

MANAGEMENT

INFORMATION SECURITY

Second Edition

mfjrr jjJ-S v T

tmc- wife rtsW

Dr. Michael E. Whitman, CISSP

oi r: r?w

Herbert J. Mattord, CISSP
Kennesaw State University

• HOCHSCHULE
LIECHTENSTEIN
Btthliothek

THOMSON
*
COURSE TECHNOLOGY

Australia • Canada • Mexico • Singapore • Spain • United Kingdom • United States

Preface	xv
Chapter 1 <i>Introduction to the Management of Information Security</i>	1
Introduction	2
What Is Security?	4
NSTISSC Security Model	4
Key Concepts of Information Security	6
What Is Management?	9
The Difference Between Leadership and Management	9
Characteristics of a Leader	10
Characteristics of Management	11
Solving Problems	14
Principles of Information Security Management	17
Chapter Summary	20
Review Questions	21
Exercises	22
Case Exercises	22
Endnotes	22
Chapter 2 <i>Planning for Security</i>	23
Introduction	25
The Role of Planning	26
Precursors to Planning	26
Values Statement	27
Vision Statement	27
Mission Statement	28
Strategic Planning	29
Creating a Strategic Plan	30
Planning Levels	31
Planning and the CISO	32
Planning for Information Security Implementation	35
Introduction to the Security Systems Development Life Cycle	37
Comparing the SDLC and the SecSDLC	53
Chapter Summary	55
Review Questions	56
Exercises	56
Case Exercises	57
Endnotes	57
Chapter 3 <i>Planning for Contingencies</i>	59
Introduction	60
What Is Contingency Planning?	61
Components of Contingency Planning	64
Business Impact Analysis	64
Incident Response Plan	68

Disaster Recovery Plan	79
Business Continuity Plan	87
Timing and Sequence of CP Elements	91
Business Resumption Planning	93
Testing Contingency Plans	99
Contingency Planning: Final Thoughts	100
Chapter Summary	101
Review Questions	102
Exercises	103
Case Exercises	104
Endnotes *	104

Chapter 4 *Information Security Policy* 107

Introduction	108
Why Policy?	109
Policy, Standards, and Practices	111
Enterprise Information Security Policy	113
Integrating an Organization's Mission and Objectives into the EISP	113
EISP Elements	114
Example EISP Components	115
Issue-Specific Security Policy	118
Components of the ISSP	119
Implementing the ISSP	122
System-Specific Security Policy	124
Managerial Guidance SysSPs	125
Technical Specifications SysSPs	125
Guidelines for Effective Policy	130
Developing Information Security Policy	130
Policy Distribution	134
Policy Reading	134
Policy Comprehension	135
Policy Compliance	136
Policy Enforcement	136
Automated Tools	137
The <i>Information Securities Policy Made Easy</i> Approach	138
SP 800-18 Rev. 1: <i>Guide for Developing Security Plans for Federal Information Systems</i>	149
A Final Note on Policy	151
Chapter Summary	152
Review Questions	153
Exercises	153
Case Exercises	154
Endnotes	154

Chapter 5 *Developing the Security Program* 157

Introduction	158
Organizing for Security	159
Security in Large Organizations	163
Security in Medium-Sized Organizations	164
Security in Small Organizations	166
Placing Information Security Within an Organization	168
Option 1: Information Technology	171
Option 2: Security	172
Option 3: Administrative Services	174
Option 4: Insurance and Risk Management	175

Option 5: Strategy and Planning	176
Option 6: Legal	178
Option 7: Internal Audit	179
Option 8: Help Desk	180
Option 9: Accounting and Finance Through I T . ^ w^frtiiM *«IH T — %.. jj f	181
Option 10: Human Resources	181
Option 11: Facilities Management	181
Option 12: Operations	181
Summary of Reporting Relationships	181
Components of the Security Program	182
Information Security Roles and Jitles	184
Chief Information Security Officer	184
Security Managers	185
Security Administrators and Analysts	185
Security Technicians	186
Security Staffers and Watchstanders	186
Security Consultants	186
Security Officers and Investigators	187
Help Desk Personnel	187
Implementing Security Education, Training, and Awareness Programs	187
Security Education	188
Security Training	191
Training Techniques	193
Security Awareness	198
Chapter Summary	206
Review Questions	207
Exercises	207
Case Exercises	208
Endnotes	208

Chapter 6 Security Management Models and Practices 211

Introduction	212
Security Management Models	213
ISO/IEC 17799:2005 <i>Information Technology—Security Techniques—Code of Practice for Information Security Management</i>	214
ISO/IEC 27001:2005: The Information Security Management System	218
NIST Security Models	221
RFC 2196 Site Security Handbook	231
COBIT	232
COSO	235
Security Management Practices	236
Standards of Due Care/Due Diligence	236
Recommended Security Practices	237
The Gold Standard	240
Selecting Recommended Practices	240
Benchmarking, and Recommended Practices Limitations	241
Baselining	242
Metrics in Information Security Management	244
Emerging Trends in Certification and Accreditation	246
SP 800-37: Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems	247
SP 800-53: Minimum Security Controls for Federal Information Technology Systems	249
Chapter Summary	251
Review Questions	252

Exercises	253
Case Exercises	253
Endnotes	253
Chapter 7 <i>Risk Management: Identifying and Assessing Risk</i>	257
Introduction	258
Risk Management	259
Knowing Ourselves	259
Knowing the Enemy	259
Accountability for Risk Management	260
Risk Identification	261
Creating an Inventory of Information Assets	261
Classifying and Categorizing Assets	266
Assessing Values for Information Assets	266
Listing Assets in Order of Importance	269
Data Classification Model	270
Security Clearances	271
Management of the Classified Information Asset	272
Threat Identification	272
The TVA Worksheet	281
Risk Assessment	283
Introduction to Risk Assessment	283
Likelihood	284
Assessing Potential Loss	284
Percentage of Risk Mitigated by Current Controls	285
Uncertainty	285
Risk Determination	285
Identify Possible Controls	286
Access Controls	286
Documenting the Results of Risk Assessment	287
Chapter Summary	290
Review Questions	291
Exercises	292
Case Exercises	293
Endnotes	293
Chapter 8 <i>Risk Management: Controlling Risk</i>	
Introduction	
Risk Control Strategies	
Avoidance	
Transference	
Mitigation	
Acceptance	
Managing Risk	
Feasibility Studies and Cost-Benefit Analysis	
Cost-Benefit Analysis	
Other Feasibility Studies	
Alternatives to Feasibility Analysis	
Recommended Risk Control Practices	
Qualitative Measures	
Delphi Technique	
A Single-Source Approach to Risk Management	
The OCTAVE Method*	
Important Aspects of the OCTAVE Method	
Phases, Processes, and Activities	

Preparing for the OCTAVE Method		
Phase 1: Build Asset-Based Threat Profiles	•	
Phase 2: Identify Infrastructure Vulnerabilities	•	322
Phase 3: Develop Security Strategy and Plans		323
Microsoft Risk Management Approach		324
Assessing Risk	^,r^iA-j	325
Conducting Decision Support		325
Implementing Controls	*<g,	325
Measuring Program Effectiveness	-., -	
Preliminary Tasks		
Roles and Responsibilities	.,	330
Chapter Summary	.,	333
Review Questions		333
Exercises		334
Case Exercises	.,.,.,iO((.f. &.surjiV	336
Entinotes	•	336
Chapter 9 Protection Mechanisms	*_	339
Introduction		341
Access Controls		342
Identification		342
Authentication	,	342
Authorization		348
Accountability		349
Evaluating Biometrics		351
Acceptability of Biometrics		352
Managing Access Controls		353
Firewalls		353
The Development of Firewalls		353
Firewall Architectures	>	356
Selecting the Right Firewall		359
Managing Firewalls		360
Intrusion Detection Systems		362
Host-Based IDS	*	362
Network-Based IDS		363
Signature-Based IDS		363
Statistical Anomaly-Based IDS		364
Intrusion Prevention Systems		364
Managing Intrusion Detection Systems		365
Remote Access Protection		365
RADIUS and TACACS		J3fir
Managing Dial-Up Connections		
Wireless Networking Protection	pj ,,,p' -\ f> ..((: ,f3g^	368
Wired Equivalent Privacy (WEP)		368
Wi-Fi Protected Access (WPA)		369
Wi-Max		369
Managing Wireless Connections		369
Scanning and Analysis Tools		370
Port Scanners		371
Vulnerability Scanners		372
Packet Sniffers		372
Content Filters		373
Trap and Trace		373
Managing Scanning and Analysis Tools		373

Cryptography	374
Encryption Operations	376
Using Cryptographic Controls	383
Managing Cryptographic Controls	386
Chapter Summary	389
Review Questions	390
Exercises	391
Case Exercises	391
Endnotes	392
	TM ..
Chapter 10 <i>Personnel and Security</i>	393
Introduction	395
Staffing the Security Function	395
Qualifications and Requirements	396
Entering the Information Security Profession	396
Information Security Positions	397
Information Security Professional Credentials	407
Certified Information Systems Security Professional (CISSP) and Systems Security Certified Practitioner (SSCP)	407
Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM)	409
Global Information Assurance Certification (GIAC)	411
Security Certified Program (SCP)	412
Security+	412
Certified Computer Examiner (CGE)	413
Certified Information Forensics Investigator (CIFI)	414
Certification Costs	414
Employment Policies and Practices	416
Hiring	417
Contracts and Employment	419
Security as Part of Performance Evaluation	419
Termination Issues	419
Personnel Security Practices	421
Security of Personnel and Personal Data	423
Security Considerations for Nonemployees	423
Chapter Summary	429
Review Questions	429
Exercises	430
Case Exercises	431
Endnotes	431
Chapter 11 <i>Law and Ethics</i>	433
Introduction	434
Law and Ethics in Information Security	435
The Legal Environment	435
Types of Law	435
Relevant U.S. Laws	436
International Laws and Legal Bodies	449
State and Local Regulations	450
Policy versus Law	453
Ethical Concepts in Information Security	454
Differences in Ethical Concepts	455
Ethics and Education	459
Deterring Unethical and Illegal Behavior	459

Professional Organizations and Their Codes of Ethics	460
Association of Computing Machinery (ACM)	460
International Information Systems Security Certification Consortium, Inc. (ISC) ²	461
System Administration, Networking, and Security Institute (SANS)	461
Information Systems Audit and Control Association (ISAGA)	462
Information Systems Security Association (ISSA)	463
Organizational Liability and the Need for Counsel	463
Key Law Enforcement Agencies	464
Chapter Summary	466
Review Questions	466
Exercises	
Case Exercises	
Endnotes	
Chapter 12 <i>Information Security Project Management</i>	
Introduction	472
Project Management	474
Applying Project Management to Security	475
PMBoK Knowledge Areas	475
Additional Project Planning Considerations	483
Controlling the Project	486
Conversion Strategies	488
To Outsource or Not	489
Dealing with Change	489
Considerations for Organizational Change	491
Project Management Tools	492
Work Breakdown Structure	493
Task-Sequencing Approaches	497
Automated Project Tools	501
Chapter Summary	502
Review Questions	502
Exercises	
Case Exercises	
Endnotes	\$M
Appendix <i>NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, and ISO 17799:2005 Overview</i>	505
NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems	505
Utilizing the Completed Questionnaire	506
Questionnaire Analysis	506
Questionnaire Cover Sheet	507
The Self-Assessment Guide Questions	508
ISO 17799: 2005 Overview	536
ISO 17799: 2005 Scoring Methodology	536
Glossary	543
Index	555