

Table of Contents

The ABA Cybersecurity Legal Task Force	xv
Judy Miller and Harvey Rishikof, Immediate Past Chairs	
Acknowledgments	xix
Section I	
CYBERSECURITY BACKGROUND	1
<i>CHAPTER 1</i>	
Purpose of This Handbook	3
Jill D. Rhodes and Robert S. Litt	
<i>CHAPTER 2</i>	
Understanding Cybersecurity Risks	11
Lucy L. Thomson	
I. New Technologies Create Unprecedented Challenges for Lawyers	11
A. Responsibilities to Protect Sensitive and Confidential Data	15
B. Lawyers and Law Firms Are Prime Targets: The Significant Resulting Damage	16
II. Protecting the Confidentiality, Integrity, and Availability of Data	17
III. Security Breaches on the Rise: Threats and Vulnerabilities Illustrated	20
A. Hacking and Advanced Persistent Threats	20
B. Social Engineering and Phishing Attacks	22
C. Ransomware	25
D. Business E-mail Compromise	28
E. Malicious Insiders	29
F. Mobile Devices	31

G. Cloud Computing and Wi-Fi Risks	34
H. Improper Disposal of Personal Information	35
I. Business Partners Can Be a Weak Link—A Two-Edged Sword for Law Firms	36
IV. Addressing Threats and Risks to Law Firm Security	38
A. What Is “Information Security”?	38
B. Why Is Information Security Important?	39
C. Who Is Responsible?	39
D. The Need for Risk Assessment	39
E. Achieving Optimal Network Security through Continuous Monitoring	41
V. Steps to Protect Confidential Law Firm Records and Prevent Data Breaches: Top Considerations	42

CHAPTER 3

Understanding Technology: What Every Lawyer Needs to Know about the Cyber Network	45
Paul Rosenzweig	
I. The Growth of the Cyber Network	46
II. The Structure of the Cyber Network	47
III. Changing Architectures	48
IV. Threats on the Cyber Network	50
V. Defensive Systems and Enterprise Challenges	53
VI. Top Ten Considerations	57

Section II

LAWYERS’ LEGAL AND ETHICAL OBLIGATIONS TO CLIENTS	59
--	----

CHAPTER 4

Lawyers’ Legal Obligations to Provide Data Security	61
Thomas J. Smedinghoff and Ruth Hill Bro	
I. Overview	61
A. What Is Data Security?	61
B. Security Law: The Basic Security Obligations	64
II. The Duty to Provide Data Security	65
A. What Is the Duty?	65

B. To Whom Does the Duty Apply?	65
C. What Is the Source of the Duty?	67
D. What Data Is Covered?	70
E. What Level of Security Is Required?	72
F. The Legal Requirements for “Reasonable Security”	73
G. Rules Governing Specific Data Elements and Controls	88
H. Frameworks for Reasonable Security	89
III. The Duty to Notify of Security Breaches	92
A. What Is the Source of the Duty?	92
B. What Is the Statutory Duty?	93
C. When Does a Contract-Based Duty Arise?	95
IV. Practical Considerations: A Top Ten List	96

CHAPTER 5

International Norms	99
Conor Sullivan, Kelly Russo, and Harvey Rishikof	
I. Introduction	99
II. International Norms and International Regulatory Framework	100
A. Tallinn	101
B. United Nations	101
C. International Organization for Standardization (ISO)	103
III. Key Laws in Europe, Latin America, China, Russia	104
A. European Union	104
B. Latin America	108
C. China	108
D. Russia	110
IV. Notable U.S. Incidents/Cases	111
V. How International Cyber Norms Affect Legal Practice	113

CHAPTER 6

Lawyers’ Obligations to Provide Data Security Arising from Ethics Rules and Other Law	115
Peter Geraghty and Lucian T. Pera	
I. ABA Formal Opinion 477R	115
II. Lawyer Ethics Rules	118
A. Confidentiality	118

B. Competence	123
C. Supervision of Lawyers and Nonlawyers	125
III. The Law of Lawyering	126
IV. Examples of the Emerging Application of Ethics and Lawyering Law to New Technology	127
A. E-mail	127
B. Portable Devices and Other Devices That Retain Data	131
C. Metadata Leaks	133
D. Outsourcing	134
E. Cloud Computing	136
F. Social Media	138
V. Conclusion	141

CHAPTER 7

Occasions When Counsel Should Consider Initiating a Conversation about Cybersecurity with the Client	145
Roland L. Trope and Lixian Loong Hantover	
I. Introduction	145
A. The Problem: Lawyers and Law Firms Have Become High-Priority Targets for Cyber Attacks	145
B. Preparations That Lawyers and Law Firms Would Be Wise to Make	149
II. Nine Occasions That Warrant Discussion of Cybersecurity	150
A. At the Start of a Representation	151
B. When the Client Enters a Regulated Field of Activity	153
C. When Cybersecurity Regulations Are Issued, Amended, or Judicially Reinterpreted	154
D. When Litigation, Enforcement Action, or Investigation Is Reasonably Anticipated	156
E. When the Client Experiences a Cyber Incident	158
F. When Counsel Experiences a Cyber Incident or When Reports of Cyber Incidents Demonstrate the Law Firm's Need to Enhance Its Safeguards of Client Confidential Information	160

G. When the Client Anticipates Being the Buyer or Target in a Merger or Acquisition, Particularly If Counsel Anticipates the Need for a Review of the Transaction by CFIUS	162
H. When the Client Anticipates Providing Goods or Services for New Communications Technologies in a Regulated Sector, Such as Providing IoT Devices for Use in Connected Vehicles	169
I. For In-House Counsel, When the Client/Organization Embarks on a Major Transition in Its Corporate or Commercial Activities and May Be Tempted to Devise Software to Circumvent Regulatory Obstacles	172
III. Practical Considerations	180

Section III

UNDERSTANDING DIFFERENT LEGAL PRACTICE SETTINGS	185
--	-----

CHAPTER 8

Large Law Firms	187
Alan Charles Raul and Michaelene E. Hanley	
I. Introduction to Cybersecurity for Large Law Firms	187
II. Cybersecurity Issues and Challenges for Large Firms	191
III. How Large Law Firms May Address Cyber Risk	197
A. Governance and Strategy	198
B. Cyber Preparedness	200
C. Administrative, Technical, and Physical Measures	201
D. Vendor Management	201
E. Incident Response and Threat Intelligence	202
F. Data Recovery and Business Continuity	203
G. Continual Process Improvements	203
IV. Top Ten Considerations for Large Law Firm Lawyers	204

CHAPTER 9

Cybersecurity for the Little Guys	207
Theodore L. Banks	

CHAPTER 10

In-House Counsel	219
Angeline G. Chen	
I. The Cyber Threat Landscape for In-House Counsel	219
A. Role Differentiation	220
B. The In-House Perspective	222
C. Duties and Responsibilities	224
II. Fundamentals of What In-House Counsel Needs to Know	225
A. The Basics	225
B. The Amorphous and Unusual Nature of the Threat Compared to Traditional Risks	226
C. Establishing Essential Relationships	227
D. Distinguishing Compliance in Operational Matters from Market-Based Considerations	229
III. Be Prepared	229
A. Understand as Much as You Can about the Risks	229
B. Ensure That the Company's Governance Framework Encompasses Cybersecurity, and Develop Cyber Incident and Cyber Breach Plans That Align with That Framework	231
C. Identify and Establish Key Relationships and Be Part of the Team	234
D. Identify Legal Issues Associated with a Cyber Incident	235
E. Cultivate a Cyber-Aware Culture and Community	238
IV. Responding to a Cyber Incident	238
A. Identify the Attack and Damage	239
B. Limit the Damage	239
C. Record and Document	239
D. Engage and Notify	240
E. Correct and Close	240
V. In the Aftermath	240
VI. Special Considerations	242
VII. Summary and Tips	242

CHAPTER 11

Considerations for Government Lawyers	245
Sandra Hodgkinson, Clark Walton, and Timothy H. Edgar	
I. Government Cyber Lawyers and Their Mission	247
A. Department of Defense (DoD)	247
B. Department of Homeland Security (DHS)	248
C. Department of Justice (DoJ)	249
D. Department of Treasury	249
E. Other Agencies	249
II. Government Data: An Increasing Problem of Data Insecurity	250
III. Government Centric Attacks: National Security and Critical Infrastructure	253
IV. Significant U.S. Cyber-Related Laws	256
V. Best Practices for the Government Lawyer for Cybersecurity	259

CHAPTER 12

Public Interest Attorneys	263
Michelle Richardson	
I. Introduction: Why Public Interest Attorneys Should Be Concerned	263
II. Issues and Strategies	265
A. Defining What Information to Protect: Nonprivileged but Sensitive Data	265
B. Budget Constraints	265
C. Use of Interns and Volunteers	267
D. Cultural Hurdles	268
E. Special-Needs Clientele	268
III. Takeaways and To-Dos	269

CHAPTER 13

Get SMART on Data Protection: Training and How to Create a Culture of Awareness	271
Ruth Hill Bro and Jill D. Rhodes	
I. Data Protection Training Basics and Core Principles	271
A. Why Train on Data Protection?	272
B. What Does SMART Training Look Like?	275

II. SMART Training in Action	279
A. Understanding the Basics of Employees: Role and Generational Differences	279
B. Building an Effective and Diverse Program	280
C. Measuring Success (Through Phishing Campaigns and Other Means)	283
III. Ten Key Points	284

Section IV

INCIDENT RESPONSE AND CYBER INSURANCE COVERAGE	287
---	-----

CHAPTER 14

Best Practices for Incident Response: Achieving Preparedness through Alignment with Voluntary Consensus Standards	289
George B. Huff Jr., John A. DiMaria, and Claudia Rast	
I. Introduction	289
A. Business Continuity and Management of the Law Firm's Business Risks	290
B. The Cybersecurity Framework	292
II. ISO 22301, the International Standard for Business Continuity Management Systems	295
A. Global Benchmark for BCMS Requirements	295
B. Law Firms: Steps for Establishing Your Firm's Business Continuity Program	296
C. Information and Communications Technology Readiness for Business Continuity	300
III. ISO 27001: Challenges for Law Firms of All Types and Sizes	301
A. Threats, Disruptions, and Trends	302
B. Impacts of Extended ICT Disruptions—A Common Cyber Incident Scenario	303
C. Best Practices for Cyber Incident Response	304
IV. Conclusion	310

*CHAPTER 15***Cyber Insurance for Law Firms and Legal**

Organizations	313
Kevin P. Kalinich and James L. Rhyner	
I. Insurance as a Cyber Risk Management Tool	313
II. Professional Liability Insurance Policies May Cover Some Cyber Incidents	315
III. Cyber Insurance Coverage Can Mitigate the Costs of an Incident in Several Respects	317
IV. Policy Wording Varies and Often Requires Customization to Match Identified and Quantified Exposures	322
V. Cyber Insurance Market Constraints	330
A. Regulatory Constraints	330
B. Capacity Constraints	330
C. Insurance Placement Constraints	331
VI. How to Respond to a Loss or Claim	331
VII. Top Ten Considerations	332
Conclusion	335
Robert S. Litt and Jill D. Rhodes	

Appendices*CHAPTER 4 APPENDICES: SELECTED SECURITY*

<i>LAW STATUTES, REGULATIONS, AND CASES</i>	
Appendix A. Federal Statutes	341
Appendix B. State Statutes	343
Appendix C. Federal Regulations	351
Appendix D. State Regulations	355
Appendix E. Best Practice Guidelines Issued by Federal Government Agencies	357
Appendix F. Best Practices Guidelines Issued by State Government Agencies	359
Appendix G. Court Decisions re Duty to Provide Data Security	361
Appendix H. CFPB Decision and Consent Decree	363

Appendix I. FTC Decisions and Consent Decrees	365
Appendix J. SEC Decision and Consent Decree	367

CHAPTER 6 APPENDICES: ABA AND STATE BAR ASSOCIATION ETHICS OPINIONS AND OTHER RESOURCES REGARDING LAWYERS' ETHICAL OBLIGATIONS TO PROVIDE DATA SECURITY TO THEIR CLIENTS

Appendix K. Ethics Opinions on Lawyer Confidentiality Obligations concerning E-mail	369
A. ABA Formal Ethics Opinions	369
B. ABA Treatises and Annotated Model Standards	371
C. State Bar Ethics Opinions That Have Addressed E-mail Usage (with Links to the Full Text Where Available)	372
D. State Bar Ethics Opinions That Address Cordless and Cell Phone Usage	385
Appendix L. Ethics Opinions concerning a Lawyer's Obligations to Prevent the Inadvertent Disclosure of Confidential Client Information in Metadata	387
A. ABA Ethics Opinions	387
B. ABA Treatises, Annotated Model Standards, and Other Resources on Metadata	388
C. Digests of State Bar Ethics Opinions on Metadata	388
Appendix M. Ethics Opinions on Lawyer Confidentiality Obligations concerning Outsourcing	397
A. ABA Formal Opinion Headnotes	397
B. ABA Treatises and Annotated Model Standards	398
C. Bar Association Reports	399
D. Digests of State Bar Association Ethics Opinions on Outsourcing	399
E. State Bar Ethics Opinions That Address Issues Similar to Those Addressed in ABA Formal Opinion 95-398 (allowing outside computer maintenance firms access to law firm computer networks)	407

Appendix N. Ethics Opinions on Lawyer Confidentiality Obligations concerning Cloud Computing	411
A. ABA Reference Material and Bar Association Reports on Cloud Computing	411
B. Digests of State Bar Ethics Opinions on Cloud Computing	412
Appendix O. Ethics Opinions Relating to Lawyers' Passive Communications with Jurors on Social Media	425
A. ABA Ethics Opinions	425
B. ABA Reference Material and Bar Association Reports on Lawyers' Passive Communications with Jurors on Social Media	426
C. Digests of State Bar Ethics Opinions regarding Lawyers' Passive Communications with Jurors on Social Media	426
 <i>CHAPTER 14 APPENDICES: INCIDENT RESPONSE AND CYBER INSURANCE COVERAGE</i>	
Appendix P. Implementing ISO 22301: The International Standard for Business Continuity Management Systems—Requirements	431
Appendix Q. Implementing ISO 22301 and/or the ISO 27000 Series of Standards	437
Appendix R. Implementing ISO/IEC 27001: The International Standard for Information Security Management Systems	441
 Author Biographies	 447
 Index	 467