SYNGRESS®

Techno Security's™ Guide to Managing Risks

FOR IT MANAGERS, AUDITORS, AND INVESTIGATORS

Your Own "Sit Down" with Internationally Known IT Security Experts

Jack Wiles Lead Author

Russ Rogers Technical Editor

thetrainingco. LLC

Raymond Todd Blackwood
Eric Cole
Phil Drake
Ron Green
Greg Kipper

Johnny Long
Dennis O'Brien
Kevin O'Shea
Amber Schroader

FOREWORD
BY DONALD WITHERS
CEO AND COFOUNDER
OF THETRAININGCO.

VISIT US AT

www.syngress.com

Syngress is committed to publishing high-quality books for IT Professionals and delivering those books in media and formats that fit the demands of our customers. We are also committed to extending the utility of the book you purchase via additional materials available from our Web site.

SOLUTIONS WEB SITE

To register your book, visit www.syngress.com/solutions. Once registered, you can access our solutions@syngress.com Web pages. There you may find an assortment of value-added features such as free e-books related to the topic of this book, URLs of related Web sites, FAQs from the book, corrections, and any updates from the author(s).

ULTIMATE CDs

Our Ultimate CD product line offers our readers budget-conscious compilations of some of our best-selling backlist titles in Adobe PDF form. These CDs are the perfect way to extend your reference library on key topics pertaining to your area of expertise, including Cisco Engineering, Microsoft Windows System Administration, CyberCrime Investigation, Open Source Security, and Firewall Configuration, to name a few.

DOWNLOADABLE E-BOOKS

For readers who can't wait for hard copy, we offer most of our titles in downloadable Adobe PDF form. These e-books are often available weeks before hard copies, and are priced affordably.

SYNGRESS OUTLET

Our outlet store at syngress.com features overstocked, out-of-print, or slightly hurt books at significant savings.

SITE LICENSING

Syngress has a well-established program for site licensing our e-books onto servers in corporations, educational institutions, and large organizations. Contact us at sales@syngress.com for more information.

CUSTOM PUBLISHING

Many organizations welcome the ability to combine parts of multiple Syngress books, as well as their own content, into a single volume for their own internal use. Contact us at sales@syngress.com for more information.

SYNGRESS®

This Page Intentionally Left Blank

SYNGRESS®

Techno Security's™ Guide to Managing Risks

FOR IT MANAGERS, AUDITORS, AND INVESTIGATORS

Jack Wiles
Russ Rogers Technical Editor

FOREWORD BY DONALD WITHERS
CEO AND COFOUNDER OF THETRAININGCO.

Elsevier, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively "Makers") of this book ("the Work") do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media®, Syngress®, "Career Advancement Through Skill Enhancement®," "Ask the Author UPDATE®," and "Hack Proofing®," are registered trademarks of Elsevier, Inc. "Syngress: The Definition of a Serious Security Library"™, "Mission Critical™," and "The Only Way to Stop a Hacker is to Think Like One™" are trademarks of Elsevier, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

KEY	SERIAL NUMBER
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	GHJ923HJMN
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Elsevier, Inc.
30 Corporate Drive
Burlington, MA 01803

Techno Security's Guide to Managing Risks for IT Managers, Auditors, and Investigators

Printed in the United States of America
1 2 3 4 5 6 7 8 9 0

ISBN-10: 1-59749-138-1
ISBN-13: 978-1-59749-138-9

Publisher: Andrew Williams
Acquisitions Editor: Gary Byrne
Technical Editor: Russ Rogers
Cover Designer: Michael Kavish

Page Layout and Art: Patricia Lupien
Copy Editors: Mike McGee, Adrienne Rebello
Indexer: Richard Carlson

For information on rights, translations, and bulk sales, contact Matt Pedersen, Commercial Sales Director, at m.pedersen@elsevier.com.

Acknowledgments

Syngress would like to acknowledge the following people for their kindness and support in making this book possible.

A million thanks to Jack Wiles and his partner, Don Withers, at TheTrainingCo. They have been a good partner to Syngress, and we are delighted to bring this first Techno book to market.

This Page Intentionally Left Blank

Lead Author

Jack Wiles is a Security Professional with over 30 years' experience in security-related fields, including computer security, disaster recovery, and physical security. He is a professional speaker and has trained federal agents, corporate attorneys, and internal auditors on a number of computer crime-related topics. He is a pioneer in presenting on a number of subjects that are now being labeled "Homeland Security" topics. Well over 10,000 people have attended one or more of his presentations since 1988. Jack is also a cofounder and President of TheTrainingCo. and is in frequent contact with members of many state and local law enforcement agencies as well as Special Agents with the U.S. Secret Service, FBI, U.S. Customs, Department of Justice, the Department of Defense, and numerous members of High-Tech Crime units. He was also appointed as the first president of the North Carolina InfraGard chapter, which is now one of the largest chapters in the country. He is also a founding member and "official" MC of the U.S. Secret Service South Carolina Electronic Crimes Task Force.

Jack is also a Vietnam veteran who served with the 101st Airborne Division in Vietnam in 1967-68. He recently retired from the U.S. Army Reserves as a lieutenant colonel and was assigned directly to the Pentagon for the final seven years of his career. In his spare time, he has been a senior contributing editor for several local, national, and international magazines.

I really appreciate reading the comments written by my new friend Johnny Long as he first thanked his creator in his Penetration Tester's book by Syngress. I'm in Johnny's camp in acknowledging that I can do nothing without the help of my Lord and Savior, Jesus Christ. I dedicate my small part of this book to Him, my wonderful wife, Valerie, and my son, Tyler. My partner Don Withers is like a brother to me in every way. For eight years, we have been fortunate to produce our Techno Security and our new Techno Forensics conferences, which have had attendees register from over 40 coun-

tries around the world. I wish that I had space to thank all of the other authors of this book. I know them all well, and I have known some of them for more than two decades. These are some of the most respected and talented security minds in the world, and I am honored to have my work in the same book as theirs. And last but certainly not least, I'd like to thank my good friend Russ Rogers for his technical editing help and Amy Pedersen from Syngress Publishing for being so patient as I learned the ropes of getting a book ready to be published.

Jack wrote Chapter 1, “Social Engineering: Risks, Threats, Vulnerabilities, and Countermeasures.

Technical Editor

Russ Rogers (CISSP, CISM, IAM, IEM, HonScD) is author of the popular *Hacking a Terror Network* (Syngress Publishing, ISBN: 1928994989); coauthor on multiple other books, including the best selling *Stealing the Network: How to Own a Continent* (Syngress, ISBN: 1931836051) and *Network Security Evaluation Using the NSA IEM* (Syngress, ISBN: 1597490350); and Editor in Chief of *The Security Journal*. Russ is Cofounder, Chief Executive Officer, and Chief Technology Officer of Security Horizon, a veteran-owned small business based in Colorado Springs, CO. Russ has been involved in information technology since 1980 and has spent the last 15 years working professionally as both an IT and INFOSEC consultant. Russ has worked with the United States Air Force (USAF), National Security Agency (NSA), and the Defense Information Systems Agency (DISA). He is a globally renowned security expert, speaker, and author who has presented at conferences around the world, including Amsterdam, Tokyo, Singapore, Sao Paulo, and cities all around the United States.

Russ has an Honorary Doctorate of Science in Information Technology from the University of Advancing Technology, a Master's Degree in Computer Systems Management from the University of Maryland, a Bachelor of Science in Computer Information Systems from the University of Maryland, and an Associate Degree in Applied Communications Technology from the Community College of the Air Force. He is a member of both ISSA and ISACA and cofounded the Global Security Syndicate (gssyndicate.org) and the Security Tribe (securitytribe.com). He acts in the role of professor of network security for the University of Advancing Technology (uat.edu).

Russ would like to thank his father for his lifetime of guidance, his kids (Kynda and Brenden) for their understanding, and Michele for her constant support. A great deal of thanks go to Andrew Williams from Syngress Publishing for the abundant opportunities and trust he gives me. Shouts go out to UAT, Security Tribe, the GSS, the Defcon Groups, and the DC Forums. I'd like to also thank my friends, Chris, Greg, Michele, Ping, Pyr0, and everyone in #dc-forums that I don't have room to list here.

Russ wrote Chapter 9, "The Basics of Penetration Testing."

Contributors

Dr. Eric Cole is currently chief scientist for Lockheed Martin Information Technology (LMIT), specializing in advanced technology research. Eric is a highly sought-after network security consultant and speaker. Eric has consulted for international banks and Fortune 500 companies. He also has advised venture capitalist firms on what start-ups should be funded. He has in-depth knowledge of network security and has come up with creative ways to secure his clients' assets. He is the author of several books, including *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft* (Syngress Publishing, ISBN: 1597490482); *Cyber Spying: Tracking Your Family's (Sometimes) Secret Online Lives* (Syngress Publishing, ISBN: 1-931836-41-8); *Hackers Beware: Defending Your Network from the Wiley Hacker*; *Hiding in Plain Sight*; and *The Network Security Bible.* Eric holds several patents and has written numerous magazine and journal articles. Eric worked for the CIA for more than seven years and has created several successful network security practices. Eric is an invited keynote speaker at government and international conferences and has appeared in interviews on CBS News, "60 Minutes," and CNN.

Eric wrote Chapter 11, "Insider Threat."

Phil Drake is Communications Manager for the *Charlotte Observer* in Charlotte, N. C. *The Observer* is a daily newspaper that serves readers throughout North and South Carolina. In addition to the newspaper, the *Charlotte Observer* produces specialty magazines, voice information, and Internet services.

Phil is responsible for all aspects of communications at *Observer* operations in both Carolinas, including telephone and data communications, wireless systems, conventional and trunked two-way radio, and satellite systems. He is also responsible for business continuity and disaster response planning and related budgeting. He is responsible for providing emergency communications facilities for reporters and photographers covering breaking news stories.

His background includes photojournalism, mainframe computer support, network management, telecommunications planning and management, and business continuity planning. Phil is a former chairman of the Contingency Planning Association of the Carolinas and currently serves as a Board Advisor of the organization. He is a Certified Business Continuity Professional with the Disaster Recovery Institute International.

Phil speaks to public and private sector groups and has been interviewed by and written for a number of national publications on a wide range of emergency communication issues and business/homeland defense planning. He leads business continuity training seminars for both the public and private sectors. He also has provided project management in business continuity and has advised major national clients in emergency planning, workforce protection, threat assessment, and incident response.

He enjoys backpacking and spending time in the outdoors. He also has taught outdoor living skills to youth group leaders. He was appointed by the North Carolina Secretary of the Department of Environment and Natural Resources as a voting member of the NC Geological Survey Advisory Committee.

Phil wrote Chapter 2, "Personal, Workforce, and Family Preparedness."

Ron Green (CISSP, ISSMP), a Senior Vice President within the Information Security Business Continuity division of Bank of America, currently serves as an Information Security Business Continuity Officer supporting the Bank's Network Computing Group. He formerly managed a bank team dedicated to handling cyber investigations, computer forensics, and electronic discovery. Prior to joining Bank of America, Ron was a Secret Service Agent and part of the agency's Electronic Crimes Agent Program (ECSAP). In addition to the investigative and protection work all agents perform, ECSAP agents perform cyber investigations and computer forensics for the agency. Ron started with the Secret Service in its Phoenix Field Office and then transferred to the agency's headquarters to become part of the Electronic Crimes Branch (ECB). While part of ECB he provided support to the ECSAP agents in the field. He also worked on national and international cyber crimes cases, initiatives, and laws. He was the project manager for Forward Edge and the Best Practice Guides for Seizing Electronic Evidence, version 2.0.

Ron graduated from the United States Military Academy at West Point, earning a bachelor's degree in Mechanical Engineering, and he earned a Graduate Certificate from George Washington University on Computer Security and Information Assurance. Ron currently serves as the Treasurer/Secretary for the Financial Services Information Sharing and Analysis Center (FS/ISAC) and as a Board Member for the Institute for Computer Forensic Professionals. Ron currently lives in North Carolina with his wife, Cheryl, and their four children.

Ron wrote Chapter 6, "Open Source Intelligence."

Greg Kipper (CISSP) is a Senior Security Engineer with Tenacity Solutions Incorporated. Tenacity is a woman-owned, small business that is headquartered in Reston, VA, that specializes in information security and information assurance. Greg has been involved in the field of security and information assurance over the past 13 years. Through his experiences in the security sector as a systems engineer, security analyst, and consultant, he moved into the emerging field of digital forensics. The last seven years of his career have been spent on working on forensic investigations studying the future of technologies and their forensic impact of that data to the process of evidence. Some of his notable works include the books *Investigator's Guide to Steganography*, *Wireless Crime and Forensic Investigation*, and the upcoming *Proactive Forensics* as well as a Congressional report outlining technical methods of reducing the risk of insider threats. Greg continues to actively contribute to the fields of security and digital forensics by giving lectures annually at DoD Cybercrime, TechnoSecurity, and TechnoForensics.

Greg wrote Chapter 10, "What Is Steganography?"

Johnny Long is a Christian by grace, a family guy by choice, a professional hacker by trade, a pirate by blood, a ninja in training, a security researcher, and an author. My home on the Web is http://johnny.ihackstuff.com.

I would like to thank my wife and kids for their continuing support of yet another hobby (writing/editing) that has spun out of control just as all the others have. I love you guys.

I have many people to thank, but first, I would like to thank God for taking the time to pierce my way-logical mind with the unfathomable gifts of sight by faith and eternal life through the sacrifice of Jesus Christ. I would also like to thank Jack Wiles and Russ for bringing me on board with this project; the real Vince, who remains an inspiration; Adam Laurie (aka Major Malfunction); StankDawg (aka David Blake); Barry Wels of Toool; Malcolm Mead; Pablos Holman; Tim "Thor" Mulllen; Stephen King; Ted Dekker; Neil Stephenson; and the wealth of amazingly talented Christian rock artists whose music is present for every word I write. I would also like to thank the C.H.A.O.S. team (nudge, nudge) for being an important part of those early days. Thanks also to the moderators and members of my Web site for your constant support.

I had a great time with this chapter, and I look forward to expanding it to a full-blown book. No-tech hackers rejoice!

Johnny wrote Chapter 8, "No-Tech Hacking."

Dennis F. O'Brien is a private consultant having held senior IT security positions within Bell Laboratories, AT&T, Citigroup, and other Fortune 100 financial sector enterprises. Dennis, a well-known technical expert having more than 30 years' experience in the exploitation of controls, comes to us as a canary to discuss the kinds of "evil things" that can be done using well-intended, generally available tools and services such as RFID. Examining the big picture and then presenting realistic scenarios, such as destabilizing public faith in the financial services industry or corrupting an asset database through input data tampering, are examples of his work.

He is known for his annual predictions of possible mal-events that may occur in the near future and what the results may be.

Dennis wrote Chapter 5, "RFID: An Introduction to Security Issues, and Concerns."

Kevin O'Shea is a Homeland Security and Intelligence Specialist for the Technical Analysis Group in the Justiceworks program at the University of New Hampshire. Kevin assisted in the development of the NH Strategic Plan to Combat Cyber Crime and currently supports the implementation of the Strategic Plan. Kevin has authored and coauthored a number of high-tech training programs for the law enforcement community and has assisted in the development of a new digital forensics paradigm in use in N.H.

Prior to working at the University of New Hampshire, he was a Research Associate for Project Management within the Technical Analysis Group in the Institute for Security Technology Studies at Dartmouth College. He was a member of the research team and substantive author of three critical national reports to document and present the most pressing impediments facing the law-enforcement community when investigating and responding to cyber attacks: *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment, Gap Analysis, and the Research and Development Agenda.*

Kevin wrote Chapter 3, "Seizure of Digital Information." This chapter was taken from Cyber Crime Investigations: Bridging the Gaps between, Security Professionals, Law Enforcement, and Prosecutors (Syngress Publishing, ISBN: 1597491330).

Amber Schroader has been involved in the field of computer forensics for the past 17 years. Amber has developed and taught numerous training courses for the computer forensic arena, specializing in the field of wireless forensics as well as mobile technologies. Amber is the CEO of Paraben Corporation and continues to act as the driving force behind some of the most innovative forensic technologies. As a pioneer in the field, Amber has been key in developing new technology to help investigators with the extraction of digital evidence from hard drives, e-mail, and handheld and mobile devices. Amber has extensive experience in dealing with a wide array of forensic investigators ranging from federal, state, local, and foreign government as well as corporate investigators. With an aggressive development schedule, Amber continues to bring new and exciting technology to the computer forensic community worldwide and is dedicated to supporting the investigator through new technologies and training services that are being provided through Paraben Corporation. Amber is involved in many different computer investigation organizations, including The Institute of Computer Forensic Professionals (ICFP) as the chairman of the board, HTCIA, CFTT, and FLETC.

Amber currently resides in Utah and Virginia with her two children, Azure and McCoy.

Amber wrote Chapter 4, "Handheld Forensics."

Raymond Todd Blackwood is an IT Manager for a private university in Tempe, AZ, with over 12 years of experience in managing technology projects, teams, and systems. He currently oversees the development of technology projects at the university and provides lectures and training on leadership principles for technology geeks. Raymond teaches several courses that focus on thinking and brain performance, as well as managing technology, systems, and change.

Raymond started his career in digital film making, which took him from his southern roots to the Southwest, where he did his undergraduate studies and received his BA in Multimedia and Digital Animation and Production. Producing independent digital films led him into technology management as he began to design and implement technology for animation and multimedia applications. A series of events catalyzed by a passion for learning and working in all kinds of technology projects led Raymond to become a Manager of Information Technology in 2000 for the university. Soon thereafter Raymond began his graduate work and received his Master's of Business Administration and Technology Management in 2006.

Raymond is the comoderator of the Phoenix Future Salon through the Accelerated Studies Foundation. He also serves on the board of directors for the Greater Arizona eLearning Association and the Arizona Telecommunications and Information Council, and he is the faculty sponsor for DC480, the university's hacking club.

Raymond wrote Chapter 7, "Wireless Awareness: Increasing the Sophistication of Wireless Users."

Foreword Contributor

Donald P. Withers is the CEO and cofounder of TheTrainingCo., which produces the Annual International Techno Security & Techno Forensic Conferences each year. Don has an extensive background in Information Security and was a member of the management team at Ernst & Young's Information Security Services practice for the mid-Atlantic region. He also served as the Director of Information Security for Bell Atlantic, where he championed the development of a corporate incident response team and implemented their war room facility used for managing investigations, vulnerability testing, and forensic analysis.

He also served as a voting member of the American National Standards Institute Committee T1 for nine years developing and representing Bell Atlantic's positions on computer and network security. He was the Sub-working Group Secretary and Technical Editor for the committee that was instrumental in developing several of the first telecommunications standards in North America relating to network security.

Don was the cofounder and two-term president of the Maryland Chapter of InfraGard and is a member of the Secret Service's Electronic Crimes Task Force. He was the cofounder and two-term President of the mid-Atlantic Chapter of the High Technology Crime Investigation Association, and he has served as secretary for its National Board of Directors. He is a member of the

American Society for Industrial Security, the Association of Former Intelligence Officers, and the Academy of Security Educators and Trainers, where he earned the academy's designation of Certified Security Trainer. Don is also a member of the Nine Lives Associates and has earned its designation of Personal Protection Specialist from the Executive Protection Institute. He has attended the Federal Law Enforcement Training Center in Glenco, GA, and has a Bachelor's degree in Criminal Justice from the University of Maryland.

This Page Intentionally Left Blank

Contents