

Contents

Preface	xiv
Acknowledgments	xviii
About the Editor	xix
About the Authors	xx

PART 1 Crisis in Information Security 1

CHAPTER 1 Cybercrime and Escalating Risks 3

Expanding Global Cybersecurity Threats	4
Advanced Persistent Threats	4
IM DDOS Botnet	4
Zeus Trojan	5
Kneber Botnet	6
Aurora Botnet and the Google Attack	7
Data Breach Risks	7
Aggregated Electronic Information at Risk	8
Credit Card, Driver's License, Bank Account, and Social Security Numbers	8
Medical Records	9
Tax and Financial Records	10
Law Firm Records	10
Mortgages and Consumer Loans	11
Mergers and Acquisitions	12
Cloud Computing	12
New Technologies, New Risks	13
Mobile Devices	13
Mobile Marketing	14
Peer-to-Peer File Sharing	14
Failed Security	15
The State of Information Security in the 21st Century?	15

CHAPTER 2**Despite the Alarming Trends,
Data Breaches Are Preventable 17**

Alarming Trends	17
Data Breach Incidents by Industry	18
Number of Records Breached by Industry	20
Millions of Medical Records Breached	20
Causes of Data Breaches	22
Lost and Stolen Computers, Laptops, and Portable Devices	23
Improper Disposal of Paper Documents	23
Accidental Exposure	25
Insider Threats	25
Hacker Attacks	27
What Information Has Been Compromised in Data Breaches?	27
Data Breaches Can and Must Be Prevented	28
Action Plan to Prevent Data Breaches—Encryption Considerations	29

CHAPTER 3**The Aftermath of Data Breaches:
Potential Liability and Damages 31**

Introduction	31
Liability and Damages Resulting from Major Data Breaches	34
TJX	34
Heartland Payment Systems	38
RBS WorldPay	40
Hannaford Bros.	40
Discount Shoe Warehouse (DSW)	43
CardSystems Solutions	44
Data Breaches Continue	45
Role of Security Standards	46
Criminal Prosecutions	47
Conclusion	47

CHAPTER 4**The Underground World of Online Identity Theft:
An Overview 49**

PART II Anatomy of the Major Data Breaches 55**CHAPTER 5****Encrypted Records—Failed Security 57**

How a Hacker Attack Unfolds	59
The Basics of Payment Card Processing	60
Heartland: Transmission of Sensitive Data in the Clear	61
What Sensitive Information Was Stolen?	62
Anatomy of the Breach	62
Hannaford: Security Failures at Critical Junctures	64
What Sensitive Information Was Stolen?	64
Anatomy of the Breach	64
RBS WorldPay: Vulnerable Network	66
What Sensitive Information Was Stolen?	66
Anatomy of the Breach	66
TJX: Sensitive Data in the Clear, Weak Encryption, Unprotected Encryption Key	69
What Sensitive Information Was Stolen?	70
Anatomy of the Breach	70
DSW: Unsecured Network, Weak Passwords	73
What Sensitive Information Was Stolen?	73
Anatomy of the Breach	74
Web Newsroom: Unprotected Encryption Key	75
What Sensitive Information Was Stolen?	76
Anatomy of the Breach	76
Guidance Software: Unencrypted Database Records	77
What Sensitive Information Was Stolen?	77
Anatomy of the Breach	77
CardSystems: Failure to Apply a Firewall, Maintain Virus Definitions, and Use Strong Passwords	79
What Sensitive Information Was Stolen?	80
Anatomy of the Breach	80
Criminal Prosecutions	82
Better Security Practices?	83
End-to-End Encryption	83
Payment Processors Information Sharing Council	84
“Military Industrial Strength” Security	84
Security Lessons Learned	84

PART III Law 87

CHAPTER 6

Ambiguities in State Security Breach Notification Statutes 89

The Basic Obligation	90
What Is Covered Personal Data?	92
What Is a Security Breach?	93
What Is Encrypted Data?	94
When Does a Breach Trigger the Obligation to Notify?	97
Who Is an Employee or Agent?	98
What Assumptions Can/Should You Make?	100

CHAPTER 7

State Data Breach Notification Laws and the Duty to Provide Information Security 103

Nevada: Professionally Based Security Standards	103
Massachusetts: Risk-Based Approach	105
What Personal Information Is Covered?	106
What Is a Security Breach?	106
What Is Encrypted Data?	107
What Data Must Be Encrypted?	108
What Is the Duty to Report a Known Security Breach or Unauthorized Use of Personal Information?	108
What Are the Requirements for Security Breach Notifications?	109
What Is a Comprehensive Information Security Program?	109
Written Information Security Plan	110
Computer Security System Requirements	110
Records Disposition	112
Verification of Third-Party Service Providers	112
Compliance	112
Maryland and New Jersey: Information Security Statutes	113
Breach of Health Information	113
Affirmative Security Measures	113

CHAPTER 8**HITECH: The First Federal Data Breach Notification Law****115**

Overview	115
Breach of Protected Health Information	116
Concept of a “Safe Harbor”	116
Standards Issued by NIST	117
Role of the Federal Trade Commission	117
What Is a Breach?	117
General Definitions	117
Rebuttable Presumption of Unauthorized Access	119
Limiting PHI and Access to the “Minimum Necessary”	120
The Concept of “Harm” and Risk Assessments	121
Risk Assessment	123
“Risk Assessment” as a Tool for Determining Harm—A Critique	124
Exceptions to the “Breach Rule”	125
Limitations of Notification Requirements	126
Heightened HIPAA Enforcement Under HITECH	128
Summary	129
What Is Unsecured Protected Health Information?	129
Encryption and Destruction	129
“Safe Harbor”	131
When Does a Breach Trigger Notice Obligations?	133
What Are the Requirements for Breach Notification?	134
Who Must Be Notified?	134
When Must Notice Be Provided?	134
What Form of Notice Is Required?	135
What Is the Content of the Notification?	135
Who Is Covered by the Breach Notification Requirements?	136
What Personal Information Is Covered?	139
Health Care Breach Challenges Remain	141

CHAPTER 9**Breach Notification and Encryption:
A Global Perspective****143**

Notification Obligations: Overview	143
Data Protection Requirements: Overview	146
Notification and Encryption Requirements by Country	150

Argentina	150
Australia	151
Austria	152
Belgium	152
Brazil	155
Canada	155
Chile	157
China (PRC)	157
Colombia	157
Czech Republic	158
Egypt	159
France	159
Germany	160
Hong Kong	161
Hungary	162
Indonesia	162
Italy	162
Japan	163
Malaysia	164
Mexico	165
Netherlands	166
Philippines	167
Poland	167
Russia	168
Singapore	168
Spain	169
Sweden	170
Switzerland	171
Taiwan	171
Thailand	171
United Kingdom	172
Vietnam	173
PART IV Technology	175
CHAPTER 10	
Encryption: The Basics	177
Encryption Overview	177
Cryptographic Algorithms	178
Key Management	179

Applying Encryption	181
In-Flight Versus At-Rest Encryption	181
SNIA Position on Encryption	181
Point of Encryption	182
Factors to Consider	183
Encryption and Key Management Guidance	184
Encryption	185
Guidance for Key Management	186
An Approach to Implementing Encryption	188
Step 1: Understand Confidentiality Drivers	188
Step 2: Classify the Data Assets	188
Step 3: Inventory Data Assets	189
Step 4: Perform Data Flow Analysis	189
Step 5: Determine the Appropriate Points of Encryption	189
Step 6: Design the Encryption Solution	189
Step 7: Begin Data Realignment	189
Step 8: Implement Solution	189
Step 9: Activate Encryption	190
Summary	190

CHAPTER 11

Encryption Best Practices

191

Encryption Fundamentals	191
NIST and the AES Encryption Standard	193
What Can Go Wrong with Encryption?	194
Short Encryption Key Lengths	194
The Key Itself Is Not a Completely Random Number	194
The Encryption Key Is Compromised	194
Layered Encryption	195
Encrypting the Keys	195
Hardware Encryption Protection	195
Access to the Encryption Keys	196
A Key Protects Other Keys	196
Multi-Factor Authentication	196
Public Key Cryptography	197
Public Key Cryptosystems	197
Critical Encryption Measures	198

CHAPTER 12**Circumventing Data Encryption:
Password Vulnerabilities 201**

Passwords and Data Encryption	201
Shared Secrets	202
Biometrics, Two-Factor Authentication, and One-Time Passwords	203
Password Attacks	204
Prevention	206

CHAPTER 13**Managing Cryptographic Keys 207**

Associated Standards and Standards Committees	207
Introduction to Enterprise Key Management Infrastructure	208
The Key Management Lifecycle	209
Creation	209
Backup	210
Deployment	211
Monitoring	211
Rotation	211
Expiration	212
Archiving a Key	213
Destruction	213
Other Considerations	213
Exercise Key Management Processes	214
Dual Control and Separation of Duties	214
Key Escrow	214
Product Interoperability	214
Catastrophic Failure	215
Using Encryption for Virtual Shredding	215
Proper Key Management	216

CHAPTER 14**The Self-Encrypting Drive 217**

Basic Characteristics	219
Variations on the Basic Self-Encrypting Drive	222
Common Concerns	224
Future Capabilities Defined by the TCG Specifications	224
What the Future of Encrypted Data May Hold	224

CHAPTER 15**Encryption Technologies: A Practical Assessment 227**

Choices for Hiding Information	227
Encryption Algorithms: An Historical Perspective	228
Factors to Be Considered in Making Encryption Decisions	229
Media That Can or Should Be Encrypted	229
Advanced Encryption Standard	230
Encryption with Web Browsers	230
Hardware Versus Software Encryption	232
Hardware Encryption	232
Software Encryption	232
Some Available Encryption and Decryption Software	232
Examples of File Software Encryption	234
Key Management	236

PART V Response 239**CHAPTER 16****Security Best Practices: The Watchword Is Prioritize! 241**

21st Century Information Security Challenges	241
Failed Security	243
Data Breaches Can and Must Be Prevented	243
Where to Begin?	244
National Institute of Standards and Technology Guidelines	244
ISO/IEC 27000-series Standards	245
COBIT	246
National Identity Management Strategy	247
The Security Response	248
Twenty Critical Controls for Effective Cyberdefense:	
Consensus Audit	248
Top 25 Most Dangerous Software Errors	249
Insider Threats Must Be Countered	250
Payment Card Industry Data Security Standard	251
Cloud Security	253
Now Is the Time to Become Serious	
About Information Security	253

CHAPTER 17**Responding to Data Breaches 255**

Report Immediately to a Designated Internal Contact Any Discovered or Suspected Breach	256
Investigate Any Reports Promptly and Thoroughly	256
Stop the Source of the Breach and the Associated Harm	257
Evaluate Your Legal Obligations Regarding the Incident	257
Strategize Communications About the Incident	259
Help the Data Subjects	259
Identify Internal Policies and Procedures That Should Be Immediately Changed	260
Notify the Affected Data Subjects and Other Relevant Entities Where Warranted	260
Evolve Practices and Procedures on an Ongoing Basis	262

CHAPTER 18**Technology to Prevent Data Leaks 265**

Protection at the Data Level	265
Rogue Devices and Software	267
Access Control	267
Data Protection	267
Tools for DLP Risk Mitigation	268
Effective Data Security Is Required	270

CHAPTER 19**Insurance Protection for Security Breaches 271**

Types of Insurance Potentially Applicable to Liability or Loss from a Security Breach	271
Overview	271
First-Party Property Insurance	272
Business-Interruption Insurance	273
Fidelity Insurance and Bonds	274
Electronic Funds Transfer Insurance	274
Third-Party Liability Insurance	275
General Liability Insurance	275
Media Liability Insurance	277
Directors and Officers and Fiduciary Liability Insurance	277
Errors and Omissions Insurance	279
Cyberrisk Insurance Coverage	280
Types of Exposures Covered	280
First-Party Versus Third-Party Coverage	280
Role of Auditing and Loss Prevention	281
Risk-Management Tips	281

Tips for Purchasing Insurance	281
Tips for Making Claims	281
All Claims	282
Claims Under Liability Insurance Policies	282
Claims Under First-Party Insurance Policies	282
Appendix A—Security Breach Notification Laws	285
Appendix B—Summary of Data Breach Notification and Encryption Laws	289
Appendix C—Resources	309
Index of Important Cases	317
Index	319