

Contents

Foreword	xix
Chapter 1 Windows of Vulnerability	1
Introduction	2
What Are Vulnerabilities?	2
Understanding the Risks Posed by Vulnerabilities	9
Summary	15
Solutions Fast Track	15
Frequently Asked Questions	16
Chapter 2 Vulnerability Assessment 101	17
Introduction	18
What Is a Vulnerability Assessment?	18
Step 1: Information Gathering/Discovery	18
Step 2: Enumeration	21
Step 3: Detection	22
Seeking Out Vulnerabilities	24
Detecting Vulnerabilities via Security Technologies	24
Deciphering VA Data	
Gathered by Security Technologies	26
Accessing Vulnerabilities	
via Remediation (Patch) Technologies	29
Extracting VA Data from Remediation Repositories ..	30
Leveraging Configuration Tools to Assess Vulnerabilities	32
The Importance of Seeking Out Vulnerabilities	34
Looking Closer at the Numbers	35
Summary	40
Solutions Fast Track	40
Frequently Asked Questions	41

Chapter 3 Vulnerability Assessment Tools	45
Introduction	46
Features of a Good Vulnerability Assessment Tool	46
Using a Vulnerability Assessment Tool	50
Step 1: Identify the Hosts on Your Network	51
Step 2: Classify the Hosts into Asset Groups	55
Step 3: Create an Audit Policy	56
Step 4: Launch the Scan	58
Step 5: Analyze the Reports	59
Step 6: Remediate Where Necessary	61
Summary	62
Solutions Fast Track	62
Frequently Asked Questions	63
Chapter 4 Vulnerability Assessment: Step One	65
Introduction	66
Know Your Network	67
Classifying Your Assets	74
I Thought This Was a Vulnerability Assessment Chapter	78
Summary	82
Solutions Fast Track	82
Frequently Asked Questions	83
Chapter 5 Vulnerability Assessment: Step Two	85
Introduction	86
An Effective Scanning Program	86
Scanning Your Network	88
When to Scan	96
Summary	100
Solutions Fast Track	100
Frequently Asked Questions	101
Chapter 6 Going Further	103
Introduction	104
Types of Penetration Tests	104
Scenario: An Internal Network Attack	106
Client Network	107
Step 1: Information Gathering	109

Operating System Detection	110
Discovering Open Ports and Enumerating	112
Step 2: Determine Vulnerabilities	116
Setting Up the VA	117
Interpreting the VA Results	120
Penetration Testing	125
Step 3: Attack and Penetrate	126
Uploading Our Data	126
Attack and Penetrate	129
Searching the Web Server for Information	134
Discovering Web Services	135
Vulnerability Assessment versus a Penetration Test	139
Tips for Deciding between Conducting a VA or a Penetration Test	139
Internal versus External	141
Summary	144
Solutions Fast Track	144
Frequently Asked Questions	145
Chapter 7 Vulnerability Management	147
Introduction	148
The Vulnerability Management Plan	149
The Six Stages of Vulnerability Management	150
Stage One: Identify	151
Stage Two: Assess	152
Stage Three: Remediate	153
Stage Four: Report	154
Stage Five: Improve	155
Stage Six: Monitor	156
Governance (What the Auditors Want to Know)	158
Measuring the Performance of a Vulnerability Management Program	160
Common Problems with Vulnerability Management	164
Summary	166
Solutions Fast Track	166
Frequently Asked Questions	170

Chapter 8 Vulnerability Management Tools	171
Introduction	172
The Perfect Tool in a Perfect World	172
Evaluating Vulnerability Management Tools	174
Commercial Vulnerability Management Tools	177
eEye Digital Security	177
Symantec (BindView)	178
Attachmate (NetIQ)	178
StillSecure	179
McAfee	179
Open Source and Free Vulnerability Management Tools	180
Asset Management, Workflow, and Knowledgebase	180
Host Discovery	180
Vulnerability Scanning and Configuration Scanning	181
Configuration and Patch Scanning	181
Vulnerability Notification	182
Security Information Management	182
Managed Vulnerability Services	183
Summary	186
Solutions Fast Track	186
Frequently Asked Questions	188
Chapter 9 Vulnerability and Configuration Management	189
Introduction	190
What is Vulnerability Management?	190
Patch Management	190
System Inventories	195
System Classification	197
System Baselines	199
Creating a Baseline	199
Baseline Example	202
The Common Vulnerability Scoring System	203
Building a Patch Test Lab	204
Establish a Patch Test Lab with “Sacrificial Systems”	204
Virtualization	205
Enviromental Simulation	207
Patch Distribution and Deployment	209

Configuration Management	211
Logging and Reporting	212
Change Control	212
Summary	216
Solutions Fast Track	217
Frequently Asked Questions	218
Chapter 10 Regulatory Compliance	221
Introduction	222
Regulating Assessments and Pen Tests	222
The Payment Card Industry (PCI) Standard	223
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)	225
The Sarbanes-Oxley Act of 2002 (SOX)	228
Compliance Recap	230
Drafting an Information Security Program	233
Summary	239
Solutions Fast Track	239
Frequently Asked Questions	240
Chapter 11 Tying It All Together	243
Introduction	244
A Vulnerability Management Methodology	244
Step One: Know Your Assets	245
What You Need to Do	245
Why You Need to Do It	246
How to Do It	246
What Tools Exist to Help You Do It	249
Step Two: Categorize Your Assets	250
What You Need to Do	250
Why You Need to Do It	251
How to Do It	252
What Tools Exist to Help You Do It	252
Step Three: Create a Baseline Scan of Assets	253
What You Need to Do	253
Why You Need to Do It	254
How to Do It	254

What Tools Exist to Help You Do It	255
Step Four: Perform a Penetration Test on Certain Assets . . .	256
What You Need to Do	256
Why You Need to Do It	257
How to Do It	257
What Tools Exist to Help You Do It	258
Step Five: Remediate Vulnerabilities and Risk	259
What You Need to Do	259
Why You Need to Do It	259
How to Do It	259
What Tools Exist to Help You Do It	261
Step Six: Create a Vulnerability Assessment Schedule	261
What You Need to Do	261
Why You Need to Do It	262
How to Do It	262
Step Seven: Create a Patch	
and Change Management Process	265
What You Need to Do	265
Why You Need to Do It	265
How to Do It	265
What Tools Exist to Help You Do It	266
Step Eight: Monitor for New Risks to Assets	266
What You Need to Do	266
Why You Need to Do It	267
How to Do It	267
What Tools Exist to Help You Do It	268
Summary	271

Appendix A Legal Principles for Information Security Evaluations 273

Introduction	274
Uncle Sam Wants You: How Your Company’s Information Security Can Affect U.S. National Security (and Vice Versa)	275
Legal Standards Relevant to Information Security	280
Selected Federal Laws	281
Gramm-Leach-Bliley Act	281
Health Insurance Portability and Accountability Act	282
Sarbanes-Oxley	283

Federal Information Security and Management Act	284
FERPA and the TEACH Act	284
Electronic Communications Privacy Act and Computer Fraud and Abuse Act	285
State Laws	285
Unauthorized Access	285
Deceptive Trade Practices	286
Enforcement Actions	286
Three Fatal Fallacies	287
The “Single Law” Fallacy	287
The Private Entity Fallacy	288
The “Pen Test Only” Fallacy	289
Do It Right or Bet the Company:	
Tools to Mitigate Legal Liability	290
We Did our Best; What’s the Problem?	290
The Basis for Liability	291
Negligence and the “Standard of Care”	291
What Can Be Done?	292
Understand your Legal Environment	293
Comprehensive and Ongoing Security Assessments, Evaluations, and Implementation	293
Use Contracts to Define Rights and Protect Information	294
Use Qualified Third-party Professionals	295
Making Sure Your Standards-of-Care Assessments Keep Up with Evolving Law	296
Plan for the Worst	297
Insurance	297
What to Cover in IEM Contracts ⁶⁴	298
What, Who, When, Where, How, and How Much	299
What	299
Who	303
When	308
Where	308
How	309
How Much	310
Murphy’s Law (When Something Goes Wrong)	312

Where the Rubber Meets the Road: The LOA as Liability Protection	314
Beyond You and Your Customer	316
The First Thing We Do...? Why You	
Want Your Lawyers Involved From Start to Finish	318
Attorney-Client Privilege	319
Advice of Counsel Defense	321
Establishment and Enforcement of Rigorous Assessment, Interview, and Report-Writing Standards	322
Creating a Good Record for Future Litigation	323
Maximizing Ability to Defend Litigation	323
Dealing with Regulators, Law Enforcement, Intelligence, and Homeland Security Officials	324
The Ethics of Information Security Evaluation	326
Solutions Fast Track	327
Frequently Asked Questions	330
References	332
Appendix B Examples of INFOSEC Tools by Baseline Activity	339
Index.	361