PRINCIPLES AND PRACTICE OF INFORMATION SECURITY
Protecting Computers from Hackers and Lawyers

Linda Volonino, Ph.D.
Canisius College

Stephen R. Robinson
Verity Partners, LLC

with contributions by Charles P. Volonino

Upper Saddle River, New Jersey 07458
PART I: DIGITAL LIABILITIES AND RISK MANAGEMENT

Chapter 1  Security in a Globally Connected Economy

Introduction 1

What Is Information Security? 1
  Definition 1
  Security Goals 1
  Applying Conventional Principles to the Cyber World 3
  The Digital Liability Management (DLM) Model 3

The Principles of Security 4
  Security Is Complex 4
  Security Is Difficult to Cost-Justify, but Not Impossible 6

Security in the Information Economy 6
  Global Economy in Transition 6
  Legal Liability Issues 6
  Guide to the Risks Inherent to Conducting Business in a
  Networked Economy 6

Mistakes, Malice, and Mischief Increase Liability—and Legislation 7
  Electronic Evidence 7
  Threats to Information Security 7

Extended Legislation and Responsibilities 8
  Liability Issues and Regulatory Obligations 8
  Electronic Records Retention 9
  International Organizations 10
  DOJ Defines Computer Crime 10
  Congress Expands Computer Crime Legislation and Authority 10

New Ethic of Responsibility 11

Chapter Summary 12

Key Terms 12

Discussion Questions 12

Endnotes 13

Chapter 2  Sources of Digital Liability

Introduction 14

Assessing and Protecting Digital Assets 14
  Risk Assessment 14
  Insufficient Protection Against Avoidable Losses 17
Chapter 3  Threats, Vulnerabilities, and Risk Exposure  31

Introduction  31

Classification of Computer Threats and Vulnerabilities  34
  Uses of the TTV  34

Taxonomy of Threats and Vulnerabilities  35

Origin of the Intrusion or Threat  37
  External Threats and Vulnerabilities  37
  Internal Threats and Vulnerabilities  41
  Wireless Threats and Vulnerabilities  44
  External Threats with Internal Intervention  44
  Internal Protocol Vulnerabilities and Threats  45

Success of Hackers and Malware  47
  Intruders Expand Their Options  47
  Complexity of Software and Configurations  47
  Why Hack Attacks Succeed So Often  47

Threats, Vulnerabilities, and First-Party and Third-Party Risks  48
  First-Party Risks  48
  Third-Party Risks  48
  First- and Third-Party Damages  49

Chapter Summary  49

Key Terms  50

Discussion Questions  50

Endnotes  51
Chapter 4  An Affirmative Model of Defense: Digital Liability Management  52

Introduction  52

The Information Security Challenge Is Not Being Met  52

The Importance of Execution  53
  Hallmarks of Proper Execution  54
  The Risk and Reward of New Initiatives  54
  Higher Standards of Security  55
  Why Is Information Security Poorly Executed?  55

The DLM Defense Model  56
  The DLM Model  56

Tier 1: Senior Management Commitment and Support  56
  Security Awareness Begins and Ends in the Boardroom  57
  Overcoming Objections and Adversaries  58

Tier 2: Acceptable-Use Policies and Other Statements of Practice  59
  AUPs Define Acceptable and Unacceptable Behavior  59
  Stakeholders Involved in AUPs  59
  AUPs Define Expectations and Demonstrate Due Diligence  60
  Everyone Must Practice Information Security  60
  Maintenance Is Important  60

Tier 3: Secure-Use Procedures  60

Tier 4: Hardware, Software, and Network Security Tools  61

Chapter Summary  61

Key Terms  62

Discussion Questions  62

Endnotes  62

Chapter 5  Models for Estimating Risk and Optimizing the Return on Security Investment  63

Introduction  63

The Importance of Risk Assessment  63
  Getting Management's Attention  63
  Risk Assessment: A Basic Requirement of ISO 17799  65
  Raising the Status of Information Security Budgets  65
  Assessing the Expected (Average) Cost of a Loss  65
  Risk Assessment Cube  66

Expected Loss Value Estimations  67
  Expected Loss Computation  67
  Marginal Cost—Benefit Analysis—An Application of Expected Value  68
  Balancing Expected Loss with the Cost of Security Defenses  69

Challenges in Estimating Loss of Digital Assets  69
  Intangible Assets  69
  Replication Increases Exposure and Probability of a Loss  70
  Outsourcing Places Data and Documents Out of Control  71
Chapter 7  Secure-Use Practices: Defensive Best Practices  94

Introduction  94

Secure Use Practices: Policies  94
  Major Risk Factors  94
  Limits on the Extent to Which Risk Factors Can Be Controlled  96
  Enforcement of Secure-Use Practices Must Be Consistent
    with the AUP  96

Key Secure-Use Procedures and Practices  97
  Introducing a Security Focus in the Organizational Planning Process  97
  Establishing Security as a Business Function  97
  Integrating Security and Business Plans  97
  Deploying Information Security Standards  98
  Documentation and Training  99
  Incident Response Policy and Incident Response Teams  99
  Developing a Notification Plan  100

Secure-Use Procedures: Technology  100
  Shut Down Unnecessary Services  101
  Set Up and Maintain Permissions Securely  101
  Conduct Background Checks  102
  Enforce Strong Passwords  102
  Review Partner Contracts  102
  Audit and Update  103

Physical Security  103

Audit and Test  105

Other Secure Principles and Practices  105
  Insurance  105
  Staying Current  106
  Reinforcing Secure-Use Procedures  106
  Rewarding Secure Behavior  106

Worst Practices  107
  Dangerous Email Practices  107
  Dangerous Sharing Practices  107

Chapter Summary  109

Key Terms  109
Chapter 8 Technology and Auditing Systems: Hardware and Software Defenses 111

Introduction 111
Factors Driving the Need for Diverse Technology Layers 113
  Growth in Computer Crime 113
  Growth in Software Complexity and Flaws 113
  Growth in the Release Rate of Security Patches and Service Packs 114

Security Technology 115
  No "Out-of-the-Box" Solutions 115
  Tools and Targets 115

Multilayered, Diverse Technology Infrastructure 115
  Characteristics of a Defensive Technology Infrastructure 116

Underlying Technical Issues 117
  Functional Requirements of Hardware and Software 117
  TCP/IP 117
  Ports 118
  File Integrity Checker 118
  Routers 118

Perimeter and File Protection 119
  Maintaining Confidentiality and Integrity 119
  Firewalls 119
  Stateful Inspection Firewalls 121
  Proxy Server Firewalls 121
  Multiple-Defense Firewalls 121
  DMZ 121
  Personal Firewalls 121
  What Firewalls Cannot Defend Against 123
  Port Scanning and Scanners 123
  Intrusion Detection Systems (IDS) 124
  Honeypots 126
  Cryptography and Encryption Keys 127
  Public Key Infrastructure (PKI) 128
  Virtual Private Networks (VPNs) 129
  Access Control: Tokens and Biometrics 132
  Antivirus (AV) Software 132

Technology for Enforcing Policy 133
  Email and Instant Messaging (IM) Filters 133
  Content Monitors 134
  Sniffers and Scanners 134

Chapter Summary 135
Key Terms 135
Discussion Questions 135
Endnotes 136
PART III: COMPUTER FORENSICS, ELECTRONIC EVIDENCE, FRAUD, AND COMPUTER CRIME LAWS 137

Chapter 9 Electronic Evidence, Electronic Records Management, and Computer Forensics 137

Introduction 137

Electronic Evidence 138

Discovery of Electronic Business Records for Use as Evidence 139
Consequences of Failing to Comply with Discovery Requests 139
Preserving and Disclosing E-Evidence 141

Federal Rules of Civil Procedure—"The Rules" 143

Rule 34 Amended to Include Electronic Records 143
Unsettled Legal Issues Add Complexity and Risk 143
Other Legal Issues with Significant Consequences 144

Electronic Records Management (ERM) 144

Sarbanes-Oxley Act of 2002 145
ERM Guide for Employees 145
ERM and AUP 146

Computer Forensics 146

What Can Be Revealed 147
What Can Be Recovered 147
Handling E-Evidence: The 3 C's 147
Eliminating Electronic Records 148
High-Profile Legal Cases 149

Chapter Summary 150

Key Terms 150

Discussion Questions 150

Endnotes 151

Chapter 10 Computer Crime, Computer Fraud, and Cyber Terrorism 153

Introduction 153

U.S. Federal Statutes Defining Computer Crime, Fraud, and Terrorism 154

New and Amended Laws Address Internet Crimes 154
The Computer Fraud and Abuse Act and Other Statutes 155
Key "Computer Fraud and Abuse" Terms Defined 155
The Computer as the Target of a Crime: Crimes Against a Computer 157
The Computer as the Instrument of a Crime: Crimes Using a Computer 159

Computer Fraud 161

Defining the Problem 161
Factors Contributing to Computer Fraud 161
The Nature of Fraud—and Its Warning Signs 161
Economic Fraud and White-Collar Crime 162
Theories and Principles of Punishment for White-Collar Crimes 162
The Prosecution and Costs of White-Collar Crime 162
Money Laundering 163
Computer Forensics Techniques for Catching Cyber Criminals 164
Documentation of Incidents and Incident Handling 165
Finding E-Evidence of an Intrusion or Attack 169
Tracking Down Cyber Criminals 169
Cyber Terrorism 170
The National Strategy to Secure Cyberspace 170
Digital Pearl Harbor Simulation 170
The Freedom Cyber Force Militia Hijacks Al-Jazeera's Websites 171
Chapter Summary 172
Key Terms 173
Discussion Questions 173
Endnotes 173
Appendix to Part III: USA PATRIOT Act 175

PART IV: PRIVACY 177

Chapter 11 Privacy and Data Protection 177
Introduction 177
Spam 177
Reasons for the Increase in Spam 177
The Economic Impact of Spam 178
Spam Defenses 179
Privacy 180
Characteristics of Security 180
Leaving a Digital Trail 181
Methods of Information Collection 181
International Privacy Law 183
OECD Privacy Guidelines 184
Compliance Initiatives 185
Chapter Summary 186
Key Terms 186
Discussion Questions 187
Endnotes 187

Appendix to Part IV: HIPAA Appendix and Glossary 188

GLOSSARY 192
ABBREVIATIONS AND ACRONYMS 211
REFERENCES 214
ONLINE REFERENCES 221
INDEX 224