

TABLE OF CONTENTS

Introduction	1
Chapter 1. What Is (Cyber)Security?	5
A. Insecurity in the Wild	5
1. Cybersecurity’s Wild History	5
2. Cybersecurity’s Wild Present.....	7
3. Cybersecurity’s Wild West (or, Cybersecurity is Hard)	11
Questions	13
B. Assets & Threats: Central Cybersecurity Concepts.....	14
Questions	17
C. (“Cyber”)Security “Law”?	17
Questions	21
D. A Note on Terminology and Navigating This Text	21
Peiter Zatko a/k/a Mudge, Unexpected Stories from a Hacker Inside the Government	22
Dan Geer, <i>T.S. Kuhn Revisited</i>	26
Chapter 2. Security, Privacy, & “Security vs. Privacy”	29
A. Defining Cybersecurity, as Risk	29
B. Defining Cybersecurity, as Process.....	35
C. Privacy (Is Not Security).....	37
Warren and Brandeis, <i>The Right to Privacy</i>	38
Daniel J. Solove, <i>A Taxonomy of Privacy</i>	43
1. Which, Naturally, Begs the Question—What if Other Societies View or Construct Privacy Differently?	49
James Q. Whitman, <i>The Two Western Cultures of Privacy</i>	50
Questions	57
D. Privacy and Security	57
Gus Hurwitz, <i>Privacy and Cybersecurity Are Not the Same, and Americans Care Far More About Cybersecurity</i>	58
Derek Bambauer, <i>Privacy vs. Security</i>	60
David Thaw, <i>Disambiguating “Cyber”</i>	65
Questions	67
Chapter 3. A Basic Introduction to Cybersecurity Risk	69
A. Risk Types.....	70
Charlotte A. Tschider, <i>Experimenting with Privacy: Driving Efficiency through a State-Informed Federal Data Breach Notification and Data Protection Law</i>	72
Daniel J. Solove & Woodrow Hartzog, <i>The FTC and the New Common Law of Privacy</i>	74
Justin (Gus) Hurwitz, <i>Data Security and the FTC’s UnCommon Law</i>	79

Questions	82
B. Risk Governance.....	83
Questions	85
C. Risk Assessment and Risk Rating	85
Questions	89
Chapter 4. The Cybersecurity Ecosystem	91
A. Hackers and Attackers.....	92
Questions	94
B. Attacker Motivations	94
“The Hacker Manifesto”	95
Public Message from TheHackerGiraffe	97
David Thaw, <i>Criminalizing Hacking, Not Dating</i>	97
Justin (Gus) Hurwitz, <i>Response to McGeeveran’s The Duty of Data Security: Not the Objective Duty He Wants, Maybe the Subjective Duty We Need</i>	104
Questions	107
1. The Special Case of Election Hacking.....	107
David Thaw, <i>From Russia With Love</i>	107
Questions	112
C. The Overall Security Ecosystem	113
Justin (Gus) Hurwitz, <i>Cyberensuring Security</i>	113
Marc Andreessen, <i>Why Software Is Eating the World</i>	117
Questions	118
D. The “Security Mindset”	118
1. The Science of Cybersecurity	119
Mulligan & Schneider, <i>Doctrine for Cybersecurity</i>	121
Sales, <i>Regulating Cyber-Security</i>	126
Anderson & Moore, <i>Information Security: Where Computer Science, Economics and Psychology Meet</i>	129
Questions	133
2. Thinking Like an Attacker	133
3. Thinking Like a Target	142
Interview: <i>Hacker OPSEC with the Grugq</i>	144
Questions	146
4. The Business of Cybersecurity	146
Ben Collier, Richard Clayton, Alice Hutchings, and Daniel R. Thomas, <i>Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies</i>	147
Questions	149
Chapter 5. Technical Foundations.....	151
A. Computers.....	151
1. Searching & Sorting—Complexity	151
2. Computability and Computers	153
3. Algorithms	154

Questions	159
4. The Halting Problem	159
5. Modularity	161
Christopher Yoo, <i>Modularity Theory and Internet Regulation</i>	161
Questions	168
B. Networks	168
1. Modules and Networks	169
Questions	170
2. Early Computers and Networks	170
a. Computers	170
b. Multi-User Computers and Terminals	171
3. Packet Switching	176
a. The Need for Packet Switching	176
b. Putting the Switching in Packet Switching	180
4. The Internet	183
C. Identity, Authentication, and Encryption	184
1. Identity	185
2. Authentication	186
3. Encryption	188
Gus Hurwitz, <i>Understanding Encryption: No Longer Just about</i> <i>Sending Secret Messages</i>	189
4. Encryption Is Not Security	194
Bruce Schneier, <i>Security Pitfalls in Cryptography</i>	195
Ross Anderson, <i>Why Cryptosystems Fail</i>	197
Questions	200
Chapter 6. Legal Foundations	203
A. Legal Structures	204
1. Structure of (Representative Republican) Government	204
Federalist No. 47, <i>The Particular Structure of the New</i> <i>Government and the Distribution of Power Among Its</i> <i>Different Parts</i>	207
Questions	209
2. Structure of Law	209
a. Legislative Choices (“Black-Letter Law”)	211
b. Interpretive Doctrine (“Common Law”)	213
3. Sources of Law	214
a. Constitutional Choices	214
b. Statutes	214
Derek Bambauer, <i>Rules, Standards, and Geeks</i>	216
c. Administrative Law and Regulations (“Agency Choices”)	221
Questions	222
d. Judicial Interpretation (“Common Law”)	222
Questions	226
e. Agency Interpretation (“Regulatory Adjudications and the <i>“(Un)Common Law”</i>)	226

B.	Legal Principles	227
1.	The Mechanism and Purpose of the Law	228
	Oliver Wendel Holmes, <i>The Path of the Law</i>	228
	Questions	233
2.	Who Bears the Burden of Avoiding Harm	233
	Gus Hurwitz, <i>The Technological Problem of Social Cost</i>	233
	Guido Calabresi & A. Douglas Melamed, <i>Property Rules, Liability Rules, and Inalienability: One View of the Cathedral</i>	236
	Questions	238
3.	A More Direct Approach: Assigning Liability with Strict Liability	239
	Michael Scott, <i>Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?</i>	239
	Gus Hurwitz, <i>Cyberensuring Security</i>	245
	Questions	251
C.	Substantive Categories of Law (Private Law, Criminal Law, and Public Law)	251
	Chapter 7. Business Foundations	253
A.	Introduction to the Organization	253
1.	Organizational Type	253
a.	Businesses Selling Goods	254
b.	Services Businesses	256
c.	Third Parties	258
2.	Organizations and Their Regulators	260
	Questions	266
B.	A Bit More About Transaction Costs	266
C.	Agency and Responsibilities	267
1.	Agency Cost	268
	Zohar Goshen & Richard Squire, <i>Principal Costs: A New Theory for Corporate Law and Governance</i>	269
2.	Management Roles/Responsibilities	271
3.	The Business Judgment Rule	272
	Charles Cresson Wood, <i>Solving the Information Security & Privacy Crisis by Expanding the Scope of Top Management Personal Liability</i>	273
	Chapter 8. Why Cybersecurity Is Hard	277
A.	The Problem of Complexity, or the “Halting” Problem	278
	Jeffrey M. Lipshaw, <i>Halting, Intuition, Heuristics, and Action: Alan Turing and the Theoretical Constraints of AI Lawyering</i>	280
1.	AI Distributed Risk Example	283
B.	The Problem of Changing, Evolving Environments	284
1.	Risks of Outsourcing to the Cloud Example	286
	Questions	287

C.	The Problem of Fit-for-Purpose Security	288
1.	Industrial Manufacturing Example 1	289
2.	Industrial Manufacturing Example 2	290
	Questions	290
D.	The Problem of Technical Debt and Complexity as-Implemented.....	291
E.	The Problem of Intransigence and Writing Laws for Cybersecurity	292
1.	Making Risk-Based Choices Example.....	292
2.	Why Cybersecurity Laws Are Written Broadly	293
	Charlotte A. Tschider, <i>Enhancing Cybersecurity for the Digital</i>	
	<i>Health Marketplace</i>	295
	David Thaw, <i>The Efficacy of Cybersecurity Regulation</i>	300
	David Thaw, <i>Cybersecurity Stovepiping</i>	305
	Questions	307
	Chapter 9. Engineering for Risk.....	309
A.	Understanding the Development and Engineering Mentalities	309
	Clayton M. Christensen, <i>Innovator’s Dilemma: When New</i>	
	<i>Technologies Cause Great Firms to Fail</i>	310
	Bill Gates, <i>‘Internet Tidal Wave’ Memo</i>	312
	Andrew Russell, <i>‘Rough Consensus and Running Code’ and the</i>	
	<i>Internet-OSI Standards War</i>	316
	Questions	321
B.	Business Influence on Technology Spend.....	322
C.	The Software Development Lifecycle.....	323
	Jukka Ruohonen & Luca Allodi, <i>A Bug Bounty Perspective on the</i>	
	<i>Disclosure of Web Vulnerabilities</i>	326
1.	Alternative Development Models	328
	Principles behind the Agile Manifesto	328
	Letter from Mark Zuckerberg.....	329
2.	Security by Design.....	332
	Questions	335
D.	Technical Debt and Deferred Costs.....	336
	Craig Timberg, <i>The long life of a quick ‘fix’: Internet protocol from</i>	
	<i>1989 leaves data vulnerable to hijackers</i>	338
	Rajiv Banker, Yi Liang & Narayan Ramasubbu, <i>Technical Debt and</i>	
	<i>Firm Performance</i>	341
	Bill Gates, <i>‘Trustworthy Computing’ Memo</i>	343
	Joel Spolsky, <i>Things You Should Never Do, Part I</i>	344
	Steven M. Bellovin, <i>Patching is Hard</i>	346
	Questions	348
E.	Considering the Interdisciplinary Struggles of Cybersecurity.....	349
	Bruce Schneier, <i>Technologists vs. Policy Makers</i>	349
	Chapter 10. Risk and the Law	353
A.	The Common Law of Tort	355
1.	Types of Tort: Negligence vs. Products Liability	356

2.	Standing	358
	Felix Wu, <i>How Privacy Distorted Standing Law</i>	358
3.	Causation	362
	Rebecca Crootof, <i>The Internet of Torts</i>	365
4.	Liability Assignment	376
5.	Economic Loss Doctrine	378
	David W. Opderbeck, <i>Cybersecurity, Data Breaches, and the Economic Loss Doctrine</i>	378
	Questions	384
B.	The Common Law of Contracts	384
1.	B2C Contracts	386
	a. Service Contracts—Terms of Use	386
	b. Goods Contracts—“Wrapped” Agreements	386
2.	Special Problems	389
	a. Common Law Problems	389
3.	B2B Contracts	390
	Questions	392
C.	Shareholder Derivative Lawsuits	393
	Lawrence J. Trautman & Peter Ormerod, <i>Corporate Directors’ and Officers’ Cybersecurity Standard of Care: The Yahoo Data Breach</i>	393
	Questions	401
D.	State Statutes & State Attorneys General	401
	<i>The New York Department of Financial Services Cybersecurity Regulation</i>	402
	<i>State of California Information Privacy of Connected Devices</i>	410
	<i>Minnesota Plastic Card Security Act</i>	412
	Questions	414
E.	General Regulatory Regimes	414
1.	Sector-Specific Federal Statutes	414
	a. HIPAA Security Rules (1996, Security Rule Adopted in 2003, Updated in 2007)	414
	<i>The Health Insurance Portability and Accountability Act of 1996</i>	415
2.	Broad Federal Statutes	424
	<i>The Federal Information Security Management Act</i>	424
	a. The U.S. Securities and Exchange Commission	430
	Gilles Hilary, Benjamin Segal & May H. Zhang, <i>Cyber-Risk Disclosure: Who Cares?</i>	430
3.	Regulatory Tools	436
	<i>LabMD, Inc. v. Federal Trade Commission</i>	437
	Justin (Gus) Hurwitz, <i>Response to McGeeveran’s The Duty of Data Security: Not the Objective Duty He Wants, Maybe the Subjective Duty We Need</i>	443
	Questions	448
F.	Criminal Statutes	449
	Jeff Kosseff, <i>Defining Cybersecurity Law</i>	449

Questions	456
Chapter 11. Business Approaches to Cybersecurity Risk	457
A. Governance	457
1. Enterprise Risk Management.....	458
2. Additional Compliance and Risk Management Functions	460
Questions	461
B. Policy Management.....	462
Scott Shackelford, Andrew Proia, Brenton Martell & Amanda Craig, <i>Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices</i>	463
1. The Information Security Policy Library	469
C. Risk Assessment.....	473
Questions	476
D. Risk Rating and Decisioning	476
1. Risk Rating Procedures.....	478
Questions	479
2. Risk Decisioning	480
Questions	482
3. Governance Review	482
E. Third Party Management	483
1. Introduction to Third-Party Risk	483
Tobi A. West & Aeron Zentner, <i>Threats and Major Data Breaches: Securing Third-Party Vendors</i>	483
2. Third-Party Risk Assessments	487
3. Third-Party Contracts.....	489
F. Industry Standards	493
1. NIST Cybersecurity Framework	494
2. PCI-DSS	498
3. HITRUST	498
4. Third-Party Certification	499
5. Industry Frameworks and Certifications	499
G. The Incident Response Process	500
1. Incident Response Planning	501
2. Detect and Contain.....	503
3. Notification	504
4. Recover and Improve.....	506
Questions	507
H. In Conclusion	507
Chapter 12. Alternative Modalities of Risk Regulation.....	509
A. Regulating Process, Not Outcomes	509
Cary Coglianese and David Lazer, <i>Management-Based Regulation: Prescribing Private Management Goals to Achieve Public Goals</i>	511

Questions	522
B. Alternative Governmental Regulation.....	522
David Thaw, <i>Data Breach (Regulatory) Effects</i>	523
Questions	529
C. Self-Regulation	529
Questions	530
D. Public-Private Partnerships	530
Justin (Gus) Hurwitz, <i>Regulation as Partnership</i>	531
David Thaw, <i>Enlightened Regulatory Capture</i>	540
Questions	555
E. Insurance	555
Gus Hurwitz, <i>Cyberensuring Security</i>	557
Questions	564
F. Concluding Thoughts and Questions	564
Questions	564
INDEX.....	567