

Enterprise Information

Security and Privacy



C. WARREN AXELROD • JENNIFER L. BAYUK
DANIEL SCHUTZER
editors

Contents

	Foreword	<i>xiii</i>
	Preface	<i>xix</i>
	Acknowledgments	<i>xxiii</i>
	Part I: Trends	1
1	Privacy Roles and Responsibilities	3
1.1	Background	4
1.2	Observations	8
1.3	Recommendations	12
1.3.1	Roles and Responsibilities of Information Security	14
1.3.2	The Impact of Outsourcing: Privacy, Security, and Enforcing Controls	16
1.3.3	Privacy and New Roles for Information Security	16
1.4	Future Trends	18
2	Data Protection	21
2.1	Background	21
2.2	Observations	24

2.3	Recommendations	27
2.3.1	Formalize a Trust Model	28
2.3.2	Utilize an Integrated and Holistic Approach to Security and Governance	30
2.3.3	Implement a Risk-Based Systemic Security Architecture	32
2.3.4	Support an Adaptive Security Approach to Security	36
2.3.5	Build Systems, Applications, Networks, Protocols, and Others Using Accepted Standards	37
2.4	Future Trends	40
3	IT Operational Pressures on Information Security	41
3.1	Background	41
3.1.1	IT Operations and IT Service Development Impede Information Security Goals	42
3.1.2	Information Security Impedes IT Operations and IT Service Development Goals	43
3.1.3	Information Security Using a Technology-Centric, Bottom-Up Risk Model	44
3.2	Observations	45
3.3	Recommendations	48
3.3.1	Stabilize the Patient and Get Plugged into Production	51
3.3.2	Find Business Risks, Identify Controls, and Fix Fragile Artifacts	53
3.3.3	Implement Development and Release Controls	55
3.3.4	Continually Improve	56
3.4	Future Trends	57
4	Information Classification	59
4.1	Background	60
4.2	Observations	62
4.3	Recommendations	65
4.4	Future Trends	69

5	Human Factors	71
5.1	Background	72
5.1.1	Historical Perspective on Privacy	73
5.1.2	Impact of Technology on Privacy	74
5.1.3	Privacy in a Corporate Setting	76
5.1.4	Evolution of Personal Information	76
5.2	Observations	77
5.2.1	Privacy Trade-offs—Human Behavioral Impact on Privacy	77
5.2.2	What is Risk?	80
5.3	Recommendations	83
5.4	Future Trends	87
	Acknowledgments	87
	Part II: Risks	89
6	Making the Case for Replacing Risk-Based Security	91
6.1	Introduction	92
6.1.1	Understanding Security Risk	92
6.2	Why Risk Assessment and Risk Management Fail	95
6.2.1	Misplaced Support for Risk-Based Security in Practice	97
6.2.2	Alternatives to Security Risk Assessment	99
6.3	Conclusion	101
7	The Economics of Loss	103
7.1	Security as the Prevention of Loss	104
7.2	Quantifying the Risk of Loss	105
7.3	Refining the Basic Risk Equation	106
7.4	The Problem of Quantifying Loss Itself	106
7.5	Confronting the Reality of Hypothetical Actions	107
7.6	Overcoming the Fixation on Assets	108

7.7	Overcoming the Fixation on Market Value	108
7.8	Overcoming the Fixation on Productivity	110
7.9	Overcoming the Neglect of Substitutes	111
7.10	Taking Account of the Duration and Extent of the Effects	112
7.11	Distinguishing Between the Different Business Categories of Attacks	113
7.12	Putting the Proper Risk Estimates Back into the ROI Calculation	114
8	Legal and Regulatory Obligations	115
8.1	The Expanding Duty to Provide Security	116
8.1.1	Where Does It Come From?	116
8.1.2	What Is Covered?	118
8.2	The Emergence of a Legal Standard for Compliance	120
8.2.1	The Developing Legal Definition of “Reasonable Security”	122
8.2.2	An Increasing Focus on Specific Data Elements and Controls	128
8.3	The Imposition of a Duty to Warn of Security Breaches	131
8.3.1	The Basic Obligation	132
8.3.2	International Adoption	134
8.4	Conclusion	135
9	Telecommunications	137
9.1	Security Issues in Mobile Telecommunications	138
9.1.1	Pressure on the Perimeter Model	138
9.1.2	Computer Security Threats for Portable Devices	139
9.2	Security Issues in Global Telecommunications	140
9.2.1	Global Cooperation on Cyber Attack	140
9.2.2	Global Attention to Software Piracy	141

9.3	Security Issues in Internet Protocol–Based Telecommunications	141
9.3.1	Reduced Technological Diversity	142
9.3.2	Increased Reliance on Shared, Decentralized Internet-Based Systems	142
9.4	Security Issues in Bandwidth-Increasing Telecommunications	143
9.4.1	Residential Users Have Greater Security Responsibility	143
9.4.2	Botnets Become a Huge Threat to the Global Economy	144
	References	146
	Part III: Experience	147

10	Financial Services	149
-----------	---------------------------	------------

10.1	Laws, Regulations, and Supervisory Requirements	150
10.1.1	Gramm-Leach-Bliley Act of 1999	153
10.1.2	The Sarbanes-Oxley Act of 2002	154
10.1.3	The Fair and Accurate Credit Transactions Act of 2003	154
10.1.4	Breach Notification Requirements	155
10.1.5	Supervisory Guidance	158
10.2	Future Focus	160
10.2.1	Identity Theft Prevention	160
10.2.2	Outsourcing and Offshoring	160
10.2.3	Cross-Border Data Flows	161
10.2.4	Encryption	161
10.2.5	Online Behavioral Advertising	162
10.2.6	Internet Governance	162
10.2.7	Wireless Security	162
10.2.8	Capital Requirements for Operational Risk	162
10.2.9	Security of Web-Based Business Applications	163
10.2.10	Other Future Focuses in Financial Sector Security	163
10.3	Compliance Challenges	163

11	Energy	165
-----------	---------------	------------

11.1	Overview of Sector	166
------	--------------------	-----

11.2	Risks Related to Security and Privacy	169
11.3	How Risks Are Addressed	171
11.4	Documentation and Its Relation to Information Security	174
11.5	Conclusion	177
	Acknowledgments	178
	Selected Bibliography	178
12	Transportation Security	181
12.1	Overview	182
12.2	Technology's Role in Transportation Security	183
12.3	Security in Transit	187
12.4	Best Practices Applied	189
13	Academia	191
13.1	Overview	192
13.1.1	Age and Demographics	192
13.1.2	You Cannot Fire Me	192
13.1.3	Hard to Educate Users	192
13.1.4	Lax Controls	193
13.1.5	How Everything Is Connected	193
13.2	Case Studies	193
13.2.1	Case Study: Social Networking and Crimeware	194
13.2.2	Case Study: Social Phishing	196
13.2.3	Case Study: Infected Access Points	196
13.3	Protection	197
	References	197
	Appendix A	
	Key Information Security Law References	199
A.1	Federal Statutes	199
A.2	State Statutes	200
A.3	Federal Regulations	204
A.4	State Regulations	206

A.5	Court Decisions	206
A.6	FTC Decisions and Consent Decrees	207
A.7	State Attorneys General Consent Decrees	208
A.8	European Union—Directives	209
A.9	European Union—Security Provisions in Country Implementations of Data Protection Directive	209
A.10	Other Countries	212

About the Authors	213
--------------------------	------------

Index	223
--------------	------------
