THOMSON
COURSE TECHNOLOGY

MANAGEMENT OF INFORMATION SECURITY

MICHAEL E. WHITMAN AND HERBERT J. MATTORD

PREPARING TOMORROW'S
INFORMATION
SECURITY
PROFESSIONALS

Table of Contents

Preface xv

Section I–Introduction

Chapter 1

Introduction to the Management of Information Security 1

Introduction 2

What Is Security? 3

NSTISSC Security Model. 5

Key Concepts of Information Security 6

What is Management? 10

The Difference Between Leadership and Management. 11

Characteristics of a Leader. 11

Characteristics of Management. 12

Solving Problems 16

Principles of Information Security Management 19

Chapter Summary 21

Review Questions 22

Exercises 23

Case Exercises 23

Section II–Planning

Chapter 2

Planning for Security 25

Introduction 26

Components of Organizational Planning 28

Mission. 28

Vision 29

Values 30

Strategy. 31

Planning and the CISO 34

Planning for Information Security Implementation 37

Introduction to the Systems Development Life Cycle. 39

The Security Systems Development Life Cycle (SecSDLC) 42

Comparing the SDLC and the SecSDLC. 56

Chapter Summary .59
Review Questions .60
Exercises .61
Case Exercises .61

Chapter 3

Planning for Contingencies 63
Introduction .64
What Is Contingency Planning? .65
Components of Contingency Planning .67
Incident Response Plan 67
Disaster Recovery 76
Business Continuity Planning 82
Timing and Sequence of CP Elements 84
Putting a Contingency Plan Together .86
Business Impact Analysis 87
Combining the DRP and the BCP 90
Testing Contingency Plans .95
Desk Check 95
Structured Walk-Through 95
Simulation 95
Parallel Testing 96
Full Interruption 96
A Single Continuity Plan .98
Chapter Summary .99
Review Questions .101
Exercises .101
Case Exercises .102

Section III–Policy and Programs

Chapter 4

Information Security Policy 105
Introduction .106
Why Policy? .107
Policy, Standards, and Practices 108
Enterprise Information Security Policy .110
Integrating an Organization's Mission and Objectives into the EISP 110
EISP Elements 110
Example EISP 112
Issue-Specific Security Policy .116
Components of the ISSP 117
Implementing the ISSP 119

System-Specific Policy 121
Management Guidance SysSPs 121
Technical Specifications SysSPs.......................................122
Combination SysSPs 126
Guidelines for Policy Development 126
The Policy Project 127
Automated Tools 131
The *Information Securities Policy Made Easy* Approach 132
SP 800-18: *Guide for Developing Security Plans for Information Technology Systems Policy Management*.......................................147
A Final Note on Policy.......................................148
Chapter Summary 151
Review Questions 152
Exercises 152
Case Exercises 153

Chapter 5

Developing the Security Program.......................................155
Introduction 156
Organizing for Security 156
Security in Large Organizations 160
Security in Medium-Sized Organizations.......................................163
Security in Small Organizations 163
Placing Information Security Within An Organization.......................................166
Option 1: Information Technology.......................................168
Option 2: Security 169
Option 3: Administrative Services.......................................171
Option 4: Insurance and Risk Management.......................................172
Option 5: Strategy and Planning.......................................173
Option 6: Legal 175
Option 7: Internal Audit 176
Option 8: Help Desk 177
Option 9: Accounting and Finance Through IT.......................................178
Option 10: Human Resources.......................................179
Option 11: Facilities Management 179
Option 12: Operations.......................................179
Summary of Reporting Relationships.......................................179
Components of the Security Program 180
Information Security Roles and Titles 181
Chief Information Security Officer.......................................182
Security Managers 182
Security Administrators and Analysts.......................................183
Security Technicians 183
Security Staffers 184

Security Consultants 184
Security Officers and Investigators 184
Help Desk Personnel 184
Implementing Security Education, Training, and Awareness Programs 184
Security Education. 186
Security Training 189
Training Techniques. 191
Security Awareness. 195
Chapter Summary 204
Review Questions 205
Exercises 206
Case Exercises 206

Chapter 6
Security Management Models and Practices. 209

Introduction 210
Security Management Models 211
BS 7799 Part 1 (ISO 17799:2002 Standard): Code of Practice for Information Security Management. 211
BS 7799 Part 2: The Information Security Management System 214
The Security Management Index and ISO 17799 216
RFC 2196 Site Security Handbook 217
NIST Security Models 218
A Hybrid Security Management Model 229
Security Management Practices 231
Standards of Due Care/Due Diligence 231
Best Security Practices 231
The Gold Standard. 235
Selecting Best Practices 235
Benchmarking and Best Practices Limitations 236
Baselining. 237
Emerging Trends in Certification and Accreditation 239
SP 800-37: Guidelines for the Security Certification and Accreditation of Federal IT Systems 239
SP 800-53: Minimum Security Controls for Federal IT Systems 241
Chapter Summary 244
Review Questions 245
Exercises 246
Case Exercises 246

Appendix A

Appendix: NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, and the Human Firewall Council's Security Management Index Survey 249
NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems 250
Utilizing the Completed Questionnaire 250
Questionnaire Analysis 251
Questionnaire Cover Sheet 251
The Self-Assessment Guide Questions 252
Human Firewall Council's Security Management Index Survey 278
Security Management Index Scoring Methodology 278
Questionnaire. 279
I. Security Policy. 279
II. Organizational Security 279
III. Asset Classification & Control 280
IV. Personnel Security. 280
V. Physical and Environmental Security. 281
VI. Communications & Operations Management. 281
VII. Access Control. 282
VIII. Systems Development and Maintenance 283
IX. Business Continuity Management 284
X. Compliance. 284

Section IV–Protection

Chapter 7

Risk Management: Identifying and Assessing Risk 285
Introduction 286
Risk Management 287
Knowing Ourselves 287
Knowing the Enemy. 287
Accountability for Risk Management 288
Risk Identification 290
Creating an Inventory of Information Assets 290
Classifying and Categorizing Assets 294
Assessing Values for Information Assets 295
Listing Assets in Order of Importance 297
Data Classification Model 297
Security Clearances 299
Management of the Classified Information Asset. 299
Threat Identification 301

Risk Assessment 308
Introduction to Risk Assessment.... 308
Likelihood 309
Assessing Potential Loss.... 309
Percentage of Risk Mitigated by Current Controls.... 310
Uncertainty 310
Risk Determination 310
Identify Possible Controls 310
Access Controls 311
Documenting the Results of Risk Assessment 312
Chapter Summary 314
Review Questions 315
Exercises 316
Case Exercises 317

Chapter 8

Risk Management: Assessing and Controlling Risk 319
Introduction 320
Risk Control Strategies 321
Avoidance.... 321
Transference.... 324
Mitigation 324
Acceptance 325
Risk Control Strategy Selection 326
Evaluation, Assessment, and Maintenance of Risk Controls 327
Categories of Controls 328
Control Function.... 328
Architectural Layer.... 329
Strategy Layer.... 329
Information Security Principle 329
Feasibility Studies and Cost-Benefit Analysis 331
Cost-Benefit Analysis.... 332
Other Feasibility Studies 337
Alternatives to Feasability 339
Risk Management Discussion Points 340
Risk Appetite 340
Residual Risk 340
Documenting Results.... 341
Recommended Risk Control Practices 343
Qualitative Measures 344
Delphi Technique.... 344
A Single-Source Approach to Risk Management 344

The OCTAVE Method .345
Important Aspects of the OCTAVE Method 345
Phases, Processes, and Activities 347
Preparing for the OCTAVE Method 347
Phase 1: Build Asset-Based Threat Profiles 349
Phase 2: Identify Infrastructure Vulnerabilities. 352
Phase 3: Develop Security Strategy and Plans. 354
Chapter Summary .356
Review Questions .357
Exercises .358
Case Exercises .359

Chapter 9
Protection Mechanisms 361
Introduction .362
Access Controls .364
Authentication 364
Authorization 371
Evaluating Biometrics 372
Acceptability of Biometrics 372
Managing Access Controls 373
Firewalls .375
The Development of Firewalls 375
Firewall Architectures 378
Selecting the Right Firewall 381
Managing Firewalls 381
Dial-Up Protection .385
RADIUS and TACACS 385
Managing Dial-Up Connections 386
Intrusion Detection Systems .387
Host-Based IDS 388
Network-Based IDS 389
Signature-Based IDS 389
Statistical Anomaly-Based IDS 389
Managing Intrusion Detection Systems 390
Scanning and Analysis Tools 390
Port Scanners 391
Vulnerability Scanners 392
Packet Sniffers 393
Content Filters 393
Trap and Trace 393
Managing Scanning and Analysis Tools 394

Cryptography 395
Encryption Definitions 395
Encryption Operations 396
Using Cryptographic Controls 403
Managing Cryptographic Controls 406
Chapter Summary 409
Review Questions 410
Exercises 410
Case Exercises 411

Section V–People and Projects

Chapter 10

Personnel and Security 413
Introduction 414
Staffing the Security Function 415
Qualifications and Requirements 415
Entering the Information Security Profession 416
Information Security Positions 417
Information Security Professional Credentials 427
Certified Information Systems Security Professional (CISSP) and Systems Security Certified Practitioner (SSCP) 427
Global Information Assurance Certification (GIAC) 428
Security Certified Program (SCP) 429
TruSecure ICSA Certified Security Associate (TICSA) 430
Security+ 431
Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) 432
Certified Information Forensics Investigator (CIFI) 433
Certification Costs 433
Employment Policies and Practices 436
Hiring 436
Contracts and Employment 438
Security as Part of Performance Evaluation 438
Termination Issues 438
Personnel Security Practices 440
Security of Personnel and Personal Data 441
Security Considerations for Nonemployees 441
Chapter Summary 447
Review Questions 448
Exercises 449
Case Exercises 449

Chapter 11

Law and Ethics 451
Introduction 452
Law and Ethics in Information Security 453
The Legal Environment 453
Types of Law 453
Relevant U.S. Laws 453
International Laws and Legal Bodies 464
State and Local Regulations 465
Policy versus Law 468
Ethical Concepts in Information Security 469
Differences in Ethical Concepts 470
Ethics and Education 473
Deterring Unethical and Illegal Behavior 473
Certifications and Professional Organizations 476
Association of Computing Machinery (ACM) 476
International Information Systems Security Certification Consortium, Inc. (ISC)² 477
System Administration, Networking, and Security Institute (SANS). 477
Information Systems Audit and Control Association (ISACA) 478
Computer Security Institute (CSI) 478
Information Systems Security Association 478
Other Security Organizations 478
Key U.S. Federal Agencies 480
Organizational Liability and the Need for Counsel 482
Chapter Summary 483
Review Questions 483
Exercises 484
Case Exercises 484

Chapter 12

Information Security Project Management 487
Introduction 488
Project Management 490
Applying Project Management to Security 491
PMBoK Knowledge Areas 491
Additional Project Planning Considerations. 499
Controlling the Project 502
Conversion Strategies. 504
To Outsource or Not 504
Dealing With Change. 505
Considerations for Organizational Change. 507

Project Management Tools 509
Work Breakdown Structure. 510
Task-Sequencing Approaches 514
Automated Project Tools 518
Chapter Summary 519
Review Questions 519
Exercises 520
Case Exercises 521
Glossary 523
Index. 535