

# **Cybersecurity Law, Standards and Regulations**

***2<sup>nd</sup> Edition***

**Tari Schreider**

**C|CISO, CRISC, ITIL® Foundation, MCRP, SSCP**

**Kristen Noakes-Fry, ABCI, Editor**

# Contents

Dedication .....	iii
Acknowledgments.....	iii
Foreword.....	v
Foreword.....	vii
Contents .....	1
Introduction to the 2 <sup>nd</sup> Edition .....	9
Chapter 1 Introduction to Cybersecurity Law .....	13
1.1 Infamous Cybercrimes .....	14
1.2 Cybercrime Taxonomy.....	15
1.3 Civil vs. Criminal Cybersecurity Offenses .....	16
1.3.1 Clarifying the Definition of Cybercrime .....	17
1.3.2 Challenging Your Current Definition of Cybercrime.....	18
1.3.3 Creating a Strong Cybercrime Definition.....	18
1.3.4 Cybercrime Categories in the Incident Response Plan.....	19
1.4 Understanding the Four Basic Elements of Criminal Law .....	20
1.4.1 Mens Rea .....	20
1.4.2 Actus Reus.....	20
1.4.3 Concurrence.....	21
1.4.4 Causation .....	21
1.5 Branches of Law.....	22
1.6 Tort Law.....	22
1.6.2 Strict Liability Tort.....	23
1.6.3 Tort Precedents .....	24
1.7 Cyberlaw Enforcement.....	24

1.7.1 Regulatory Enforcement.....	25
1.7.2 Local Enforcement .....	26
1.7.3 State Enforcement.....	26
1.7.4 Federal Enforcement.....	27
1.7.5 International Enforcement .....	27
1.8 Cybersecurity Law Jurisdiction.....	28
1.8.1 Challenging Jurisdiction.....	29
1.8.2 Extradition .....	30
1.9 Cybercrime and Cyber Tort Punishment.....	32
1.9.1 Cybercrime Punishment .....	32
1.9.2 Cyber Tort Punishment.....	32
<b>Chapter 2 Overview of US Cybersecurity Law .....</b>	<b>37</b>
2.1 Brief History of Resolving Cybersecurity Disputes.....	38
2.1.1 Computer Crime Laws in the Public Sector .....	38
2.1.2 Computer Crime Laws in the Private Sector .....	39
2.1.3 Application of Laws to Cybersecurity.....	39
2.2 Alternative Dispute Resolution (ADR).....	40
2.2.1 Cybersecurity Case Mediation Law .....	41
2.2.2 Cybersecurity Case Arbitration Law .....	42
2.2.3 Cybersecurity Case Dispositive Motion Law .....	43
2.3 Successful Data Breach Lawsuits .....	47
2.4 Duty of Care Doctrine.....	48
2.4.1 Duty to Provide Reasonable Security.....	49
2.4.2 Duty to Reveal Security Breaches .....	49
2.4.3 Duty to Accurately Disclose Safeguards .....	51
2.4.4 Duty to Protect Information.....	51
2.4.5 State-Based Duty of Care Laws.....	52
2.5 Failure to Act Doctrine.....	52
2.5.1 Failure to Act Duty.....	52
2.5.2 Failure to Warn Duty.....	53
2.5.3 Cybersecurity Good Samaritan Law.....	53
2.6 Reasonable Person Doctrine.....	54
2.7 Common Law Duty.....	54
2.8 Criminal Cyberlaw .....	55

2.8.1 Cybercrime Penalties .....	55
2.9 Federal Computer Crime Statutes .....	56
2.9.1 Federal Laws Addressing Computer Security .....	56
2.9.2 The US Code .....	58
2.10 Procedural Law .....	59
2.10.1 Rules of Criminal Procedure .....	60
2.10.2 Rules of Civil Procedure (Cyber Tort) .....	60
2.11 State Computer Crime Laws .....	62
2.11.1 State Ransomware Laws.....	63
2.11.2 Federal Ransomware Laws.....	64
2.11.3 State Cyber Reserve Laws .....	65
2.11.4 State Denial of Service Laws.....	65
2.11.5 State Election Security Legislation.....	66
2.11.6 State Anti-Phishing Laws .....	67
2.11.7 Identity Theft Laws .....	67
2.11.8 State Cyberbullying Laws .....	68
2.12 False Claims Act (FCA).....	69
<b>Chapter 3_Cyber Privacy and Data Protection Law .....</b>	<b>75</b>
3.1 Common Law of Privacy .....	76
3.2 Privacy Laws .....	76
3.2.1 Children's Privacy Laws .....	77
3.2.2 Healthcare Data Privacy Laws .....	80
3.2.3 Federal Privacy Laws .....	87
3.2.4 Cybercrime on Tribal Lands.....	89
3.2.5 State Privacy Laws .....	91
3.2.6 State Chief Information Privacy Officer (CIPO) Laws .....	91
3.2.7 International Privacy Laws .....	92
3.3 Data Breach Laws .....	93
3.3.1 State Data Breach Laws.....	94
3.3.2 Federal Data Breach Laws.....	95
3.3.3 International Data Breach Laws .....	99
3.3.4 General Data Protection Regulation (GDPR).....	102
3.4 Data Breach Litigation .....	105
3.4.1 Injury vs. No-Injury Class Action Lawsuits.....	105

3.4.2 Data Privacy and the US Supreme Court .....	107
3.4.3 Shareholder Derivative Lawsuits.....	109
3.4.4 Securities Fraud Lawsuits.....	110
3.5 Privacy Notice Law .....	111
3.6 Personal Liability .....	112
3.6.1 Directors and Officers Insurance.....	113
3.6.2 Preemptive Liability Protection.....	113
3.6.3 Cybersecurity Whistleblower Protections .....	114
3.7 Data Disposal Laws.....	115
3.8 Electronic Wiretap Laws.....	116
3.9 Digital Assistant Privacy Issues .....	117
3.10 Social Media Privacy .....	117
3.11 Event Data Recorder (EDR) Privacy .....	118
3.12 Automated License Plate Reader (ALPR) Privacy .....	120
<b>Chapter 4 Cryptography and Digital Forensics Law .....</b>	<b>127</b>
4.1 Brief Overview of Cryptography .....	128
4.2 Cryptography Law.....	129
4.2.1 Export Control Laws .....	130
4.2.2 Import Control Laws .....	132
4.2.3 Cryptography Patent Infringement.....	133
4.2.4 Search and Seizure of Encrypted Data .....	136
4.2.5 Encryption Personal Use Exemption.....	138
4.3 State Encryption Laws .....	139
4.3.1 State Encryption Safe Harbor Provision.....	139
4.4 Fifth Amendment and Data Encryption .....	140
4.5 Laws and Regulations Requiring Encryption.....	141
4.6 International Cryptography Law Perspective.....	142
4.7 International Key Disclosure Law.....	143
4.8 Legal Aspects of Digital Forensics .....	144
4.8.1 Preservation Order.....	144
4.8.2 Digital Best Evidence Rule.....	145
4.8.3 Digital Chain of Custody.....	146
4.8.4 Digital Data Admissibility in Court.....	147
4.8.5 Digital Evidence Spoliation.....	147

4.8.6 Fourth Amendment Rights and Digital Evidence.....	148
4.8.7 Expert Witnesses .....	149
4.8.8 Security Consultant Client Privilege .....	149
4.9 State Digital Forensics Law .....	150
4.10 The CLOUD Act.....	151
4.11 Emerging Data Encryption Laws .....	152
4.11.1 Ensuring National Constitutional Rights for Your Private Telecommunications (ENCRYPT) Act.....	152
4.11.2 Secure Data Act.....	152
4.12 Biometrics Law .....	152
4.13 Genetic Information Privacy Laws .....	154
<b>Chapter 5 Acts, Standards &amp; Regulations.....</b>	<b>159</b>
5.1 Basel III Accord .....	160
5.2 Chemical Facility Anti-Terrorism Standards (CFATS) Act .....	161
5.3 Defense Federal Acquisition Regulations Supplement (DFARS) .....	163
5.3.1 Minimum Requirements for DFARS .....	164
5.3.2 Termination of Contracts and Penalties for Non-Compliance .....	165
5.4 Directive on Security of Network and Information Systems NIS Directive.....	165
5.5 European Union Cybersecurity Act .....	166
5.6 Family Educational Rights and Privacy Act (FERPA).....	167
5.7 Federal Financial Institutions Examination Council (FFIEC) .....	168
5.8 Federal Information Security Management Act (FISMA).....	168
5.9 Financial Industry Regulatory Authority (FINRA) Rules .....	169
5.10 Food and Drug Administration Code of Federal Regulations Title 21 Part 11.....	170
5.10.1 ALCOA Model.....	171
5.11 Health Information Technology for Economic and Clinical Health Act (HITECH).....	172
5.12 Health Insurance Portability and Accountability Act (HIPAA).....	173
5.13 Joint Commission on the Accreditation of Healthcare Organizations (JCAHO).....	173
5.14 North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP).....	176
5.15 Payment Card Industry– Data Security Standard (PCI-DSS) .....	177
5.16 Sarbanes Oxley Act (SOX) .....	178
5.16.1 Cybersecurity Flaw Whistleblower Protection.....	179
5.17 Standards .....	179
5.17.1 International Organization for Standardization (ISO) Security Standards.....	180

Chapter 6 Creating a Cybersecurity Law Program .....	<b>195</b>
6.1 Cybersecurity Law Program.....	196
6.1.1 Model.....	196
6.1.2 Architecture .....	199
6.1.3 Program Staffing and Roles.....	200
6.1.4 Program Policies.....	203
6.1.5 Program Procedures.....	206
6.1.6 Program Technology .....	208
6.1.7 Mapping Legal Requirements to Controls.....	212
6.1.8 ISO/IEC 27002 on Compliance Controls .....	214
6.2 Cyber Liability Insurance.....	214
6.2.1 Coverage Categories.....	215
6.2.2 Policy Restrictions.....	217
6.2.3 Policy Value .....	217
6.2.4 Policy Cost.....	218
6.2.5 Policy Claims.....	218
6.2.6 Policy Claim Disputes .....	219
6.2.7 Policy Lawsuits.....	219
6.2.8 Act of War Defense .....	222
6.2.9 Insurable vs Uninsurable Risk.....	222
6.2.10 Cyber Risk Insurance Pools.....	223
6.2.11 Silent Cyber Risk Insurance .....	223
6.3 Data Breach Worksheet.....	224
6.3.1 Data Breach Calculators .....	224
6.4 Compliance Auditing .....	225
6.4.1 Critical Audit Matters (CAM) .....	226
6.4.2 Internal vs. External Auditing .....	227
6.4.3 Auditing Associations.....	229
Chapter 7 Future Developments in Cybersecurity Law.....	<b>235</b>
7.1 Future of Cybersecurity Legislation.....	236
7.1.1 Constutionality of Cybersecurity Law.....	236
7.2 Impact of Technology on Cybersecurity Law.....	237
7.2.1 Legal Implications of the Internet of Things (IoT).....	237
7.2.2 Legal Implications of Big Data .....	238

7.2.3 Legal Implications of Cloud Computing .....	239
7.2.4 Legal Implications of Security Testing .....	240
7.3 Future US Cybersecurity Legislation.....	242
7.4 US Foreign Policy on Cybersecurity.....	244
7.5 National Association of Insurance Commissioners (NAIC) Model Cybersecurity Law ..	246
7.6 Harmonization of International Cybersecurity Laws .....	248
7.6.1 Cybersecurity Law and Trade Pacts .....	248
7.6.2 Harmonization of Cybersecurity and Privacy Law .....	249
7.6.3 Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) Cybersecurity Framework .....	249
7.6.4 Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System .....	252
7.6.5 US-Mexico-Canada Agreement (USMCA).....	254
7.6.6 Cyberbalkanization Laws .....	255
7.6.7 Data Localization Laws .....	255
7.6.8 Singapore Payment Services Act.....	257
7.7 Aligning the Law of the Sea to Cybersecurity Law .....	258
7.8 Cybersecurity Law in Outer Space.....	259
7.9 The Law of Armed Conflict in Cyberwar .....	260
7.10 North Atlantic Treaty Organization (NATO) Cyberlaw Stance .....	261
7.11 United Nations – Universal Cybersecurity Legal Framework .....	262
7.12 International Treaties on Cybersecurity .....	263
7.13 Brexit Impact on European Union Cybersecurity Law .....	264
7.14 G7 Perspective on Cybercrime.....	265
<b>Appendix A.....</b>	<b>273</b>
<b>Useful Checklists and Information.....</b>	<b>273</b>
<b>Index.....</b>	<b>283</b>
<b>Credits.....</b>	<b>310</b>
<b>About the Author .....</b>	<b>314</b>