, EnCE, RCA (Chapter 9), Manager, Infrastructure Engineering Team,kCura, Chicago, IL 60604

Errin W. Fulp (Chapter 6), Professor, Department of Computer Science, Wake Forest University, Winston-Salem, North Carolina 27109

Yong Guan (Chapter 11), Litton Assistant Professor, Department of Electrical and Computer Engineering, Iowa State University, Ames, Iowa 50011

Cem Gurkok (Chapter 10), Threat Intelligence Development Manager, Terremark, Worldwide, Inc., Miami, Florida 33131

James T. Harmening (Chapter 2), President, Computer Bits, Inc., Chicago, Illinois 60602

Almantas Kakareka, CISSP, GSNA, GSEC, CEH (Chapter 8), CTO, Demyo, Inc., Sunny Isles Beach, Florida 33160

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

Jean-Marc Seigneur (Chapter 4), Advanced Systems Group, University of Geneva, Switzerland

Introduction

This Managing Information Security derivative 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, the reader should have general familiarity with- and have knowledge equivalent to the following:

- Project Management: Skills for Success
- Deploying Internet and Intranet Firewalls
- Implementing Web Security
- Management Skills
- Influence Skills
- Project Risk Management
- Detecting and Analyzing Intrusions
- Vulnerability Assessment
- Disaster Recovery Planning

ORGANIZATION OF THIS BOOK

The book is composed of 11 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 this data is usually described as maintaining the confidentiality, integrity, and availability (CIA) of the organization's assets, operations, and information.

As identified throughout this chapter, security goes beyond technical controls and encompasses people, technology, policy, and operations in a way that few other business objectives do. 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, contributor James T. Harmening (Chapter 2, "Security Management Systems") examines documentation requirements and maintaining 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 your organization.

Then, 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 intentionally or otherwise. Information technology security management can be defined as processes that supported enabling organizational structure and technology to protect an organization's IT operations and assets

against internal and external threats, intentional or otherwise. The principle purpose of IT security management is to ensure confidentiality, integrity, and availability (CIA) 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. These include security policies and procedures, security organization structure, IT security processes, and rules and regulations.

Contributor Dr. Jean-Marc Seigneur (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 provides an overview of identity management from Identity 1.0 to 2.0 and higher, with emphasis on user-centric approaches. He surveys how the requirements for user-centric identity management and their associated technologies have evolved, with emphasis on federated approaches and user-centricity. Second, he focuses on related standards XRI and LID, issued from the Yadis project, as well as platforms, mainly ID-WSF, OpenID, InfoCard, Sxip, and Higgins. Finally, he treats identity management in the field of mobility and focuses on the future of mobile identity management.

Seigneur then surveys how the different most advanced identity management technologies fulfill present day requirements. Then, he 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 surveys 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 has underlined 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. In this chapter, Day will discuss the nature of computer system intrusions, those who commit these attacks, and the various technologies that can be utilized to detect and prevent them.

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; as well as, provide the information security team greater flexibility to bring the right tools to bear for an ever-shifting threat environment.

Next, contributor Errin W. Fulp (Chapter 6, "Firewalls," provides an overview of firewall: 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 of 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 rules 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), that will require updating the policy. Finally, it is important to remember that a firewall is not a complete security solution, but is a key part of a security solution.

Then, contributor Sanjay Bavisi (Chapter 7, "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 could care less whether your systems crash during one of their "tests." Bavisi will talk more about this later. Right now, before he can talk any more about penetration testing, he needs to talk 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 the 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: *"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 that 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!

Next, contributor Almantas Kakareka (Chapter 8, "What Is Vulnerability Assessment?") covers the fundamentals: defining vulnerability, exploit, threat and risk; analyzes vulnerabilities and exploits; configures scanners and shows you how to generates reports; assesses risks in a changing environment; and, show you how to 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 kind of flaw. If the attacker can bypass the security guard at the front door and get into the building via a back door, it 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

Then, contributor Scott R. Ellis (Chapter 9, "Cyber Forensics") provides an in depth familiarization with computer forensics as a career, a job, and a science. It will help you *avoid mistakes* and find your way through the many aspects of this diverse and rewarding field.

This chapter is intended to provide in-depth information on computer forensics as a career, a job, and a science. It will help 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 will emerge: Data that has 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.

Next, contributor **Cem Gurkok** (Chapter 10, "**Cyber Forensics and Incident Response**"), discusses the steps and methods that are needed in order to respond to incidents and conduct cyber forensics investigations. He mainly focuses on Windows systems as target systems and utilizes open- source or freeware tools for discovery and analysis.

Listening to the news on a daily basis suggests that it is a matter of when, rather than if any given computing device will be compromised. Gurkok emphasis that what really matters is how fast one responds to the compromise to mitigate loss and to prevent future incidents. To be able to react with speed, proper plans and procedures need to be implemented beforehand, and tested on a regular basis for preparedness. Part of the response process is to investigate and understand the nature of the compromise.

Finally, in this chapter, Gurkok shows you why cyber forensics is an integral part of incident response that fills the investigative role. He explains that it is a form of forensic science whose aim is to identify, preserve, recover, analyze and present facts and opinions regarding evidence stored on or transferred between digital devices.

Finally, contributor Yong Guan (Chapter 11, "Network Forensics,") continues 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 discusses the current network forensic techniques in cyber attack traceback. He focuses on the current schemes in IP spoofing traceback and stepping-stone attack attribution. Furthermore, he introduces the traceback issues in Voice over IP, Botmaster, and online fraudsters.

John R. Vacca
Editor-in-Chief

Contents