

INFORMATION SECURITY

MANAGEMENT OF INFORMATION SECURITY

Sixth Edition



Michael E. Whitman
Herbert J. Mattord



Australia • Brazil • Mexico • Singapore • United Kingdom • United States

Brief Contents

PREFACE	XV
CHAPTER 1	
Introduction to the Management of Information Security	1
CHAPTER 2	
Compliance: Law and Ethics	63
CHAPTER 3	
Governance and Strategic Planning for Security	123
CHAPTER 4	
Information Security Policy	169
CHAPTER 5	
Developing the Security Program	219
CHAPTER 6	
Risk Management: Assessing Risk	303
CHAPTER 7	
Risk Management: Treating Risk	365
CHAPTER 8	
Security Management Models	411
CHAPTER 9	
Security Management Practices	457
CHAPTER 10	
Planning for Contingencies	497
CHAPTER 11	
Security Maintenance	567
CHAPTER 12	
Protection Mechanisms	619
GLOSSARY	683
INDEX	709

Table of Contents

PREFACE	XV
---------------	----

CHAPTER 1

Introduction to the Management of Information Security	1
---	----------

Introduction to Security	2
--------------------------------	---

CNSS Security Model	5
---------------------------	---

The Value of Information and the C.I.A. Triad.....	7
--	---

Key Concepts of Information Security: Threats and Attacks	11
--	-----------

The 12 Categories of Threats	13
------------------------------------	----

Management and Leadership	45
--	-----------

Behavioral Types of Leaders.....	46
----------------------------------	----

Management Characteristics	47
----------------------------------	----

Governance	50
------------------	----

Solving Problems	50
------------------------	----

Principles of Information Security Management.....	52
---	-----------

Planning.....	53
---------------	----

Policy.....	54
-------------	----

Programs	55
----------------	----

Protection.....	55
-----------------	----

People.....	55
-------------	----

Projects.....	55
---------------	----

Additional Reading	57
---------------------------------	-----------

Chapter Summary.....	57
-----------------------------	-----------

Review Questions	58
-------------------------------	-----------

Exercises	59
------------------------	-----------

Closing Case.....	60
--------------------------	-----------

Discussion Questions	60
----------------------------	----

Ethical Decision Making	60
-------------------------------	----

Endnotes	61
-----------------------	-----------

CHAPTER 2

Compliance: Law and Ethics	63
---	-----------

Introduction to Law and Ethics	64
--------------------------------------	----

Ethics in InfoSec	66
Ethics and Education	70
Deterring Unethical and Illegal Behavior	72
Professional Organizations and Their Codes of Conduct	74
Association for Computing Machinery (ACM)	74
International Information Systems Security Certification Consortium, Inc. (ISC) ²	75
SANS	75
Information Systems Audit and Control Association (ISACA).....	76
Information Systems Security Association (ISSA).....	77
Information Security and Law.....	78
Types of Law	78
Relevant U.S. Laws	79
International Laws and Legal Bodies	95
State and Local Regulations.....	97
Standards Versus Law.....	101
Policy Versus Law	104
Organizational Liability and the Management of Digital Forensics	104
Key Law Enforcement Agencies	105
Managing Digital Forensics	109
Additional Reading	117
Chapter Summary.....	117
Review Questions	118
Exercises	119
Closing Case.....	120
Discussion Questions	120
Ethical Decision Making.....	120
Endnotes	120
CHAPTER 3	
Governance and Strategic Planning for Security	123
The Role of Planning.....	125
Precursors to Planning.....	127
Strategic Planning.....	129
Creating a Strategic Plan	131
Planning Levels.....	132
Planning and the CISO.....	133
Information Security Governance	135
The ITGI Approach to Information Security Governance	136
NCSP Industry Framework for Information Security Governance	138

CERT Governing for Enterprise Security Implementation.....	140
ISO/IEC 27014:2013 Governance of Information Security.....	143
Security Convergence	145
Planning for Information Security Implementation.....	147
Implementing the Security Program using the SecSDLC.....	154
Additional Reading	163
Chapter Summary.....	164
Review Questions	165
Exercises	165
Closing Case.....	166
Discussion Questions	167
Ethical Decision Making.....	167
Endnotes.....	167

CHAPTER 4

Information Security Policy.....	169
Why Policy?.....	170
Policy, Standards, and Practices	175
Enterprise Information Security Policy.....	177
Integrating an Organization’s Mission and Objectives into the EISP	178
EISP Elements.....	178
Example EISP Elements.....	180
Issue-Specific Security Policy.....	183
Elements of the ISSP.....	185
Implementing the ISSP.....	188
System-Specific Security Policy.....	190
Managerial Guidance SysSPs.....	191
Technical Specification SysSPs.....	192
Guidelines for Effective Policy Development and Implementation	197
Developing Information Security Policy	197
Policy Distribution.....	198
Policy Reading.....	199
Policy Comprehension.....	199
Policy Compliance	200
Policy Enforcement.....	201
Policy Development and Implementation Using the SDLC	201
Software Support for Policy Administration.....	206
Other Approaches to Information Security Policy Development	207
SP 800-18, Rev. 1: Guide for Developing Security Plans for Federal Information Systems.....	209

A Final Note on Policy.....	212
Additional Reading	213
Chapter Summary.....	214
Review Questions	215
Exercises	216
Closing Case.....	217
Discussion Questions	217
Ethical Decision Making.....	217
Endnotes	218
CHAPTER 5	
Developing the Security Program.....	219
Organizing for Security	220
Security in Large Organizations	225
Security in Medium-Sized Organizations	228
Security in Small Organizations.....	229
Placing Information Security Within an Organization	230
Components of the Security Program.....	241
Staffing the Security Function.....	244
Information Security Professional Credentials	254
Entering the Information Security Profession	265
Implementing Security Education, Training, and Awareness (SETA) Programs.....	267
Security Education.....	269
Security Training	271
Security Awareness	278
Project Management in Information Security	286
Projects Versus Processes	286
Organizational Support for Project Management	288
PMBOK Knowledge Areas	289
Project Management Tools	292
Additional Reading	296
Chapter Summary.....	297
Review Questions	298
Exercises	299
Closing Case.....	299
Discussion Questions	299
Ethical Decision Making.....	300
Endnotes	300

CHAPTER 6**Risk Management: Assessing Risk 303****Introduction to the Management of Risk
in Information Security 304**

Knowing Yourself and Knowing the Enemy 305

The Information Security Risk Management Framework 305

Roles of Communities of Interest in Managing Risk 308

Executive Governance and Support 308

Framework Design 312

Framework Implementation 315

Framework Monitoring and Review 315

Continuous Improvement 316

The Risk Management Process 316

RM Process Preparation—Establishing the Context 317

Risk Assessment: Risk Identification 319

Risk Assessment: Risk Analysis 343

Risk Evaluation 355

Risk Treatment/Risk Control 359

Process Communications, Monitoring, and Review 359

Additional Reading 359**Chapter Summary 360****Review Questions 361****Exercises 361****Closing Case 362**

Discussion Questions 362

Ethical Decision Making 362

Endnotes 363**CHAPTER 7****Risk Management: Treating Risk 365****Introduction to Risk Treatment 366**

Risk Treatment Strategies 368

Managing Risk 374

Feasibility and Cost-benefit Analysis 379

Other Methods of Establishing Feasibility 387

Alternatives to Feasibility Analysis 389

Recommended Alternative Risk Treatment Practices 392

Alternative Risk Management Methodologies 393

The OCTAVE Methods 393

Microsoft Risk Management Approach 394

FAIR	395
ISO Standards for InfoSec Risk Management	397
NIST Risk Management Framework (RMF)	399
Other Methods	403
Selecting the Best Risk Management Model	404
Additional Reading	405
Chapter Summary.....	405
Review Questions	406
Exercises	407
Closing Case.....	408
Discussion Questions	409
Ethical Decision Making.....	409
Endnotes	409
CHAPTER 8	
Security Management Models.....	411
Introduction to Blueprints, Frameworks, and Security Models	412
Security Management Models	414
The ISO 27000 Series	414
NIST Security Publications	420
Control Objectives for Information and Related Technology	428
Committee of Sponsoring Organizations	430
Information Technology Infrastructure Library.....	431
Information Security Governance Framework	431
Security Architecture Models	434
TCSEC and the Trusted Computing Base.....	434
Information Technology System Evaluation Criteria	437
The Common Criteria	437
Access Control Models	438
Categories of Access Controls.....	440
Other Forms of Access Control.....	446
Academic Access Control Models	447
Bell-LaPadula Confidentiality Model	447
Biba Integrity Model.....	448
Clark-Wilson Integrity Model.....	449
Graham-Denning Access Control Model.....	450
Harrison-Ruzzo-Ullman Model	450
Brewer-Nash Model (Chinese Wall)	450

Additional Reading	451
Chapter Summary.....	451
Review Questions	452
Exercises	453
Closing Case.....	453
Discussion Questions	453
Ethical Decision Making.....	454
Endnotes	454
CHAPTER 9	
Security Management Practices	457
Introduction to Security Practices	458
Security Employment Practices	459
Hiring	459
Contracts and Employment.....	462
Security Expectations in the Performance Evaluation	462
Termination Issues	463
Personnel Security Practices.....	464
Security of Personnel and Personal Data	466
Security Considerations for Temporary Employees, Consultants, and Other Workers	466
Information Security Performance Measurement.....	468
InfoSec Performance Management.....	469
Building the Performance Measurement Program	471
Specifying InfoSec Measurements	473
Collecting InfoSec Measurements	473
Implementing InfoSec Performance Measurement.....	478
Reporting InfoSec Performance Measurements	479
Benchmarking	481
Standards of Due Care/Due Diligence	482
Recommended Security Practices	483
Selecting Recommended Practices	484
Limitations to Benchmarking and Recommended Practices.....	485
Baselining	486
Support for Benchmarks and Baselines	487
ISO Certification.....	489
Additional Reading	490
Chapter Summary.....	491
Review Questions	492

Exercises	493
Closing Case.....	493
Discussion Questions	493
Ethical Decision Making.....	493
Endnotes	494
CHAPTER 10	
Planning for Contingencies.....	497
Introduction to Contingency Planning.....	498
Fundamentals of Contingency Planning.....	500
Components of Contingency Planning	504
Business Impact Analysis.....	506
Contingency Planning Policies	513
Incident Response	513
Getting Started	514
Incident Response Policy.....	516
Incident Response Planning.....	517
Detecting Incidents.....	522
Reacting to Incidents	526
Recovering from Incidents	530
Disaster Recovery	538
The Disaster Recovery Process	540
Disaster Recovery Policy.....	541
Disaster Classification.....	542
Planning to Recover.....	545
Responding to the Disaster.....	546
Simple Disaster Recovery Plan	546
Business Continuity.....	549
Business Continuity Policy.....	550
Continuity Strategies	552
Timing and Sequence of CP Elements	554
Crisis Management.....	556
Business Resumption.....	558
Testing Contingency Plans.....	558
Final Thoughts on CP.....	560
Additional Reading	560
Chapter Summary.....	561
Review Questions	562

Exercises	563
Closing Case.....	563
Discussion Questions	564
Ethical Decision Making.....	564
Endnotes	564

CHAPTER 11

Security Maintenance	567
Introduction to Security Maintenance.....	568
Security Management Maintenance Models.....	569
NIST SP 800-100, Information Security Handbook: A Guide for Managers.....	569
The Security Maintenance Model	587
Additional Reading	614
Chapter Summary.....	614
Review Questions	615
Exercises	616
Closing Case.....	616
Discussion Questions	617
Ethical Decision Making.....	617
Endnotes	617

CHAPTER 12

Protection Mechanisms	619
Introduction to Protection Mechanisms.....	620
Access Controls and Biometrics	622
Managing Network Security.....	630
Firewalls.....	631
Intrusion Detection and Prevention Systems	643
Wireless Networking Protection.....	647
Scanning and Analysis Tools.....	651
Managing Server-Based Systems with Logging.....	655
Managing Security for Emerging Technologies	660
Cryptography.....	662
Encryption Operations	664
Using Cryptographic Controls	671
Managing Cryptographic Controls	674

Additional Reading	677
Chapter Summary.....	677
Review Questions	679
Exercises	679
Closing Case.....	680
Discussion Questions	681
Ethical Decision Making.....	681
Endnotes	681
GLOSSARY	683
INDEX.....	709