

Contents

Foreword	ix
Preface	xi
Acknowledgments	xv
1 Introduction	1
1.1 What Is Cyber Security?	1
1.2 What Is Cyber Security Policy?	3
1.3 Domains of Cyber Security Policy	7
1.3.1 Laws and Regulations	7
1.3.2 Enterprise Policy	9
1.3.3 Technology Operations	10
1.3.4 Technology Configuration	10
1.4 Strategy versus Policy	11
2 Cyber Security Evolution	15
2.1 Productivity	15
2.2 Internet	21
2.3 e-Commerce	28
2.4 Countermeasures	34
2.5 Challenges	37
3 Cyber Security Objectives	39
3.1 Cyber Security Metrics	40
3.2 Security Management Goals	45
3.3 Counting Vulnerabilities	49
3.4 Security Frameworks	51
3.4.1 e-Commerce Systems	52

3.4.2	Industrial Control Systems	57
3.4.3	Personal Mobile Devices	62
3.5	Security Policy Objectives	67
4	Guidance for Decision Makers	69
4.1	Tone at the Top	69
4.2	Policy as a Project	71
4.3	Cyber Security Management	73
4.3.1	Arriving at Goals	74
4.3.2	Cyber Security Documentation	77
4.4	Using the Catalog	79
5	The Catalog Approach	83
5.1	Catalog Format	87
5.2	Cyber Security Policy Taxonomy	89
6	Cyber Security Policy Catalog	93
6.1	Cyber Governance Issues	94
6.1.1	Net Neutrality	95
6.1.2	Internet Names and Numbers	96
6.1.3	Copyrights and Trademarks	103
6.1.4	Email and Messaging	107
6.2	Cyber User Issues	112
6.2.1	Malvertising	116
6.2.2	Impersonation	117
6.2.3	Appropriate Use	121
6.2.4	Cyber Crime	125
6.2.5	Geolocation	136
6.2.6	Privacy	138
6.3	Cyber Conflict Issues	140
6.3.1	Intellectual Property Theft	144
6.3.2	Cyber Espionage	145
6.3.3	Cyber Sabotage	150
6.3.4	Cyber Warfare	150
6.4	Cyber Management Issues	155
6.4.1	Fiduciary Responsibility	162
6.4.2	Risk Management	163
6.4.3	Professional Certification	171
6.4.4	Supply Chain	172
6.4.5	Security Principles	175
6.4.6	Research and Development	185
6.5	Cyber Infrastructure Issues	186
6.5.1	Banking and Finance	190

6.5.2	Health Care	194
6.5.3	Industrial Control Systems	197
7	One Government's Approach to Cyber Security Policy	211
7.1	U.S. Federal Cyber Security Strategy	211
7.2	A Brief History of Cyber Security Public Policy Development in the U.S. Federal Government	212
7.2.1	The Bombing of New York's World Trade Center on February 26, 1993	212
7.2.2	Cyber Attacks against the United States Air Force, March–May 1994: Targeting the Pentagon	213
7.2.3	The Citibank Caper, June–October, 1994: How to Catch a Hacker	214
7.2.4	Murrah Federal Building, Oklahoma City—April 19, 1995: Major Terrorism Events and Their U.S. Outcomes	215
7.2.5	President's Commission on Critical Infrastructure Protection—1996	216
7.2.6	Presidential Decision Directive 63—1998	218
7.2.7	National Infrastructure Protection Center (NIPC) and ISACs—1998	219
7.2.8	Eligible Receiver—1997	219
7.2.9	Solar Sunrise—1998	220
7.2.10	Joint Task Force—Computer Network Defense (JTF-CND)—1998	221
7.2.11	Terrorist Attacks against the United States—September 11, 2001 Effects of Catastrophic Events on Transportation System Management and Operations	222
7.2.12	U.S. Government Response to the September 11, 2001 Terrorist Attacks	224
7.2.13	Homeland Security Presidential Directives	226
7.2.14	National Strategies	227
7.3	The Rise of Cyber Crime	230
7.4	Espionage and Nation-State Actions	232
7.5	Policy Response to Growing Espionage Threats: U.S. Cyber Command	233

7.6	Congressional Action	235
7.7	Summary	236
8	Conclusion	239
	Glossary	243
	References	255
	Index	267