

Table of Contents

About the Author	vii
Table of Chapters	ix
Acknowledgments	xvii
Introduction	xix

Chapter 1 The Cybersecurity Threat Landscape

§ 1:1	Overview	1
§ 1:2	Background.....	3
§ 1:3	Specific Types of Cyber Threats.....	7
§ 1:3.1	Ransomware.....	8
§ 1:3.2	Data Breaches.....	10
§ 1:3.3	Ongoing Monitoring of Communications	12

Chapter 2 Lawyers’ Professional Obligations in Response to Cyberattacks

§ 2:1	Cyber Threat Activity Targeting Law Firms	14
§ 2:2	Early ABA Responses to Cyberattacks Against Law Firms	15
§ 2:3	ABA Formal Opinion 483	16
§ 2:3.1	What Is a Data Breach?	18
§ 2:3.2	Preventing a Data Breach.....	19
§ 2:3.3	Detecting a Data Breach	21
§ 2:3.4	Mitigating the Effects of a Data Breach.....	22
[A]	Stopping the Breach.....	23
[B]	Recovering from a Breach.....	25
§ 2:3.5	Informing Clients of a Data Breach	26

Cybersecurity Obligations

§ 2:4	State Ethical Obligations to Address Cybersecurity....	29
§ 2:4.1	State Ethics Opinions That Mirror ABA Formal Opinion 483	29
[A]	California.....	29
[B]	Colorado.....	30
[C]	Kentucky.....	30
[D]	Louisiana.....	31
[E]	Maine.....	31
[F]	Michigan.....	32
[G]	New Hampshire.....	32
[H]	New Jersey.....	33
[I]	Virginia.....	34
§ 2:4.2	State Codes Adopting Model Rule 1.6.....	35
§ 2:4.3	Ethical Obligations Pertaining to Cybersecurity in States That Do Not Explicitly Incorporate Rule 1.6(c)	39
§ 2:5	Continuing Cyber Threats to and Data Breaches of Law Firms After Adoption of Formal Opinion 483.....	41

Chapter 3 State Data Breach Notification Laws and Data Privacy Laws

§ 3:1	Overview	43
§ 3:2	Massachusetts Data Breach Notification Law.....	44
§ 3:3	State Notification Laws with Reasonable Security Measure Requirements	47
§ 3:3.1	Arkansas	47
§ 3:3.2	Connecticut.....	48
§ 3:3.3	Florida	50
§ 3:3.4	Indiana	51
§ 3:3.5	Maryland	52
§ 3:3.6	New York SHIELD Act	53

Table of Contents

§ 3:4	Consumer Privacy Protection Laws	54
§ 3:4.1	The Role of the GDPR in the United States	54
§ 3:4.2	State Consumer Privacy Laws	55
[A]	California	56
[B]	Colorado	57
[C]	Connecticut	57
[D]	Utah	58
[E]	Virginia	58

Chapter 4 Federal Regulation of Cybersecurity Obligations

§ 4:1	Overview	61
§ 4:2	Regulations Based on the Characteristics of the Breached Data	62
§ 4:2.1	Health Care Data	62
[A]	The Privacy Rule—Defining What Data Is Protected	63
[B]	The Security Rule—Setting Standards for Data Protection	64
[C]	The Breach Notification Rule—Obligations in the Case of a Data Breach	70
§ 4:2.2	Critical Infrastructure	72
§ 4:3	Regulations Based on Relationship with the Federal Government	75
§ 4:3.1	Federal Acquisition Regulation and Defense Federal Acquisition Regulation Supplement Obligations	75
§ 4:3.2	Defense Department’s Cybersecurity Maturity Model Certification	81
[A]	CMMC 1.0	82
[B]	CMMC 2.0	84

Chapter 5 Demonstrating Reasonable Cybersecurity through the Use of the SAFETY Act

§ 5:1 “Reasonable” Cybersecurity Measures..... 87
§ 5:2 SAFETY Act 91
§ 5:3 Background on the SAFETY Act 92
§ 5:4 SAFETY Act Liability Protections 94
§ 5:5 Invoking the SAFETY Act through an
 “Act of Terrorism” 94

Chapter 6 Insuring Against Data Breaches and Other Cyber Threats

§ 6:1 Introduction..... 106
§ 6:2 Malpractice Insurance for Data Breach Claims 106
§ 6:3 Cyber Insurance 108
 § 6:3.1 First-Party Cyber Insurance Coverages..... 108
 [A] Breach Response Costs 109
 [B] Cyber Extortion Response..... 109
 [C] Social Engineering Fraud..... 110
 [D] Data Restoration Expense 110
 [E] Computer Hardware Replacement Costs 110
 [F] Business Interruption Losses..... 111
 [G] Service Provider Interruption Loss..... 112
 [H] Crisis Management and Reputational
 Harm..... 112
 § 6:3.2 Third-Party Liability Cyber Coverages..... 113
 [A] Privacy Liability..... 113
 [B] Network Security Liability 114
 [C] Regulatory Proceedings 114
 § 6:3.3 Key Conditions and Exclusions 114
 [A] Reporting, Cooperation, and Consent..... 115
 [B] Failure to Maintain Adequate Network
 Security..... 116
 [C] War Exclusions 116
 [D] Betterment Exclusions 118

Table of Contents

§ 6:4	Other Insurance That May Provide Coverage in Event of a Data Breach	118
§ 6:4.1	Property Insurance.....	119
§ 6:4.2	Commercial General Liability Insurance	120
§ 6:4.3	Crime Insurance.....	122
Chapter 7	Practical Cybersecurity Strategy Guidance for Lawyers	
§ 7:1	Introduction.....	125
§ 7:2	NIST Cybersecurity Framework.....	128
§ 7:2.1	Framework Core.....	130
§ 7:2.2	Framework Implementation Tiers	132
§ 7:2.3	Framework Profile.....	138
§ 7:2.4	Sample Implementation of the Cybersecurity Program Using the CSF.....	139
§ 7:3	“Zero Trust” Cybersecurity for Lawyers	142
Index		151

