TABLE OF CONTENTS

PREFACE

CONTRIBUTORS

Chapter 1. **INFORMATION ASSET PROTECTION** 1

1.1 Introduction 1
1.2 History of Espionage and Business Intelligence Collection 2
1.3 Risk Management Approach to IAP 4
1.3.1 Today's Global Information Environment 4
1.3.2 Threat Categories and Examples 5
1.3.3 Risk Assessment and Due Diligence 9
1.3.4 Attaining Buy-In 9
1.4 Approaches to Risk Mitigation 11
1.4.1 Basic Protection Practices 11
1.4.2 Physical Security 12
1.4.3 Personnel Security 15
1.4.4 Privacy Protection 15
1.4.5 Business Practices 16
1.4.6 Operations Security or Information Risk Management 17
1.4.7 Travel and Meeting Security 18
1.4.8 Preventing and Detecting Counterfeiting and Illegal Copying 20
1.5 Legal Protections 21
1.5.1 Copyrights 22
1.5.2 Trademarks, Trade Dress, and Service Marks 23
1.5.3 Patents 23
1.5.4 Trade Secrets 24
1.5.5 International Concerns 24
1.5.6 Nondisclosure Agreements and Contracts 25
1.6 Technical Protective Measures 26
1.6.1 Technical Surveillance Countermeasures 26
1.6.2 Protection in an IT Environment 26
1.6.3 Protection in Special Environments 28
1.7 Response and Recovery After an Information Loss 29
1.8 Summary 30
Appendix A: Sample Policy on Information Asset Protection 31
Appendix B: Quick Reference Guide for Information Asset Protection 39
Appendix C: Sample Nondisclosure Agreements 43
Appendix D: Technical Reports and Laboratory Notebooks 49
Appendix E: Information Disposal and Destruction 55
References 57

Chapter 2. **THE INCREASING IMPORTANCE OF INFORMATION SYSTEMS SECURITY** 61

2.1 The Human Challenge: Failure of Imagination 62
2.2 State of Information Systems Security 64
2.3 Economics of Information Systems Security 68
2.4 Critical Success Factors 69
2.5 Implications to Physical Security in a Converged World 71
2.6 The Cybercrime Challenge: A National Challenge 78
References 81

Chapter 3. **THE INFORMATION SYSTEMS SECURITY BODY OF KNOWLEDGE**. 85

3.1 The Elements of ISS Risk 86
3.1.1 ISS Terms 86
3.1.2 Fundamental Equation of ISS. 87
3.1.3 Information System Threats 87
3.1.4 Information System Vulnerabilities 89
3.1.5 Information System Control Objectives 90
3.1.6 Information System Countermeasures 90
3.2 Down the Rabbit Hole: Computer Logic, System Complexity, and Inherent Vulnerability. 93
3.2.1 How Computer Systems Work 94
3.2.2 Managing the IT Infrastructure 106
3.2.3 Real World, Networked Computer Systems 107
3.2.4 Additional Information Security Concepts 115
3.2.5 Information Security Technologies 116
3.3 ISS Practitioner Frameworks 118
3.3.1 ISO/IEC 27001:2005 and ISO/IEC 27002:2005 118
3.3.2 CISSP Common Body of Knowledge 120
3.3.3 Information Security Governance: Guidance for Boards of Directors and Executive Management 121
3.3.4 Generally Accepted Information System Security Practices (GAISSP) 122
3.4 The Emerging Legal, Regulatory and Contractual Landscape Regarding ISS 123
3.4.1 Payment Card Industry Data Security Standard (PCI DSS) 123
3.4.2 Health Care and Insurance Portability and Accountability Act (HIPAA) 125
3.4.3 Gramm-Leach-Bliley Act (GLBA) 126
3.4.4 Children's Online Privacy Protection Act (COPPA). 127
3.4.5 Sarbanes-Oxley Act (SOX) 128
3.4.6 Red Flag Rules 129
3.4.7 FTC Enforcement Actions 130

3.4.8 State Breach Disclosure and Related ISS and Privacy Laws . . . 134
3.4.9 European Union Data Protection Directive . . . 135
3.4.10 Emerging Case Law . . . 136
3.5 Special Topics in ISS . . . 139
3.5.1 ISS Risk and Vulnerability Assessment . . . 139
3.5.2 ISS Policy Implementation . . . 141
3.5.3 Incident Response . . . 142
3.6 Total ISS Management . . . 144
3.6.1 ISO 27001 Information Security Management Systems . . . 144
3.6.2 Making Continual Improvement Happen . . . 146
Appendix A: Information Systems Security Resources . . . 149
References 155

Chapter 4. **SECURITY CHALLENGES OF CONVERGENCE** . . . 159

4.1 Network Risk . . . 159
4.1.1 Network Case Study 1: Camera System . . . 160
4.1.2 Network Case Study 2: Access Control . . . 162
4.2 Communications Attacks . . . 168
4.2.1 Social Engineering . . . 169
4.2.2 Direct Hacking . . . 169
4.2.3 Malware . . . 170
4.2.4 Web Attacks . . . 171
4.3 Information Security Management System . . . 174
4.3.1 Security Policy . . . 175
4.3.2 Organizing Information Systems Security . . . 176
4.3.3 Asset Management . . . 176
4.3.4 Human Resources Management . . . 176
4.3.5 Physical and Environmental Security . . . 176
4.3.6 Communications and Operations Management . . . 177
4.3.7 Access Control . . . 181
4.3.8 Information Systems Acquisition, Development, and Maintenance . . . 182
4.3.9 Information Security Incident Management . . . 182
4.3.10 Business Continuity Management . . . 182
4.3.11 Compliance . . . 183
4.3.12 ISMS Summary . . . 183
4.4 Conclusion . . . 184
References . . . 185

INDEX . . . 187

TABLE OF FIGURES

2-1 Video-to-Recorder Layout. 72
2-2 Video Infrastructure 72
2-3 Basic Access Control Card Flow 74
2-4 Basic Wiegand Flow 75
2-5 Networked Access Control System 76

3-1 ISS Overall Objectives and Control Objectives 90
3-2 Basic Components of Computer Operation. 95
3-3 Direct Communication 98
3-4 Communications by Router. 99
3-5 Computer Logic Entry Points 100
3-6 Authentication 103
3-7 AAA Triad 103
3-8 CIA Triad, Expanded 104
3-9 Firewall 107
3-10 Virtual Private Network 108
3-11 Traditional PBX System 111
3-12 Phone Company Central Office 112
3-13 Voice-over-IP (VOIP) System 113
3-14 Information Security Management Maturity Level 122
3-15 Plan-Do-Check-Act Model Applied to ISMS Processes 145

4-1 Networked Video System 160
4-2 Networked Access Control System 162
4-3 Access Control System Communication: Reader to Controller to Network 163
4-4 Access Control System Communication: Server to Network 163
4-5 Logical Communication Flow 164
4-6 Access Control Elements Connected to Switch 165
4-7 Layer 2 Communication. 165
4-8 Access Control Router Communication 166
4-9 Workstation to Access Control Server Data Flow 167

