

Contents

Foreword	xix
Introduction	xxi
Part I Background on Cyber Crime, Insider Threats, and ESM	1
Chapter 1 Cyber Crime and Cyber Criminals 101	3
About this Chapter	4
Computer Dependence and Internet Growth	4
The Shrinking Vulnerability Threat Window	5
Motivations for Cyber Criminal Activity	7
Black Markets	11
Hackers	13
Script Kiddies	14
Solitary Cyber Criminals and Exploit Writers for Hire	15
Organized Crime	17
Identity Thieves (Impersonation Fraudsters)	19
Competitors	24
Activist Groups, Nation-State Threats, and Terrorists	24
Activists	25
Nation-State Threats	27
China	27
France	27
Russia	28
United Kingdom	28
United States	28
Terrorists	30
Insiders	32
Tools of the Trade	34
Application-Layer Exploits	35
Botnets	35
Buffer Overflows	36
Code Packing	36
Denial-of-service (DoS) Attacks	36
More Aggressive and Sophisticated Malware	37

Nonwired Attacks and Mobile Devices	38
Password-cracking	38
Phishing	39
Reconnaissance and Googledorks	41
Rootkits and Keyloggers	41
Social Engineering Attacks	42
Voice-over-IP (VoIP) Attacks	43
Zero-Day Exploits	44
Summary	46
Chapter 2 Insider Threats	49
Understanding Who the Insider Is	50
Psychology of Insider Identification	55
Insider Threat Examples from the Media	57
Insider Threats from a Human Perspective	59
A Word on Policies	60
Insider Threats from a Business Perspective	62
Risk	63
Insider Threats from a Technical Perspective	63
Need-to-know	64
Least Privileges	65
Separation of Duties	65
Strong Authentication	65
Access Controls	66
Incident Detection and Incident Management	66
Summary	68
Chapter 3 Enterprise Security Management (ESM) . . .	69
ESM in a Nutshell	70
Key ESM Feature Requirements	71
Event Collection	71
Normalization	72
Categorization	72
Asset Information	73
Vulnerability Information	73
Zoning and Global Positioning System Data	73
Active Lists	75
Actors	76
Data Content	77
Correlation	77

Prioritization	77
Event and Response Time Reduction	78
Anomaly Detection	78
Pattern Discovery	79
Alerting	80
Case Management	80
Real-Time Analysis and Forensic Investigation	81
Visualization	81
High-Level Dashboards	81
Detailed Visualization	81
Reporting	83
Remediation	84
Return On Investment (ROI)	
and Return On Security Investment (ROSI)	85
Alternatives to ESM	90
Do Nothing	90
Custom In-house Solutions	91
Outsourcing and Cosourcing	93
Cosourcing examples:	95
Summary	97
Part II Real Life Case Studies	99
Chapter 4 Imbalanced Security—	
A Singaporean Data Center	101
Chapter 5 Comparing Physical & Logical Security	
Events—A U.S. Government Agency	107
Chapter 6 Insider with a Conscience—	
An Austrian Retailer	115
Chapter 7 Collaborative Threat—	
A Telecommunications Company in the U.S.	123
Chapter 8 Outbreak from Within—	
A Financial Organization in the U.K.	129
Chapter 9 Mixing Revenge and Passwords—	
A Utility Company in Brazil	137
Chapter 10 Rapid Remediation—	
A University in the United States.	145

Chapter 11 Suspicious Activity— A Consulting Company in Spain	155
Chapter 12 Insiders Abridged	161
Malicious use of Medical Records	162
Hosting Pirated Software	163
Pod-Slurping	164
Auctioning State Property	165
Writing Code for Another Company	166
Outsourced Insiders	167
Smuggling Gold in Rattus Norvegicus	168
Part III The Extensibility of ESM	169
Chapter 13 Establishing Chain-of- Custody Best Practices with ESM	171
Disclaimer	172
Monitoring and Disclosure	172
Provider Protection Exception	173
Consent Exception	173
Computer Trespasser Exception	174
Court Order Exception	174
Best Practices	174
Canadian Best Evidence Rule	176
Summary	177
Chapter 14 Addressing Both Insider Threats and Sarbanes-Oxley with ESM	179
Why Sarbanes-Oxley	180
A Primer on Sarbanes-Oxley	181
Section 302: Corporate Responsibility for Financial Reports	182
Section 404: Management Assessment of Internal Controls	182
Separation of Duties	182
Monitoring Interaction with Financial Processes	183
Detecting Changes in Controls over Financial Systems	183
Section 409: Real-time Issuer Disclosures	184
Summary	185

Chapter 15 Incident Management with ESM 187

Incident Management Basics	188
Improved Risk Management	189
Improved Compliance	190
Reduced Costs	190
Current Challenges	190
Process	190
Organization	191
Technology	191
Building an Incident Management Program	192
Defining Risk	192
Five Steps to Risk Definition for Incident Management	193
Process	193
Training	195
Stakeholder Involvement	195
Remediation	196
Documentation	196
Reporting and Metrics	197
Summary	198

Chapter 16 Insider Threat Questions and Answers . . . 199

Introduction	200
Insider Threat Recap	200
Question One – Employees	201
The Hiring Process	201
Reviews	202
Awareness	202
NIST 800-50	203
Policies	205
Standards	205
Security Memorandum Example	206
Procedure	208
Question Two – Prevention	210
Question Three – Asset Inventories	211
Question Four – Log Collection	214
Security Application Logs	215
Operating System Log	216
Web Server Logs	216

NIST 800-92217

Question Five – Log Analysis219

Question Six – Specialized Insider Content221

Question Seven – Physical and
Logical Security Convergence222

Question Eight – IT Governance227

NIST 800-53231

Question Nine – Incident Response234

Question Ten – Must Haves235

Appendix A Examples of Cyber Crime Prosecutions . . 237

U.S. Department of Justice Cases238

California—Central District—United States v. Jay R.
Echouafni et al. (Operation Cyberslam)238

United States v. Jie Dong239

United States v. Calin Mateias239

California—Northern District—

United States v. Robert McKimmey241

United States v. Laurent Chavet241

United States v. Shan Yan Ming242

United States v. Robert Lyttle242

United States v. Roman Vega242

United States v. Michael A. Bradley243

Missouri—Western District—

United States v. Melissa Davidson243

United States v. Soji Olowokandi244

New York—Southern District—United States
v. Jason Smathers and Sean Dunaway244

Pennsylvania Western District—United States
v. Calin Mateias246

United States v. Scott Eric Catalano247

United States v. Myron Tereshchuk247

United States v. Jeffrey Lee Parson248

Bibliography. 249

Articles, Webcasts and Podcasts with the Author250

Online Articles250

Webcasts251

Podcasts252

Index. 253