

Contents

About the Authors	ix
Acknowledgments	xi
CHAPTER 1	
Counting the Costs of Cyber Attacks	1
1.1 Anatomy of a Data Exfiltration Attack	1
1.2 A Modern Scourge	7
1.3 Cyber Catastrophes	12
1.4 Societal Cyber Threats	19
1.5 Cyber Risk	21
1.6 How Much Does Cyber Risk Cost Our Society?	24
Endnotes	30
CHAPTER 2	
Preparing for Cyber Attacks	33
2.1 Cyber Loss Processes	33
2.2 Data Exfiltration	34
2.3 Contagious Malware Infection	41
2.4 Denial of Service Attacks	56
2.5 Financial Theft	63
2.6 Failures of Counterparties or Suppliers	68
Endnotes	78
CHAPTER 3	
Cyber Enters the Physical World	81
3.1 A Brief History of Cyber-physical Interactions	81
3.2 Hacking Attacks on Cyber-physical Systems	83
3.3 Components of Cyber-physical Systems	86
3.4 How to Subvert Cyber-physical Systems	88

3.5	How to Cause Damage Remotely	91
3.6	Using Compromises to Take Control	92
3.7	Operating Compromised Systems	93
3.8	Expect the Unexpected	95
3.9	Smart Devices and the Internet of Things	99
	Endnotes	101
CHAPTER 4		
	Ghosts in the Code	103
4.1	All Software Has Errors	103
4.2	Vulnerabilities, Exploits, and Zero Days	104
4.3	Counting Vulnerabilities	108
4.4	Vulnerability Management	113
4.5	International Cyber Response and Defense	118
	Endnotes	122
CHAPTER 5		
	Know Your Enemy	125
5.1	Hackers	125
5.2	Taxonomy of Threat Actors	127
5.3	The Insider Threat	143
5.4	Threat Actors and Cyber Risk	145
5.5	Hackonomics	147
	Endnotes	151
CHAPTER 6		
	Measuring the Cyber Threat	153
6.1	Measurement and Management	153
6.2	Cyber Threat Metrics	158
6.3	Measuring the Threat for an Organization	162
6.4	The Likelihood of Major Cyber Attacks	170
	Endnotes	182
CHAPTER 7		
	Rules, Regulations, and Law Enforcement	183
7.1	Cyber Laws	183
7.2	US Cyber Laws	186

7.3	EU General Data Protection Regulation (GDPR)	190
7.4	Regulation of Cyber Insurance	192
7.5	A Changing Legal Landscape	194
7.6	Compliance and Law Enforcement	196
7.7	Law Enforcement and Cyber Crime	199
	Endnotes	205
CHAPTER 8		
	The Cyber-Resilient Organization	207
8.1	Changing Approaches to Risk Management	207
8.2	Incident Response and Crisis Management	208
8.3	Resilience Engineering	212
8.4	Attributes of a Cyber-resilient Organization	214
8.5	Incident Response Planning	218
8.6	Resilient Security Solutions	219
8.7	Financial Resilience	225
	Endnotes	234
CHAPTER 9		
	Cyber Insurance	235
9.1	Buying Cyber Insurance	235
9.2	The Cyber Insurance Market	244
9.3	Cyber Catastrophe Risk	248
9.4	Managing Portfolios of Cyber Insurance	251
9.5	Cyber Insurance Underwriting	258
9.6	Cyber Insurance and Risk Management	263
	Endnotes	264
CHAPTER 10		
	Security Economics and Strategies	267
10.1	Cost-Effectiveness of Security Enhancements	267
10.2	Cyber Security Budgets	271
10.3	Security Strategies for Society	276
10.4	Strategies of Cyber Attack	283
10.5	Strategies of National Cyber Defense	289
	Endnotes	294

CHAPTER 11	
Ten Cyber Problems	295
11.1 Setting Problems	295
1 The Canal Safety Decision Problem	298
2 The Software Dependency Problem	300
3 The Vulnerability Inheritance Problem	301
4 The Vulnerability Count Problem	302
5 The Malware Overlap Problem	303
6 The Vulnerability Lifespan Problem	304
7 The Binary Similarity Problem	304
8 The Virus Modification Problem	306
9 The Cyber Criminal's Dilemma Problem	306
10 The Security Verification Problem	307
Endnotes	308
CHAPTER 12	
Cyber Future	309
12.1 Cybergeddon	309
12.2 Cybertopia	315
12.3 Future Technology Trends	321
12.4 Getting the Cyber Risk Future We Want	328
Endnotes	331
References	333
Index	355