

SYNGRESS®

**BEST
DAMN**

IT SECURITY MANAGEMENT

BOOK

PERIOD

Everything You Need to Know About Security Management

- Complete Coverage of Taking Inventory of Cores Assets, Identifying and Prioritizing Threats, Creating Penetrations Tests, and Analyzing Security Logs
- How to Manage Internal and Insider Threats
- Detailed Instructions on Contingency Planning and Disaster Recovery

Bryan Cunningham
Ted Dykstra
Ed Fuller
Chris Gatford
André Gold
Matthew Paul Hoagberg
Amanda Hubbard
Chuck Little

Steve Manzuik
Greg Miles
C. Forrest Morgan
Ken Pfeil
Russ Rogers
Travis Schack
Susan Snedaker

The Best Damn IT Security Management Book Period

Bryan Cunningham
Ted Dykstra
Ed Fuller
Chris Gatford
André Gold
Matthew Paul Hoagberg
Amanda Hubbard
Chuck Little

Steve Manzuik
Greg Miles
C. Forrest Morgan
Ken Pfeil
Russ Rogers
Travis Schack
Susan Snedaker

This page intentionally left blank

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	BAL923457U
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY

Syngress Publishing, Inc.

Elsevier, Inc.

30 Corporate Drive

Burlington, MA 01803

The Best Damn IT Security Management Book Period

Copyright © 2007 by Elsevier, Inc. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Printed in the United States of America

1 2 3 4 5 6 7 8 9 0

ISBN: 978-1-59749-227-0

Publisher: Amorette Pedersen

Cover Designer: Michael Kavish

Copy Editor: Adrienne Rebello

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

This page intentionally left blank



About the Authors

Bryan Cunningham (JD, Certified in NSA IAM, Top Secret security clearance) has extensive experience in information security, intelligence, and homeland security matters, both in senior U.S. Government posts and the private sector. Cunningham, now a corporate information and homeland security consultant and Principal at the Denver law firm of Morgan & Cunningham LLC, most recently served as Deputy Legal Adviser to National Security Advisor Condoleezza Rice. At the White House, Cunningham drafted key portions of the Homeland Security Act, and was deeply involved in the formation of the National Strategy to Secure Cyberspace, as well as numerous Presidential Directives and regulations relating to cybersecurity. He is a former senior CIA Officer, federal prosecutor, and founding co-chair of the ABA CyberSecurity Privacy Task Force, and, in January 2005, was awarded the National Intelligence Medal of Achievement for his work on information issues. Cunningham has been named to the National Academy of Science Committee on Biodefense Analysis and Countermeasures, and is a Senior Counselor at APCO Worldwide Consulting, as well as a member of the Markle Foundation Task Force on National Security in the Information Age. Cunningham counsels corporations on information security programs and other homeland security-related issues and, working with information security consultants, guides and supervises information security assessments and evaluations.

Ted Dykstra (CISSP, CISA, CCNP, MCSE, IAM/IEM) is a Security Consultant for Security Horizon, Inc., a Colorado-based professional security services and training provider. Ted is a key contributor in the technical security efforts and service offerings for Security Horizon, and an instructor for the National Security Agency (NSA) Information Assurance Methodology (IAM). Ted's background is in both commercial and government support efforts, focusing on secure architecture development and deployment, INFOSEC assessments and audits, as well as attack and

penetration testing. His areas of specialty are Cisco networking products, Check Point and Symantec Enterprise Security Products, Sun Solaris, Microsoft, and Linux systems. Ted is a regular contributor to *The Security Journal*, as well as a member of the Information System Security Association (ISSA) and Information Systems Audit and Control Association (ISACA).

Ed Fuller (CISSP, GIAC GSEC) is the Chief Operating Officer and Principle Security Consultant with Security Horizon, Inc., a Colorado-based professional security services and training provider. He currently is the lead instructor for the NSA IAM and IEM courses and leads assessments and evaluations as well leading the IA-CMM appraisals. His specialties include implementation of the NSA IAM and IEM into commercial environments and the IA-CMM. Ed's background includes positions as a senior consultant for Titan Systems, and JAWZ, Inc, and Averstar, Inc.

Ed is a retired United States Navy Chief Petty Officer and later participated on the development of System Security Engineering Capability Maturity Model (SSE-CMM). Ed has also been involved in the development of the Information Assurance Capability Maturity Model (IA-CMM). Ed is a frequent contributor to *The Security Journal* and co-author of *Security Assessment: Case Studies for Implementing the NSA IAM*. Ed holds a Bachelor of Science in Information Management from the University of Maryland. He lives in Colorado with his family Patience and Leila.

Chris Gatford works for Pure Hacking Ltd. in Sydney, Australia as a Senior Security Consultant performing penetration tests for organizations all around the world. Chris has reviewed countless IT environments and has directed and been responsible for numerous security assessments for a variety of corporations and government departments.

Chris is an instructor for the Pure Hacking OPST course and in his previous role at Ernst & Young he was the lead instructor for eXtreme Hacking course. In both these roles Chris has taught the art of professional hacking to hundreds of students from global organizations.

Chris is a frequent speaker at many security related conferences (most recently presenting at AusCERT 2006). He is a member of several security professional organizations and is a Certified Information Systems

Security Professional. More details and contact information is available from his homepage, www.penetrationtester.com and his current employer <http://www.purehacking.com>.

André Gold is currently the Director of Information Security at Continental Airlines, one of the world's largest and most successful commercial and freight transportation providers. André was appointed to this position by the company's former CIO, making him the first person to hold this post in the company's 50-year history. As the Director of Information Security, André has established a risk-based information security program based in part on increasing the security IQ of over 42,000 employees and protecting the over \$2.5 billion continental.com property.

As an identified security practitioner, André has been featured in SC, Information Security, and CSO Magazine. André also presents at or participates in industry-related events. In 2006 André was named an Information Security 7 award winner in the retail sector, for his security contributions in the start-up and air transportation markets.

Before assuming his current role, André served as Technical Director of Internet and Network Services. In this role, he built and was responsible for Continental's infrastructure and continental.com property; a property which accounts for close to 25% of the company's revenue.

In his spare time, André is pursuing his MBA at Colorado State and has a BBA in Computer Information Systems from the University of Houston-Downtown. André was also a commissioned officer in the Army, receiving his commission from Wentworth Military Academy.

In addition to his position at Continental, André serves on the Microsoft Chief Security Officer Council, the Skyteam Data Privacy and Security Subcommittee, Goldman Sachs' Security Council, as well as eEye Digital Security's and ConSentry Networks' Executive Advisory Councils.

Matthew Paul Hoagberg is an information technology and security professional with diverse experience in IT, personnel management, technology training, and business development support with Security Horizon, Inc., a Colorado-based professional security services and training provider. Matthew contributes to the security training, assessments, and evaluation that Security Horizon offers.

He currently serves as a Security Consultant, along with guidance from the Department of the Interior (DOI) and National Institute of Standards and Technology (NIST), to enhance the Bureau of Reclamation's (BOR) IT security management processes with a goal of improving the BOR's compliance with the Federal Information Security Management Act (FISMA) requirements. Review gap analysis performed by BOR identifying FISMA weaknesses. Work to establish a mechanism for identifying the minimum products necessary to ensure the target Departmental FISMA reporting grade.

Matthew holds a bachelor's degree from Northwester College and is a member of the Information Systems Security Association (ISSA), and co-author of *Security Assessment: Case Studies for Implementing the NSA IAM* (Syngress Publishing, ISBN 1-932266-96-8). Matthew currently resides in Monument, Colorado with his family.

Amanda Hubbard [JD] is a Trial Attorney assigned to the Computer Crime and Intellectual Property Section of the U.S. Department of Justice working on national security and computer intrusion issues. Prior to this assignment, Ms. Hubbard worked as an attorney for the Intelligence Community and the military on issues of computer forensics, electronic evidence, encryption, network security, vulnerability assessments, criminal law, and information sharing. She also serves as an Adjunct Professor for the Columbus School of Law at Catholic University where she co-teaches the seminar "National Security Law in Cyberspace," and a guest lecturer at: the Naval Postgraduate School Information Warfare Workshops; the Air Force Judge Advocate General School Information Warfare Course; the U.S. Secret Service; Federal Bureau of Investigation, and the United States Department of Justice National Advocacy Center. Ms. Hubbard regularly speaks to international audiences on cybersecurity and cybercrime. Prior works include portions of the 2002 ABA Committee on Cyberspace publication, "Patriot 'Games' No Longer: The Business Community's Role in Cybersecurity", and submissions to the International Telecommunications Union and the United Nations. She has been named as a 2005-06 Fulbright Scholar to the Norwegian Research Center for Computers and Law at the University of Oslo to research and write on transnational cybercrime issues.

Chuck Little (CCSA, NSA IAM, NSA IEM) is a Senior Security Consultant for Security Horizon Inc. Security Horizon is a small veteran-owned business focused on INFOSEC, headquartered in Colorado Springs, Colorado. His specialties include Checkpoint FW-1, NetScreen Firewall/IDS/IPS, Perl coding, Linux, Solaris, Mac OS X, compliance auditing, network security architecture and design, and snowboarding.

Chuck is a veteran of the US Army, having spent over seven years on active duty. Chuck holds a bachelor's degree in Applied Computer Science from Illinois State University, with a minor in Philosophy. He is an occasional contributor to the MIND Project, a research venture into cognitive sciences, at Illinois State University. Chuck currently resides in Denver, Colorado; with winter weekends spent at Loveland Ski Area.

Steve Manzuik currently holds the position of Senior Manager, Security Research at Juniper Networks. He has more than 14 years of experience in the information technology and security industry, with a particular emphasis on operating systems and network devices. Prior to joining Juniper Networks, Steve was the Research Manager at eEye Digital Security and in 2001, he founded and was the technical lead for Entrench Technologies. Prior to Entrench, Steve was a manager in Ernst & Young's Security & Technology Solutions practice, where he was the solution line leader for the Canadian Penetration Testing Practice. Before joining Ernst & Young, he was a security analyst for a world wide group of white hat hackers and security researchers on BindView RAZOR Team.

Steve has co-authored *Hack Proofing Your Network, Second Edition*. In addition, he has spoken at Defcon, Black Hat, Pacsec, and CERT conferences around the world and has been quoted in industry publications including CNET, CNN, InfoSecurity Magazine, Linux Security Magazine, Windows IT Pro and Windows Magazine.

Greg Miles, (Ph.D., CISSP#24431, CISM#0300338, IAM, IEM) co-author of *Security Assessment: Case Studies for implementing the NSA IAM* (Syngress Publishing, ISBN 1-932266-96-8) is a Co-Founder, President, and Chief Financial Officer of Security Horizon, Inc. Security Horizon is a global veteran-owned small business headquartered in Colorado Springs, Colorado. Security Horizon provides global information security professional service,

training, and publishes *The Security Journal*. Greg is an U.S. Air Force Veteran and has been supporting the technology and security community for the last 18 years. Greg's background includes work with NSA, NASA, and DISA. Greg has supported efforts covering security assessments, evaluations, policy, penetration testing, incident response, and computer forensics.

Greg holds a Ph.D. in Engineering Management from Kennedy Western University, a master's degree in Management Administration from Central Michigan University, and a bachelor's degree in Electrical Engineering from the University of Cincinnati. Greg is a member of the Information System Security Association (ISSA) and the Information System Audit and Control Association (ISACA). He is also a co-founder of the Global Security Syndicate and teaches network security for the University of Advancing Technology.

C. Forrest Morgan (JD (1987), Trained in NSA IAM) has extensive experience in corporate practice and structure including contracting, corporate formation, and operations. Mr. Morgan advises information security consultants on drafting and negotiating contracts with their customers to best protect them against potential legal liability. Mr. Morgan's practice also has emphasized commercial contract drafting and reorganization, and corporate litigation, providing in-depth understanding of the business and legal environment. He has represented both national corporations and regional firms in state and federal courts and administrative agencies in matters of litigation, creditors' rights, bankruptcy, administrative law and employment issues. Mr. Morgan served as the Regional Editor of the Colorado Bankruptcy Court Reporter from 1989 to 1992, and he co-authored the Bankruptcy section of the Annual Survey of Colorado from 1991 to 1997. As a Principal of the Denver law firm of Morgan & Cunningham, LLC, Mr. Morgan's practice also includes corporate information and security consulting. He counsels corporations on information security programs, including development of corporate policies and procedures to minimize business risks and litigation exposure.

Ken Pfeil's IT and security experience spans over two decades with companies such as Microsoft, Dell, Avaya, Identix, BarnesandNoble.com, Merrill Lynch, Capital IQ, and Miradient Global Network. While at Microsoft Ken coauthored Microsoft's "Best Practices for Enterprise Security"

white paper series. Ken has contributed to many books including *Hack Proofing Your Network, Second Edition* (Syngress, 1928994709) and *Stealing the Network: How to Own the Box* (Syngress, 1931836876).

Russ Rogers (CISSP, CISM, IAM, IEM, HonScD), author of the popular *Hacking a Terror Network* (Syngress Publishing, ISBN 1-928994-98-9), co-author on multiple other books including the best selling *Stealing the Network: How to Own a Continent* (Syngress Publishing, ISBN 1-931836-05-1), and Editor in Chief of *The Security Journal*; is Co-Founder, Chief Executive Officer, and Chief Technology Officer of Security Horizon; a veteran-owned small business based in Colorado Springs, Colorado. 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). Mr. Rogers 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.

Mr. Rogers has an Honorary Doctorate of Science in Information Technology from the University of Advancing Technology, a Masters 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 Co-Founded the Global Security Syndicate (gssyndicate.org), the Security Tribe (securitytribe.com), and acts in the role of Professor of Network Security for the University of Advancing Technology (uat.edu).

Travis Schack (CISSP) is the founder and CEO of Vitalisec Inc., a Denver-based information security research and services company. Prior to founding Vitalisec, Travis worked in the network communications and financial industries, where he has performed numerous security application reviews as well as network attack and penetration tests against Unix, Linux, Windows, network, and communication systems. He has extensive knowledge in attack methodologies, intrusion detection, wireless networking, VoIP, security tools,

physical security, fraud detection and investigation, incident response, and computer security standards. He maintains his own test laboratory for researching the latest system vulnerabilities, attack methods/trends, and how to defend against them.

Travis has been published in multiple publications and has been a featured speaker at numerous security events around the world. He is an adjunct instructor for Denver University, teaching a technical hands-on Security Testing course for DU's Master program in Information Security. In his spare time, he organizes DC303, contributes to the Open Source Vulnerability Database (OSVDB) and Voice over IP Security Alliance (VOIPSA), and is a co-founder of the Global Security Syndicate (GSS).

Travis currently resides in Arvada, Colorado with his wife Kendra and 5 children, Kelsea, Austin, Gavin, Olivia, and Vivienne.

Susan Snedaker, Principal Consultant and founder of Virtual Team Consulting, LLC has over 20 years experience working in IT in both technical and executive positions including with Microsoft, Honeywell, and Logical Solutions. Her experience in executive roles at both Keane and Aptia Software provided extensive strategic and operational experience in managing hardware, software and other IT projects involving both small and large teams. As a consultant, she and her team work with companies of all sizes to improve operations, which often entails auditing IT functions and building stronger project management skills, both in the IT department and company-wide. She has developed customized project management training for a number of clients and has taught project management in a variety of settings. Susan holds a Masters degree in Business Administration (MBA) and a Bachelors degree in Management. She is a Microsoft Certified Systems Engineer (MCSE), a Microsoft Certified Trainer (MCT), and has a certificate in Advanced Project Management from Stanford University. She recently completed an Executive program in International Management at Thunderbird University's Garvin School of International Management.

Contents

Part 1 From Vulnerability to Patch	1
Chapter 1 Windows of Vulnerability	3
Introduction	4
What Are Vulnerabilities?	4
Understanding the Risks Posed by Vulnerabilities.	9
Summary.	13
Chapter 2 Vulnerability Assessment 101	15
Introduction	16
What Is a Vulnerability Assessment?	16
Step 1: Information Gathering/Discovery	16
Step 2: Enumeration	19
Step 3: Detection	19
Seeking Out Vulnerabilities	21
Detecting Vulnerabilities via Security Technologies	21
Deciphering VA Data Gathered by Security Technologies.	22
Accessing Vulnerabilities via Remediation (Patch) Technologies	26
Extracting VA Data from Remediation Repositories.	26
Leveraging Configuration Tools to Assess Vulnerabilities	29
The Importance of Seeking Out Vulnerabilities	30
Looking Closer at the Numbers	31
Summary.	36
Chapter 3 Vulnerability Assessment Tools	37
Introduction	38
Features of a Good Vulnerability Assessment Tool	38
Using a Vulnerability Assessment Tool	40
Step 1: Identify the Hosts on Your Network.	42
Step 2: Classify the Hosts into Asset Groups	45
Step 3: Create an Audit Policy.	46
Step 4: Launch the Scan	48
Step 5: Analyze the Reports	50
Step 6: Remediate Where Necessary	51
Summary.	52

Chapter 4 Vulnerability Assessment: Step One.	53
Introduction	54
Know Your Network	54
Classifying Your Assets	60
I Thought This Was a Vulnerability Assessment Chapter	63
Summary	66
Chapter 5 Vulnerability Assessment: Step Two.	67
Introduction	68
An Effective Scanning Program.	68
Scanning Your Network	69
When to Scan	75
Summary	79
Chapter 6 Going Further	81
Introduction	82
Types of Penetration Tests	82
Scenario: An Internal Network Attack.	84
Client Network	84
Step 1: Information Gathering.	86
Operating System Detection.	87
Discovering Open Ports and Enumerating.	88
Step 2: Determine Vulnerabilities	91
Setting Up the VA	92
Interpreting the VA Results	94
Penetration Testing.	99
Step 3: Attack and Penetrate	100
Uploading Our Data	100
Attack and Penetrate	103
Searching the Web Server for Information.	108
Discovering Web Services.	109
Vulnerability Assessment versus a Penetration Test	114
Tips for Deciding between Conducting a VA or a Penetration Test	114
Internal versus External	115
Summary	118
Chapter 7 Vulnerability Management	119
Introduction	120
The Vulnerability Management Plan	120
The Six Stages of Vulnerability Management.	121

Stage One: Identify	122
Stage Two: Assess.	123
Stage Three: Remediate	124
Stage Four: Report.	124
Stage Five: Improve.	125
Stage Six: Monitor	126
Governance (What the Auditors Want to Know)	127
Measuring the Performance of a Vulnerability Management Program.	128
Common Problems with Vulnerability Management	132
Summary.	134
Chapter 8 Vulnerability Management Tools	135
Introduction	136
The Perfect Tool in a Perfect World.	136
Evaluating Vulnerability Management Tools	137
Commercial Vulnerability Management Tools.	139
eEye Digital Security	139
Symantec (BindView).	139
Attachmate (NetIQ)	140
StillSecure	140
McAfee	140
Open Source and Free Vulnerability Management Tools	141
Asset Management, Workflow, and Knowledgebase	141
Host Discovery.	141
Vulnerability Scanning and Configuration Scanning.	141
Configuration and Patch Scanning	142
Vulnerability Notification	142
Security Information Management	142
Managed Vulnerability Services	143
Summary.	145
Chapter 9 Vulnerability and Configuration Management	147
Introduction	148
Patch Management.	148
System Inventories	151
System Classification.	152
System Baselines.	153
Creating a Baseline	154
Baseline Example.	155
The Common Vulnerability Scoring System	156

Building a Patch Test Lab	157
Establish a Patch Test Lab with “Sacrificial Systems”	157
Virtualization	157
Environmental Simulation	159
Patch Distribution and Deployment	161
Logging and Reporting	162
Configuration Management	162
Change Control	162
Summary	166
Chapter 10 Regulatory Compliance	167
Introduction	168
Regulating Assessments and Pen Tests	168
The Payment Card Industry (PCI) Standard	168
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)	170
The Sarbanes-Oxley Act of 2002 (SOX)	172
Compliance Recap	173
Drafting an Information Security Program	175
Summary	180
Chapter 11 Tying It All Together	181
Introduction	182
A Vulnerability Management Methodology	182
Step One: Know Your Assets	182
What You Need to Do	182
Why You Need to Do It	183
How to Do It	183
What Tools Exist to Help You Do It	185
Step Two: Categorize Your Assets	186
What You Need to Do	186
Why You Need to Do It	187
How to Do It	187
What Tools Exist to Help You Do It	188
Step Three: Create a Baseline Scan of Assets	188
What You Need to Do	188
Why You Need to Do It	189
How to Do It	189
What Tools Exist to Help You Do It	190
Step Four: Perform a Penetration Test on Certain Assets	190
What You Need to Do	190

Why You Need to Do It	191
How to Do It	191
What Tools Exist to Help You Do It	192
Step Five: Remediate Vulnerabilities and Risk	192
What You Need to Do	192
Why You Need to Do It	193
How to Do It	193
What Tools Exist to Help You Do It	194
Step Six: Create a Vulnerability Assessment Schedule	194
What You Need to Do	194
Why You Need to Do It	194
How to Do It	194
Step Seven: Create a Patch and Change Management Process	197
What You Need to Do	197
Why You Need to Do It	197
How to Do It	197
What Tools Exist to Help You Do It	198
Step Eight: Monitor for New Risks to Assets	198
What You Need to Do	198
Why You Need to Do It	198
How to Do It	198
What Tools Exist to Help You Do It	199
Part 2 Network Security Evaluation	201
Chapter 12 Introducing the INFOSEC Evaluation	203
Methodology	203
Introduction	204
What Is the IEM?	204
Tying the Methodologies Together	205
What the IEM Is Not	209
The IEM Is <i>Not</i> an Audit or Inspection	211
The IEM Is Not a Risk Assessment	212
Standards and Regulations	212
Lack of Expertise	213
Certification Does Not Give You Expertise	214
Summary	215
Chapter 13 Before the Evaluation Starts	217
Introduction	218
The Evaluation Request	218

Why Are Evaluations Requested?	218
Compliance With Laws and Regulations	218
The Sarbanes-Oxley Act	218
Federal Information Security Management Act	218
Health Insurance Portability and Accountability Act of 1996	219
The Gramm-Leach-Bliley Act	219
The Family Educational Rights and Privacy Act	219
The DoD Information Technology Security Certification and Accreditation Process	219
The National Information Assurance Certification and Accreditation Process	219
Defense Information Assurance Certification and Accreditation Process	220
ISO 17799	220
The North American Electric Reliability Council	220
Response to Suspicious Activities	221
Recent Successful Penetration	221
Suspected Possible Penetration	221
Unsuccessful Penetration Attempt	221
“I Don’t Know If Our Organization Has Been Penetrated”	222
Third-Party Independent Reviews of Security Posture	222
Customer-Required Reviews	222
Insurance-Required Reviews	222
SLA-Required Reviews	223
It’s The Right Thing To Do	223
How Are Evaluations Requested?	223
Validating the Evaluation Request	224
Sources of Information for Validation	225
Validating with the Customer	225
The Engagement Scoping Questionnaire	225
Customer Discussions and Information Confirmation	226
Publicly Available Information	226
Understanding the Level of Effort	226
The Formal Engagement Agreement	227
Nondisclosure Agreements	227
Engagement Agreement Composition	227
Minimum Engagement Agreement Contents	228
Understanding the Pricing Options	229

Government Contracting	230
Commercial Contracting	230
Fixed Price vs. Hourly Rate	230
Additional Engagement Agreement Contents	231
Dealing with Contract Pitfalls	233
“Scope Creep” and Timelines	233
Uneducated Salespeople	234
Evaluations 101	234
Bad Assumptions	235
Assumption Topic Areas	235
Poorly Written Contracts	235
Poor Scope Definition	235
Underbid or Overbid: The Art of Poor	
Cost Estimating	236
Customer and Evaluation Team Approval	237
The Customer Approval Process	237
The Evaluation Team Approval Process	237
Summary	238

Chapter 14 Setting Expectations 239

Introduction	240
Objectives of the Pre-Evaluation Phase	240
Understanding Concerns and Constraints	242
What Are the Requirements?	242
Other Significant Regulations	243
Budgetary Concerns	244
Cyber-Insurance	245
System Accreditation	246
FISMA	246
DoD Information Technology Security Certification and	
Accreditation Process	247
National Information Assurance Certification and	
Accreditation Process	247
Defense Information Assurance Certification and	
Accreditation Process	247
Response to Suspected Threats or Intrusions	247
Obtaining Management Buy-In	249
Obtaining Technical Staff Buy-In	251
Establishing Points of Contact	252
Summary	254

Chapter 15 Scoping the Evaluation	257
Introduction	258
Focusing the Evaluation	258
The Power of Expectations	258
What Does the Customer Expect for Delivery?	259
Adjusting Customer Expectations	259
When Scoping Fails	260
“Scope Creep” and Time Lines	260
Restricting Scope Slippage in the Contract	260
Contracting Differences	261
Uneducated Salespeople	261
Evaluations 101	261
Bad Assumptions	262
Assumption Topic Areas	262
Poorly Written Contracts	263
Poor Scope Definition	263
Underbid or Overbid: The Art of Poor Cost Estimating	263
Identifying the Rules of Engagement	264
Customer Concerns	264
Stating the Evaluation Purpose	264
Customer Constraints	264
Impact Resistance and Acceptable Levels of Invasiveness	265
Identifying Scanning Times	265
Off-Limit Nodes	265
Evaluation Tool Limitations	266
Notification Procedures	266
Evaluation Addressing	266
Reporting Level of Detail	267
Clear and Concise Writing	267
Establishing the Evaluation Boundaries	267
Physical Boundaries	268
Logical Boundaries	268
Critical Path and Critical Components	269
Finding the Sources of Scoping Information	270
Customer	270
The Scoping Questionnaire	270
Information Gained from the Questionnaire	271
Value of the Questionnaire	273
Example Responses on a Scoping Questionnaire	273
Evaluation Requestor	276

Customer Senior Leadership	276
Administrative Customer Contact	276
Technical Customer Contacts	277
Evaluation Team	277
Evaluation Team Lead	277
Evaluation Team Members	277
Validating Scoping Information	277
Staffing Your Project	277
Job Requirements	278
Networking and Operating Systems	278
Hardware Knowledge	278
Picking the Right People	279
Matching Consultants to Customers	279
Personality Issues	279
Summary	280

Chapter 16 Legal Principles for Information

Security Evaluations	283
Introduction	284
Uncle Sam Wants You: How Your Company's Information	
Security Can Affect U.S. National Security	284
Legal Standards Relevant to Information Security	289
Selected Federal Laws	289
Gramm-Leach-Bliley Act	289
Health Insurance Portability and Accountability Act	290
Sarbanes-Oxley	292
Federal Information Security and Management Act	292
FERPA and the TEACH Act	292
Electronic Communications Privacy Act and Computer	
Fraud and Abuse Act	293
State Laws	293
Unauthorized Access	293
Deceptive Trade Practices	294
Enforcement Actions	294
Three Fatal Fallacies	295
The "Single Law" Fallacy	295
The Private Entity Fallacy	295
The "Pen Test Only" Fallacy	296
Do It Right or Bet the Company: Tools to Mitigate Legal Liability	297
We Did our Best; What is the Problem?	297

The Basis for Liability	298
Negligence and the “Standard of Care”.	298
What Can Be Done?	299
Understand your Legal Environment	299
Comprehensive and Ongoing Security Assessments, Evaluations, and Implementation	299
Use Contracts to Define Rights and Protect Information	299
Use Qualified Third-party Professionals.	300
Making Sure Your Standards-of-care Assessments Keep Up with Evolving Law	301
Plan for the Worst	301
Insurance.	302
What to Cover in IEM Contracts	302
What, Who, When, Where, How, and How Much.	303
What.	303
Description of the Security Evaluation and Business Model.	303
Definitions Used in the Contract	304
Description of the Project	304
Assumptions, Representations, and Warranties	304
Boundaries and Limitations	305
Identification of Deliverables	306
Who	306
Statement of Parties to the Contractual Agreement	306
Authority of Signatories to the Contractual Agreement	306
Roles and Responsibilities of Each Party to the Contractual Agreement.	307
Non-disclosure and Secrecy Agreements.	307
Assessment Personnel.	308
Crisis Management and Public Communications.	308
Indemnification, Hold Harmless, and Duty to Defend	308
Ownership and Control of Information	308
Intellectual Property Concerns.	309
Licenses	309
When	309
Actions or Events that Affect Schedule	309
Where.	310
How	310
How Much	311

Fees and Cost	311
Billing Methodology	311
Payment Expectations and Schedule	311
Rights and Procedures to Collect Payment	311
Insurance for Potential Damage During Evaluation	312
Murphy's Law (When Something Goes Wrong)	312
Governing Law	312
Acts of God, Terror Attacks, and other Unforeseeable Even	312
When Agreement is Breached and Remedies	312
Liquidated Damages	312
Limitation on Liability.	313
Survival of Obligations	313
Waiver and Severability	313
Amendments to the Contract.	313
Where the Rubber Meets the Road: The LOA as	
Liability Protection	314
Beyond You and Your Customer	315
Software License Agreements	315
Your Customer's Customer	315
The First Thing We Do...? Why You <i>Want</i> Your Lawyers	
Involved From Start to Finish	316
Attorney-client Privilege.	317
Advice of Counsel Defense.	318
Establishment and Enforcement of Rigorous Assessment,	
Interview, and Report-writing Standards	319
Creating a Good Record for Future Litigation.	319
Maximizing Ability to Defend Litigation	320
Dealing with Regulators, Law Enforcement, Intelligence,	
and Homeland Security Officials	320
The Ethics of Information Security Evaluation	322
Chapter 17 Building the Technical Evaluation Plan.	323
Introduction	324
Purpose of the Technical Evaluation Plan	324
The IEM TEP as an Agreement	325
The TEP as Road Map.	326
Building the Technical Evaluation Plan	327
Source of the Technical Evaluation Plan Information	327
TEP Section I: Points of Contact.	328
Evaluation Team Contacts.	328
Customer Contacts	328

TEP Section II: Methodology Overview	329
Purpose of the IEM	329
Description of the IEM	329
Evaluation Tools to Be Used	329
TEP Section III: Criticality Information	330
Organizational Criticality Matrices	330
System Criticality Information	331
TEP Section IV: Detailed Network Information	332
TEP Section V: Customer Concerns	333
TEP Section VI: Customer Constraints	334
TEP Section VII: Rules of Engagement	334
Evaluation Team Requirements	334
External Requirements	334
Internal Requirements	335
Customer Requirements	335
TEP Section VIII: Coordination Agreements	335
Level of Detail of Recommendations	335
List of Agreed-On Deliverables	336
The Coordination Agreements Section: A Catchall	336
TEP Section IX: Letter of Authorization	336
TEP Section X: Timeline of Events	336
Customizing and Modifying the Technical Evaluation Plan	337
Modifying the Ten NSA-Defined Areas	337
Level of Detail	338
Format	338
Getting the Signatures	338
Customer Approval	338
Evaluation Team Approval	339
Summary	340
Chapter 18 Starting Your Onsite Efforts	341
Introduction	342
Preparing for the Onsite Evaluation Phase	342
Scheduling	343
Day One Accomplishments	343
Day Two Accomplishments	343
Day Three Accomplishments	344
Day Four Accomplishments	344
Day Five Accomplishments	344
Flexibility and Adaptation	345

Administrative Planning	345
Technical Planning	345
IAM vs. IEM	346
Vulnerability Definitions	347
Onsite Evaluation Phase Objectives	347
Verification of “Known” and “Rogue” Components	348
Discovery of Technical Vulnerabilities	348
Validation = Value Add?	349
IEM Baseline Activities	350
I. Port Scanning	351
II. SNMP Scanning	351
III. Enumeration and Banner Grabbing	352
IV. Wireless Enumeration	352
V. Vulnerability Scanning	353
VI. Host Evaluation	354
VII. Network Device Analysis	354
VIII. Password Compliance Testing	354
IX. Application-Specific Scanning	355
X. Network Sniffing	355
Other Activities	355
The Role of CVE and CAN	356
The In-Brief	357
Presenting the TEP	357
Cultural Sensitivity	360
Summary	362
Chapter 19 Network Discovery Activities	363
Introduction	364
Goals and Objectives	364
Results as Findings and Evaluation Task Attributes	365
System Mapping	366
Tool Basics	367
Expected Usage and Requirements	367
Port Scanning	368
Nmap	369
NMAP Options	370
TCP SYN	370
UDP Scanning	371
Ping Scanning	372
Basic Nmap Options	373

SuperScan	374
ScanLine	378
SolarWinds.	379
Port Scan System Mapping	380
SNMP Scanning	380
SolarWinds.	381
SNMPSweep.	382
MIB Walk	382
MIB Browser.	384
SNScan	385
WS_Ping Pro-Pak	386
SNMP Scan System Mapping	387
Enumeration and Banner Grabbing.	388
Nmap	389
THC-Amap.	391
NBTScan.	392
SuperScan	393
WS_Ping Pro-Pak	396
UNIX Enumeration	397
Telnet	398
DNS Queries.	399
Enumeration and Banner-Grabbing System Mapping.	400
Wireless Enumeration.	401
Wireless Enumeration Obstacles	402
Kismet.	403
NetStumbler	404
Wireless Encryption Evaluation.	406
Wireless Enumeration System Mapping.	406
Summary.	408
Chapter 20 Collecting the Majority of Vulnerabilities	409
Introduction	410
Vulnerability and Attack Trends.	411
Vulnerability Scanning's Role in the IEM	414
Conducting Vulnerability Scans.	416
Breaking Out the Scanning Tools	417
Vulnerability Scanners: Commercial and Freeware	418
Conducting Host Evaluations	428
Host Evaluation Example Tools and Scripts	429
Benchmark Scripts and Custom Scripts.	430

Host Evaluations: What to Look For	433
Auditing	433
File/Directory Permissions	434
OS and Application Services	436
User Rights Assignments	437
Patch Management	437
Mapping the Findings to the IEM Process	438
Vulnerability Scans and Host Evaluations: Correlating the Data	438
Summarize and Validate Findings	441
Summary	442
Chapter 21 Fine-Tuning the Evaluation	443
Introduction	444
Network Device Analysis	444
Approaches Used in Network Device Analysis	444
Evaluating the Perimeter Design and Defenses	445
Evaluating Network Device Configurations	446
Password-Compliance Testing	448
Password-Compliance Testing Methods	448
Methods of Obtaining the Password File	449
Password-Compliance Testing Tools	451
Application-Specific Scanning	453
The DMZ	454
Types of Applications to Be Scanned	454
Network Protocol Analysis	457
Why Perform Network Protocol Analysis?	457
Introducing Network Protocol Analyzers	457
Summary	461
Chapter 22 The Onsite Closing Meeting	463
Introduction	464
Organizing the Meeting	464
Time and Location	464
Evaluation Team and Customer Involvement	465
The Customer	465
The Evaluation Team	466
Presentation Needs	466
The Agenda	467
TEP Overview	467
The Evaluation Process	468
How Was Information Collected?	468

The Tools	468
Customer Documentation	468
Customer Concerns	469
What Is Driving the Evaluation?	469
Customer Constraints	469
Protecting Testing Data	470
Setting Timelines	470
Important Events During Testing.	470
Final Report Delivery.	471
Overview of Critical Findings	471
How Does the Vulnerability Impact the System?	472
What Is the Likelihood That a Threat Will Exploit the Vulnerability?	472
Mapping to Business Mission and Objectives	472
Positive vs. Negative Findings	472
Points of Immediate Resolution	473
Short Term vs. Long Term.	473
What Do You Do With the Information That You Have Collected?	473
Summary	474
Chapter 23 Post-Evaluation Analysis	475
Introduction	476
Getting Organized	476
Analysis Needs.	476
Reporting Needs.	478
Categorization, Consolidation, Correlation, and Consultation.	479
False Positives and False Negatives.	479
Evaluation Perspectives	480
External Exposures.	480
Internal Exposures	481
System Boundaries.	481
Conducting Additional Research	481
Resources	482
Consulting Subject Matter Experts	483
Other Team Members	483
External Resources	484
Analyzing Customer Documentation	484
INFOSEC Policies and Procedures.	484
Previous Evaluations/VA/Penetration-Testing Results	485
Developing Practical Recommendations	486
Level of Detail	486

Finding	487
Description	487
References.	487
Criticality Rating.	487
Business Impact	488
Threat Likelihood	488
Recommendations.	489
Tying in Regulations, Legislation, Organizational Policies, and Industry Best Practices	490
Summary.	491
Chapter 24 Creating Measurements and Trending Results	493
Introduction	494
The Purpose and Goal of the Matrixes	494
Information Types	495
Common Vulnerabilities and Exposures.	498
NIST ICAT.	499
Developing System Vulnerability Criticality Matrixes	500
Developing Overall Vulnerability Criticality Matrixes.	508
Using the OVCM and SVCM	509
Summary.	511
Chapter 25 Trending Metrics.	513
Introduction	514
Metrics and Their Usefulness	514
Return on Investment	514
How Do We Compare?	515
The INFOSEC Posture Profile.	515
Defense in Depth.	516
Adversaries or Threats.	516
Protect	516
Detect.	517
Respond	517
Sustain.	517
People.	517
Technology	517
Defense in Multiple Places.	518
Layered Defenses.	518
Specify the Security Robustness.	518
Robust Key Management	518
Event Correlation	518
Operations.	519

Developing the INFOSEC Posture Profile	519
The INFOSEC Posture Rating	525
Value-Added Trending	526
Summary	528
Chapter 26 Final Reporting	531
Introduction	532
Pulling All the Information Together	532
The Team Meeting	533
Research	533
The SVCM and OVCM	534
Review	534
Making Recommendations	534
Findings	535
Recommendations	538
Creating the Final Report	539
Organizing the Data	539
Discussion of Findings	539
Final Report Delivery Date	539
The Cover Letter	539
The Executive Summary	539
The INFOSEC Profile	540
The Introduction	540
INFOSEC Analysis	541
Technical Areas	542
High-Criticality Findings	542
Medium-Criticality Findings	543
Low-Criticality Findings	544
The Conclusion	545
Posture Description	545
Posture Profile	545
Security Practices	546
Presenting the Final Report	547
Summary	548
Chapter 27 Summing Up the INFOSEC Evaluation Methodology	549
Introduction	550
The Pre-Evaluation Phase	551
The Onsite Evaluation	552
The Post-Evaluation Phase	553
Examples of INFOSEC Tools by Baseline Activity	553

Port Scanning	554
SNMP Scanning	555
Enumeration and Banner Grabbing.	557
Wireless Enumeration.	559
Vulnerability Scanning	561
Host Evaluation	563
Network Device Analysis	565
Password-Compliance Testing	565
Application-Specific Scanning.	567
Network Protocol Analysis	570
Technical Evaluation Plan Outline and Sample	572
Sample Technical Evaluation Plan	574
I. Evaluation Points of Contact	574
II. Methodology Overview.	575
III. Organizational and System Criticality Information	575
The OUCH Mission	575
OUCH Impact Definitions.	576
OUCH Organizational Criticality.	576
System Information Criticality	577
IV. Detailed Network Information.	577
V. Customer Concerns	578
VI. Customer Constraints	578
VII. Rules of Engagement	579
VIII. Internal and External Customer Requirements	579
IX. Coordination Agreements	579
Level of Detail of Recommendations	580
Deliverables	580
Other Agreements	580
X. Letter of Authorization	580
XI. Timeline of Evaluation Events	580
Part 3 Business Continuity & Disaster Recovery	581
Chapter 28 Business Continuity and	
 Disaster Recovery Overview	583
Introduction	584
Business Continuity and Disaster Recovery Defined	585
Components of Business.	586
People in BC/DR Planning	587
Process in BC/DR Planning.	588
Technology in BC/DR Planning	590

The Cost of Planning versus the Cost of Failure	591
People	594
Process	595
Technology	596
Types of Disasters	597
Natural Hazards	597
Cold Weather Related Hazards	598
Warm Weather Related Hazards	598
Geological Hazards	599
Human-Caused Hazards	599
Accidents and Technological Hazards	600
Electronic Data Threats	602
Personal Privacy	602
Privacy Standards and Legislation	603
Gramm-Leach-Bliley Act (GLBA)	603
Health Insurance Portability and Accountability Act (HIPAA)	604
Social Engineering	605
Fraud and Theft	605
General Business Fraud	605
Managing Access	608
Business Continuity and Disaster Recovery Planning Basics	608
Project Initiation	610
Risk Assessment	611
Business Impact Analysis	611
Mitigation Strategy Development	611
Plan Development	611
Training, Testing, Auditing	612
Plan Maintenance	612
Summary	613
Chapter 29 Project Initiation	615
Introduction	616
Elements of Project Success	617
Executive Support	617
User Involvement	620
Experienced Project Manager	621
Clearly Defined Project Objectives	621
Clearly Defined Project Requirements	622
Clearly Defined Scope	623
Shorter Schedule, Multiple Milestones	623
Clearly Defined Project Management Process	624

Project Plan Components	625
Project Definition	627
Problem and Mission Statement	627
Potential Solutions	627
Requirements and Constraints	628
Success Criteria	629
Project Proposal	629
Estimates	630
Project Sponsor	630
Forming the Project Team	631
Organizational	632
Technical	633
Logistical	633
Political	634
Project Organization	634
Project Objectives	634
Business Continuity Plan	635
Continuity of Operations Plan	635
Disaster Recovery Plan	635
Crisis Communication Plan	635
Cyber Incident Response Plan (CIRP)	636
Occupant Emergency Plan	636
Project Stakeholders	637
Project Requirements	638
Project Parameters	639
Project Infrastructure	642
Project Processes	643
Team Meetings	644
Reporting	644
Escalation	644
Project Progress	645
Change Control	645
Quality Control	646
Project Communication Plan	646
Project Planning	648
Work Breakdown Structure	648
Critical Path	648
Project Implementation	649
Managing Progress	650
Managing Change	650

Project Tracking	651
Project Close Out	651
Key Contributors and Responsibilities	652
Information Technology	653
Experience Working on a Cross-Departmental Team	653
Ability to Communicate Effectively	653
Ability to Work Well with a Wide Variety of People	654
Experience with Critical Business and Technology Systems	654
IT Project Management Leadership	655
Human Resources	655
Facilities/Security	655
Finance/Legal	656
Warehouse/Inventory/Manufacturing/Research	657
Purchasing/Logistics	658
Marketing and Sales	658
Public Relations	659
Project Definition	661
Business Requirements	662
Functional Requirements	664
Technical Requirements	665
Business Continuity and Disaster Recovery Project Plan	666
Project Definition, Risk Assessment	667
Business Impact Analysis	667
Risk Mitigation Strategies	667
Plan Development	667
Emergency Preparation	667
Training, Testing, Auditing	668
Plan Maintenance	668
Summary	670
Chapter 30 Risk Assessment	671
Introduction	672
Risk Management Basics	673
Risk Management Process	675
Threat Assessment	676
Vulnerability Assessment	677
Impact Assessment	677
Risk Mitigation Strategy Development	678
People, Process, Technology, and Infrastructure in Risk Management	678

People	678
Process	679
Technology	679
Infrastructure	680
IT-Specific Risk Management	680
IT Risk Management Objectives	680
The System Development Lifecycle Model	681
Risk Assessment Components	684
Information Gathering Methods	685
Natural and Environmental Threats	686
Fire	687
Floods	688
Severe Winter Storms	689
Electrical Storms	691
Drought	693
Earthquake	694
Tornados	696
Hurricanes/Typhoons/Cyclones	696
Tsunamis	697
Volcanoes	698
Avian Flu/Pandemics	698
Human Threats	701
Fire	701
Theft, Sabotage, Vandalism	701
Labor Disputes	702
Workplace Violence	702
Terrorism	703
Chemical or Biological Hazards	704
War	705
Cyber Threats	705
Cyber Crime	707
Loss of Records or Data—Theft, Sabotage, Vandalism	709
IT System Failure—Theft, Sabotage, Vandalism	710
Infrastructure Threats	710
Building Specific Failures	710
Public Transportation Disruption	711
Loss of Utilities	711
Disruption to Oil or Petroleum Supplies	711
Food or Water Contamination	712
Regulatory or Legal Changes	712

Looking Back	713
Threat Checklist	713
Threat Assessment Methodology	717
Quantitative Threat Assessment	717
Qualitative Threat Assessment	721
Vulnerability Assessment	725
People, Process, Technology, and Infrastructure	726
People	726
Process	727
Technology	727
Infrastructure	727
Vulnerability Assessment	728
Summary	731
Chapter 31 Business Impact Analysis	733
Introduction	734
Business Impact Analysis Overview	734
Upstream and Downstream Losses	736
Understanding the Human Impact	737
Key Positions	737
Human Needs	738
Understanding Impact Criticality	739
Criticality Categories	739
Mission-Critical	739
Vital	740
Important	740
Minor	740
Recovery Time Requirements	741
Identifying Business Functions	746
Facilities and Security	747
Finance	748
Human Resources	748
IT	749
Legal/Compliance	749
Manufacturing (Assembly)	749
Marketing and Sales	750
Operations	750
Research and Development	750
Warehouse (Inventory, Order Fulfillment, Shipping, Receiving)	751
Other Areas	751

Gathering Data for the Business Impact Analysis	752
Data Collection Methodologies.	753
Questionnaires.	753
Interviews	754
Workshops.	755
Determining the Impact.	756
Business Impact Analysis Data Points.	757
Understanding IT Impact	762
Example of Business Impact Analysis For Small Business.	763
Preparing the Business Impact Analysis Report	770
Summary.	771
Chapter 32 Mitigation Strategy Development	773
Introduction	774
Types of Risk Mitigation Strategies.	775
Risk Acceptance.	775
Risk Avoidance	776
Risk Limitation	776
Risk Transference	777
The Risk Mitigation Process	778
Recovery Requirements	778
Recovery Options	778
As Needed	780
Prearranged.	780
Preestablished	780
Recovery Time of Options	781
Cost versus Capability of Recovery Options	781
Recovery Service Level Agreements	783
Review Existing Controls.	783
Developing Your Risk Mitigation Strategy.	784
Sample 1: Section from Mitigation Strategy for Critical Data	785
Sample 2: Section from Mitigation Strategy for Critical Data	786
People, Buildings, and Infrastructure	788
IT Risk Mitigation.	789
Critical Data and Records.	789
Critical Systems and Infrastructure.	789
Reviewing Critical System Priorities	790
Backup and Recovery Considerations.	790
Alternate Business Processes	790
IT Recovery Systems	791

Alternate Sites	792
Fully Mirrored Site	792
Hot Site	792
Warm Site.	792
Mobile Site.	793
Cold Site	793
Reciprocal Site	793
Disk Systems	793
RAID.	793
Remote Journaling	793
Replication.	794
Electronic Vaulting.	794
Standby Operating Systems	794
Network-Attached Storage (NAS)	794
Storage Area Network (SAN).	794
Desktop Solutions	794
Software and Licensing.	796
Web Sites	796
Summary.	797

Chapter 33 Business Continuity/Disaster Recovery

Plan Development	799
Introduction	800
Phases of the Business Continuity and Disaster Recovery.	801
Activation Phase.	801
Major Disaster or Disruption	802
Intermediate Disaster or Disruption	802
Minor Disaster or Disruption	802
Activating BC/DR Teams	803
Developing Triggers	803
Transition Trigger—Activation to Recovery	805
Recovery Phase	805
Transition Trigger—Recovery to Continuity.	805
Business Continuity Phase.	806
Maintenance/Review Phase	807
Defining BC/DR Teams and Key Personnel	807
Crisis Management Team	808
Management	808
Damage Assessment Team	808
Operations Assessment Team	808

IT Team	809
Administrative Support Team.	809
Transportation and Relocation Team	809
Media Relations Team	810
Human Resources Team	810
Legal Affairs Team.	810
Physical/Personnel Security Team	810
Procurement Team (Equipment and Supplies)	811
General Team Guidelines	811
BC/DR Contact Information.	813
Defining Tasks, Assigning Resources	815
Alternate Site	815
Selection Criteria.	816
Contractual Terms	816
Comparison Process.	816
Acquisition and Testing	816
Contracts for BC/DR Services	817
Develop Clear Functional and Technical Requirements	817
Determine Required Service Levels	817
Compare Vendor Proposal/Response to Requirements	818
Identify Requirements Not Met by Vendor Proposal	818
Identify Vendor Options Not Specified in Requirements	818
Communications Plans	820
Internal	820
Employee.	820
Customers and Vendors.	821
Shareholders.	821
The Community and the Public	821
Event Logs, Change Control, and Appendices	822
Event Logs	822
Change Control	823
Distribution	824
Appendices.	825
Additional Resources	826
What's Next	826
Summary.	827
Chapter 34 Emergency Response and Recovery	829
Introduction	830
Emergency Management Overview	830

Emergency Response Plans	831
Emergency Response Teams	833
Crisis Management Team	834
Emergency Response and Disaster Recovery	834
Alternate Facilities Review and Management.	835
Communications	835
Human Resources	835
Legal	836
Insurance	836
Finance	836
Disaster Recovery	837
Activation Checklists	837
Recovery Checklists	837
IT Recovery Tasks	837
Computer Incident Response	838
CIRT Responsibilities	839
Monitor	839
Alert and Mobilize	840
Assess and Stabilize	840
Resolve	840
Review.	840
Business Continuity	841
Summary	843
Chapter 35 Training, Testing, and Auditing.	845
Introduction	846
Training for Disaster Recovery and Business Continuity	846
Emergency Response	847
Disaster Recovery and Business Continuity	
Training Overview	847
Training Scope, Objectives, Timelines, and Requirements.	848
Performing Training Needs Assessment	849
Developing Training.	849
Scheduling and Delivering Training	851
Monitoring and Measuring Training	851
Training and Testing for Your Business Continuity and	
Disaster Recovery Plan	852
Paper Walk-through	854
Develop Realistic Scenarios	854
Develop Evaluation Criteria	855

Provide Copies of the Plan	855
Divide Participants by Team	856
Use Checklists	856
Take Notes	856
Identify Training Needs	856
Develop Summary and Lessons Learned	856
Functional Exercises	857
Field Exercises	858
Full Interruption Test	858
Training Plan Implementers	858
Testing the BC/DR Plan	859
Understanding of Processes	859
Validation of Task Integration	860
Confirm Steps	860
Confirm Resources	860
Familiarize with Information Flow	861
Identify Gaps or Weaknesses	861
Determines Cost and Feasibility	861
Test Evaluation Criteria	864
Recommendations	864
Performing IT Systems and Security Audits	864
IT Systems and Security Audits	864
Summary	867
Chapter 36 BC/DR Plan Maintenance	869
Introduction	870
BC/DR Plan Change Management	870
Training, Testing, and Auditing	871
Changes in Information Technologies	871
Changes in Operations	872
Corporate Changes	873
Legal, Regulatory, or Compliance Changes	873
Strategies for Managing Change	873
Monitor Change	874
People	875
Process	875
Technology	875
Evaluate and Incorporate Change	875
BC/DR Plan Audit	877
Plan Maintenance Activities	877

Project Close Out	878
Summary	880
Chapter 37 BC/DR Checklists	883
Risk Assessment	884
Threat and Vulnerability Assessment	884
Business Impact Analysis	884
Mitigation Strategies	885
Crisis Communications Checklist	885
Communication Checklist	885
Message Content	886
Business Continuity and Disaster Recovery Response Checklist	887
Emergency and Recovery Response Checklist	887
Activation Checklists	887
Initial Response	888
Damage and Situation Assessment	888
Disaster Declaration and Notification	888
Emergency Response Checklists	889
Emergency Checklist One—General Emergency Response	889
Emergency Checklist Two—Evacuation or Shelter-in-Place Response	889
Emergency Checklist Three—Specific Emergency Responses	890
Emergency Checklist Four—Emergency Response Contact List, Maps, Floor Plans	890
Emergency Checklist Five—Emergency Supplies and Equipment	891
Recovery Checklists	891
Recovery Checklist One—General	891
Recovery Checklist Two—Inspection, Assessment, and Salvage	892
Business Continuity Checklist	893
Resuming Work	893
Resuming Work	893
Human Resources	894
Insurance and Legal	895
Manufacturing, Warehouse, Production, and Operations	895
Resuming Normal Operations	896
Existing Facility	896
New Facility	897
Transition to Normalized Activities	897

IT Recovery Checklists	898
IT Recovery Checklist One—Infrastructure	898
Recovery Checklist Two—Applications.	899
Recovery Checklist Three—Office Area and End-User Recovery	899
Recovery Checklist Four—Business Process Recovery	900
Recovery Checklist Five—Manufacturing, Production, and Operations Recovery	901
Training, Testing, and Auditing Checklists	902
Training and Testing	902
IT Auditing	902
BC/DR Plan Maintenance Checklist	903
Change Management	903
Index	905

Part 1

From Vulnerability to Patch

This page intentionally left blank

Chapter 1

Windows of Vulnerability

Solutions in this chapter:

- What Are Vulnerabilities?
- Understanding the Risks Posed by Vulnerabilities

☒ **Summary**

Introduction

This chapter will address vulnerabilities and why they are important. It also discusses a concept known as Windows of Vulnerability, and shows how to determine the risk a given vulnerability poses to your environment.

What Are Vulnerabilities?

So, what are vulnerabilities? In the past, many people considered a vulnerability to be a software or hardware bug that a malicious individual could exploit. Over the years, however, the definition of *vulnerability* has evolved into a software or hardware bug or *misconfiguration* that a malicious individual can exploit. Patch management, configuration management, and security management all evolved from single disciplines, often competing with each other, into one IT problem known today as vulnerability management.

NOTE

Throughout this book, we will reference vulnerabilities by their CVE numbers. CVE stands for Common Vulnerabilities and Exposures, and a list of CVE numbers was created several years ago to help standardize vulnerability naming. Before this list was compiled, vendors called vulnerabilities by whatever names they came up with, making vulnerability tracking difficult and confusing. The CVE created a list of all vulnerabilities and assigned each one a CVE ID in the format *CVE-year-number*. Vendors have been encouraged to use CVE numbers when referencing vulnerabilities, a practice which has removed most of the confusion. More information on CVE numbers is available at <http://cve.mitre.org>.

On the surface, vulnerability management appears to be a simple task. Unfortunately, in most corporate networks, vulnerability management is difficult and complicated. A typical organization has custom applications, mobile users, and critical servers, all of which have diverse needs that cannot be simply secured and forgotten. Software vendors are still releasing insecure code, hardware vendors do not build security into their products, and systems administrators are left to clean up the mess. Add to this compliance regulations that make executives nervous, and you have a high-stress situation which is conducive to costly mistakes.

The complications surrounding vulnerability management create what is known as a Window of Vulnerability. Although this may sound like a clever play on words to draw attention to the most commonly run operating system, it is actually used in reference to the length of time a system is vulnerable to a given security flaw, configuration issue, or some other factor that reduces its overall security. There are two types of Windows of Vulnerability:

- **Unknown Window of Vulnerability** The time from when a vulnerability is discovered to when the system is patched.
- **Known Window of Vulnerability** The time from when a vendor releases a patch to when the system is patched.