

Principles of INFORMATION SYSTEMS SECURITY

Text
and
Cases

Gurpreet Dhillon

CONTENTS

PREFACE v

CHAPTER 1 INFORMATION SYSTEMS SECURITY: NATURE AND SCOPE 1

| | |
|---|----|
| Coordination in Threes | 3 |
| Security in Threes | 5 |
| Technical Controls | 6 |
| Formal Controls | 7 |
| Informal Controls | 7 |
| Institutionalizing Security in Organizations | 8 |
| Questions and Exercises | 10 |
| Case Study | 11 |

PART I

TECHNICAL ASPECTS OF INFORMATION SYSTEMS SECURITY

CHAPTER 2 SECURITY OF TECHNICAL SYSTEMS IN ORGANIZATIONS: AN INTRODUCTION 15

| | |
|--------------------------------|----|
| Vulnerabilities | 17 |
| Data Security Requirements | 19 |
| Methods of Defense | 23 |
| Encryption | 23 |
| Software Controls | 24 |
| Physical and Hardware Controls | 25 |
| Concluding Remarks | 25 |
| Questions and Exercises | 26 |
| Case Study | 26 |

CHAPTER 3 MODELS FOR TECHNICAL SPECIFICATION OF INFORMATION SYSTEMS SECURITY 28

| | |
|---------------------------------------|----|
| Models for Security Specification | 30 |
| Evaluation Criteria and Their Context | 31 |
| Bell La Padula | 31 |
| Denning Information Flow Model | 33 |

| | |
|--|----|
| The Reference Monitor and Rushby's Solution | 34 |
| Away from the Military | 35 |
| Military and Nonmilitary: Toward Integrity | 36 |
| Toward Integrity: Biba, Clark-Wilson, and Chinese Walls | 36 |
| Biba | 36 |
| The Clark-Wilson Model | 37 |
| Emergent Issues | 40 |
| Questions and Exercises | 42 |
| Case Study | 43 |

CHAPTER 4 CRYPTOGRAPHY AND TECHNICAL INFORMATION SYSTEMS SECURITY 44

| | |
|------------------------------------|----|
| Cryptography | 46 |
| Cryptanalysis | 48 |
| Basics of Cryptanalysis | 49 |
| Using Digrams for Cryptanalysis | 53 |
| Conventional Encryption Algorithms | 53 |
| Data Encryption Standard | 55 |
| IDEA | 57 |
| CAST | 57 |
| AES | 57 |
| Asymmetric Encryption | 57 |
| Authentication of the Sender | 59 |
| RSA | 60 |
| Questions and Exercises | 61 |
| Case Study | 62 |

CHAPTER 5 NETWORK SECURITY 64

| | |
|--|----|
| TCP/IP Protocol Architecture | 65 |
| LAN Security | 68 |
| Security and TCP/IP Protocol Architecture | 70 |
| Operating-System-based Attacks | 71 |
| Network-based Attacks | 75 |
| Securing Systems | 80 |
| Securing the File System | 80 |
| Securing Access from the Network | 89 |
| Questions and Exercises | 91 |
| Case Study | 92 |

PART II

FORMAL ASPECTS OF INFORMATION SYSTEMS SECURITY

CHAPTER 6 SECURITY OF FORMAL SYSTEMS IN ORGANIZATIONS: AN INTRODUCTION 97

- Formal IS Security Dimensions 100
 - Responsibility and Authority Structures 100
 - Organizational Buy-In 103
 - Security Policy 105
- Concluding Remarks 106
- Questions and Exercises 108
- Case Study 108

CHAPTER 7 PLANNING FOR INFORMATION SYSTEMS SECURITY 110

- Security Strategy Levels 112
- Classes of Security Decisions in Firms 114
 - Strategic Decisions 114
 - Administrative Decisions 117
 - Operational Decisions 119
 - Prioritizing Decisions 120
- Security Planning Process 121
 - Orion Strategy Process Overview 122
- IS Security Planning Principles 125
- Summary 128
- Questions and Exercises 129
- Case Study 129

CHAPTER 8 DESIGNING INFORMATION SYSTEMS SECURITY 131

- Security Breaches in Systems
 - Development 133
- Control Structures 133
 - Auditing 133
 - Application Controls 134
 - Modeling Controls 135
 - Documentation Controls 137
- Process Improvement Software 137
- The SSE-CMM 138
- Key Constructs and Concepts in SSE-CMM 142
 - Organization and Projects 142
 - System 143
 - Work Product 143
 - Customer 143

- Process 143
- Process Area 144
- Role Independence 144
- Process Capability 144
- Institutionalization 144
- Process Management 145
- Capability Maturity Model 146
- SSE-CMM Architecture Description 146
 - Basic Model 146
- Concluding Remarks 151
- Questions and Exercises 152
- Case Study 153

CHAPTER 9 RISK MANAGEMENT FOR INFORMATION SYSTEMS SECURITY 155

- Risk Assessment 158
 - System Characterization 158
 - Threat Identification 159
 - Vulnerability Identification 161
 - Control Analysis 162
 - Likelihood Determination and Impact Analysis 163
 - Risk Determination 164
 - Control Recommendations and Results Documentation 165
- Risk Mitigation 166
 - Control Categories 167
- Risk Evaluation and Assessment 169
- COBRA: Hybrid Model for Software Cost Estimation, Benchmarking, and Risk Assessment 170
- The I2S2 Model 172
 - Three Levels of I2S2 Model 172
 - Six Components of I2S2 Model 174
- Concluding Remarks 178
- Questions and Exercises 179
- Case Study 180

PART III

INFORMAL ASPECTS OF INFORMATION SYSTEMS SECURITY

CHAPTER 10 SECURITY OF INFORMAL SYSTEMS IN ORGANIZATIONS: AN INTRODUCTION 185

- The Concept of Pragmatics and IS Security 187
 - What Is Pragmatics? 187



nature of IS Security at the Pragmatic
Level **189**

Informal Behavior **194**

Concluding Remarks **195**

Questions and Exercises **196**

Case Study **196**

CHAPTER 11 *CORPORATE GOVERNANCE FOR IS SECURITY* **198**

What Is Corporate Governance? **200**

Models of Corporate Governance:

Civic Republicanism **201**

An Opposing View: Liberalism **202**

Enter the Corporation **202**

The Science of Management:

Enter the Professional Manager **202**

Professional Managers as

Trustees of Society **203**

The New Power Elite: The Managerial

Technocracy **204**

Minding the Minders: Contractual

Shareholder Model **204**

Analysis of the Structure

of American Corporations **204**

Owners **204**

Board of Directors **205**

CEO and Executives **205**

Corporate Governance for IS Security **206**

Security Governance Principles **208**

Constructing Information System

Security Governance **213**

Concluding Remarks **215**

Questions and Exercises **217**

Case Study **217**

CHAPTER 12 *CULTURE AND INFORMATION SYSTEMS SECURITY* **219**

Security Culture **221**

Silent Messages and IS Security **224**

Security Culture Framework **229**

OECD Principles for Security Culture **233**

Concluding Remarks **235**

Questions and Exercises **236**

Case Study **237**

PART IV

REGULATORY ASPECTS OF INFORMATION SYSTEMS SECURITY

CHAPTER 13 *INFORMATION SYSTEMS SECURITY STANDARDS* **241**

ISO 17799 **241**

ISO 17799 Framework **242**

The Rainbow Series **247**

ITSEC **249**

International Harmonization **251**

Common Criteria **252**

Common Problems with CC **254**

Other Miscellaneous Standards

and Guidelines **257**

RFC 2196 Site Security Handbook **257**

ISO/IEC TR 13335 Guidelines

for the Management of IT Security **258**

Generally Accepted Information

Security Principles (GAISP) **259**

OECD Guidelines for the Security

of Information Systems **259**

Concluding Remarks **260**

Questions and Exercises **262**

Case Study **263**

CHAPTER 14 *LEGAL ASPECTS OF INFORMATION SYSTEMS SECURITY* **264**

Computer Fraud and Abuse Act (CFAA) **266**

Computer Security Act (CSA) **268**

Health Insurance Portability

and Accountability Act (HIPAA) **269**

Requirements **269**

Compliance and Recommended Protection **270**

HIPAA: Help or Hindrance? **272**

USA Patriot Act **274**

IT and the Act **275**

Sarbanes-Oxley Act (SOX) **277**

IT-Specific Issues **279**

Federal Information Security

Management Act (FISMA) **279**

Concluding Remarks **281**

Questions and Exercises **282**

Case Study **282**

CHAPTER 15 COMPUTER FORENSICS 283

| | |
|--|-----|
| The Basics | 284 |
| Types and Scope of Crimes | 285 |
| Lack of Uniform Law | 286 |
| What Is Computer Forensics? | 287 |
| Gathering Forensic Evidence | 288 |
| Formal Procedure for Gathering Data | 290 |
| Law Dictating Formal Procedure | 293 |
| Laws Governing Seizure of Evidence | 294 |
| Law Governing Analysis and Presentation of Evidence | 306 |
| Emergent Issues | 309 |
| International Arena | 309 |
| National Arena | 311 |
| Concluding Remarks | 312 |
| Questions and Exercises | 313 |
| Case Study 1 | 314 |
| Case Study 2 | 314 |

**CHAPTER 16 SUMMARY PRINCIPLES FOR
INFORMATION SYSTEMS SECURITY 316**

| | |
|--|-----|
| Principles for Technical Aspects of IS Security | 317 |
| Principles for Formal Aspects of IS Security | 319 |

| | |
|---|-----|
| Principles for Informal Aspects of IS Security | 321 |
| Concluding Remarks | 322 |

CASES

| | |
|---|-----|
| 1. Case of a Computer Hack | 325 |
| 2. Botnet: Anatomy of a Case | 335 |
| 3. Cases in Computer Crime | 349 |
| 4. IS Security at Southam Council | 356 |
| 5. Security Management at the Tower | 369 |
| 6. Computer Crime and the Demise of Barings Bank | 375 |
| 7. Technology-Enabled Fraud and the Demise of Drexel Burnham Lambert | 392 |
| 8. It Won't Part Your Hair: The INSLAW Affair | 401 |
| 9. Taylor City Police Department Security Breach | 426 |
| 10. Developing a Security Policy at M&M Procurement, Inc. | 431 |

INDEX 441



Health Information Technology Department
Mashhad University of Medical Sciences