

Principles of Information Security

Sixth Edition

Michael E. Whitman, *Ph.D., CISM, CISSP*

Herbert J. Mattord, *Ph.D., CISM, CISSP*

Kennesaw State University



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

Brief Table of Contents

PREFACE	ix
CHAPTER 1 Introduction to Information Security	1
CHAPTER 2 The Need for Security	49
CHAPTER 3 Legal, Ethical, and Professional Issues in Information Security.	123
CHAPTER 4 Planning for Security	171
CHAPTER 5 Risk Management	253
CHAPTER 6 Security Technology: Access Controls, Firewalls, and VPNs	325
CHAPTER 7 Security Technology: Intrusion Detection and Prevention Systems, and Other Security Tools	385
CHAPTER 8 Cryptography	449
CHAPTER 9 Physical Security.	501
CHAPTER 10 Implementing Information Security	537
CHAPTER 11 Security and Personnel.	579
CHAPTER 12 Information Security Maintenance	627
GLOSSARY	693
INDEX	711

Table of Contents

PREFACE	ix
CHAPTER 1	
Introduction to Information Security	1
Introduction	3
The History of Information Security	3
What Is Security?	10
CNSS Security Model	18
Components of an Information System	20
Balancing Information Security and Access	23
Approaches to Information Security Implementation	24
Security in the Systems Development Life Cycle	25
Security Professionals and the Organization	38
Communities of Interest	40
Information Security: Is It an Art or a Science?	41
Selected Readings	43
Chapter Summary	43
Review Questions	44
Exercises	45
Case Exercises	45
Endnotes	46
CHAPTER 2	
The Need for Security	49
Introduction	51
Threats and Attacks	53
Compromises to Intellectual Property	60
Deviations in Quality of Service	64
Espionage or Trespass	66
Forces of Nature	77
Human Error or Failure	80
Information Extortion	86
Sabotage or Vandalism	87
Software Attacks	90
Technical Hardware Failures or Errors	103
Technical Software Failures or Errors	105
Technological Obsolescence	112
Theft	114
Selected Readings	114
Chapter Summary	114
Review Questions	116
Exercises	117
Case Exercises	117
Endnotes	118

CHAPTER 3

Legal, Ethical, and Professional Issues in Information Security	123
Introduction	124
Law and Ethics in Information Security	125
Relevant U.S. Laws	127
International Laws and Legal Bodies	143
Ethics and Information Security	146
Codes of Ethics of Professional Organizations	153
Key U.S. Federal Agencies	155
Selected Readings	164
Chapter Summary	164
Review Questions	165
Exercises	166
Case Exercises	166
Endnotes	166

CHAPTER 4

Planning for Security	171
Introduction	172
Information Security Planning and Governance	172
Information Security Policy, Standards, and Practices	177
The Information Security Blueprint	194
Security Education, Training, and Awareness Program	211
Continuity Strategies	214
Selected Readings	245
Chapter Summary	245
Review Questions	246
Exercises	247
Case Exercises	248
Endnotes	249

CHAPTER 5

Risk Management	253
Introduction	254
An Overview of Risk Management	255
Risk Identification	260
Risk Assessment	282
Risk Control	295
Quantitative Versus Qualitative Risk Management Practices	306
Recommended Risk Control Practices	314
Selected Readings	318
Chapter Summary	318
Review Questions	319
Exercises	320
Case Exercises	321
Endnotes	322

CHAPTER 6

Security Technology: Access Controls, Firewalls, and VPNs	325
Introduction	326
Access Control	326
Firewalls	343
Protecting Remote Connections	371
Selected Readings	379
Chapter Summary	380
Review Questions	381
Exercises	382
Case Exercises	382
Endnotes	383

CHAPTER 7

Security Technology: Intrusion Detection and Prevention Systems, and Other Security Tools	385
Introduction	387
Intrusion Detection and Prevention Systems	387
Honeypots, Honeynets, and Padded Cell Systems	424
Scanning and Analysis Tools	428
Selected Readings	443
Chapter Summary	443
Review Questions	444
Exercises	445
Case Exercises	445
Endnotes	446

CHAPTER 8

Cryptography	449
Introduction	450
Foundations of Cryptology	451
Cipher Methods	455
Cryptographic Algorithms	467
Cryptographic Tools	475
Protocols for Secure Communications	483
Selected Readings	494
Chapter Summary	494
Review Questions	495
Exercises	496
Case Exercises	497
Endnotes	498

CHAPTER 9

Physical Security	501
Introduction	503
Physical Access Controls	504
Fire Security and Safety	514
Failure of Supporting Utilities and Structural Collapse	519
Interception of Data	526
Securing Mobile and Portable Systems	527
Special Considerations for Physical Security	531

Selected Readings	531
Chapter Summary	531
Review Questions	533
Exercises	534
Case Exercises	535
Endnotes	535
CHAPTER 10	
Implementing Information Security	537
Introduction	539
Information Security Project Management	539
Technical Aspects of Implementation	550
Nontechnical Aspects of Implementation	557
Information Systems Security Certification and Accreditation	559
Selected Readings	573
Chapter Summary	573
Review Questions	575
Exercises	576
Case Exercises	576
Endnotes	577
CHAPTER 11	
Security and Personnel	579
Introduction	580
Positioning and Staffing the Security Function	581
Credentials for Information Security Professionals	594
Employment Policies and Practices	608
Security Considerations for Temporary Employees, Consultants, and Other Workers	614
Selected Readings	619
Chapter Summary	619
Review Questions	620
Exercises	622
Case Exercises	622
Endnotes	623
CHAPTER 12	
Information Security Maintenance	627
Introduction	628
Security Management Maintenance Models	629
Digital Forensics	677
Selected Readings	686
Chapter Summary	687
Review Questions	688
Exercises	689
Case Exercises	689
Endnotes	691
GLOSSARY	693
INDEX	711