
Contents

Preface xv

Authors' Notes xvii

Synopsis xix

Acknowledgments xxiii

Authors xxv

1 Introduction to Critical Infrastructure Assurance and Protection 1

1.1 Introduction 1

1.2 What Is Critical Infrastructure? 3

1.3 What Is the Private Sector? 4

1.4 What Is the Public Sector? 5

1.5 What Is CIP? 7

1.6 What Is CIA? 8

1.7 What Are Public-Private Partnerships? 11

1.8 Critical Infrastructure Functions 11

1.9 Evolution of Critical Infrastructure 12

2 Demand, Capacity, Fragility, and the Emergence of Networks 15

2.1 Introduction 15

2.2 What Are We Trying to Protect? The Concept of Capacity 15

2.3 Demand: The Reason for Capacity 16

2.3.1 The Concept of Performance 16

2.3.2 Local Impact and the Influence on Capacity 17

2.3.3 Results of a Local Impact in the Immediate Sense 18

2.3.4 Relevance to CIP 20

2.3.5 Push, Pull, Lag, and Delay in the Network Environment ... 20

2.4 At the Regional (Small System) Level 21

2.4.1 Influence at the Small System Level 21

2.4.2 Current Efforts and Research 22

2.4.3 The Interdependency Hydra 23

2.4.4 Network Fragmentation and Dissolution 23

2.5	Cyberterrorism	24	5.6	The Cloud as an Amplifier.....	84
2.5.1	The Pendulum of Convergence	26	5.7	Clouds and Concealed Conduits	85
2.5.2	Convergence and the Understanding of Threat	27	5.8	Linking the Trusted Computing Base and User Communities.....	87
2.5.3	Setting the Stage for Fragility.....	29	5.9	Barriers to Information Sharing.....	90
2.5.4	Fragility and Destabilization of Systems	31	5.10	The Rise of Open Sources.....	91
2.5.5	Fragmentation and Dissolution of Networks.....	31	5.11	Open-Source Information and Intelligence	92
2.6	Dissolution and Convergence: An Emerging Risk	32	5.12	An Approach to Information Sharing—The Consequence-Benefit Ratio.....	93
2.6.1	Convergence, Network Expansion, Open Architecture, and Common Criteria.....	33			
2.7	Marking the Journey	33	6	Critical Infrastructure Information	95
2.7.1	Overview	34	6.1	Introduction	95
2.7.2	Legislation: 107th Congress (2001–2002).....	34	6.2	What Is Critical Infrastructure Information (CII)?	96
2.7.3	Legislation: 108th Congress to 109th Congress	35	6.3	How Does the Government Interpret CII?	98
2.7.4	The State Today: A Recap	35	6.4	Exemption 3 of the FOIA.....	100
2.7.5	Research and Understanding	36	6.5	Exemption 4 of the FOIA.....	102
2.8	Authors' Notes.....	36	6.6	Section 214 of the Homeland Security Act.....	102
3	Beyond National Frameworks	37	6.7	Enforcement of Section 214 of the Homeland Security Act.....	105
3.1	Introduction	37	6.8	What Does “Sensitive but Unclassified” Mean?	106
3.2	Meeting the Dragons on the Map	37	6.9	Information Handling Procedures.....	108
3.3	Who Owns the Treasure?	41	6.10	Freedom of Information Act.....	109
3.4	What Value?	42	6.11	Need to Know	109
3.5	Target Audiences	45	6.12	“For Official Use Only”	111
3.6	Expanding Beyond the Traditional Response	48	6.13	Enforcement of FOUO Information.....	112
3.7	Areas of Potential Risk or Concern.....	56	6.14	Reviewing Web Site Content	112
4	Public-Private Partnerships.....	59	6.15	Export-Controlled Information	116
4.1	Introduction	59	6.16	Enforcement of Export-Controlled Information	117
4.2	What Is a Public-Private Partnership (P3)?	59	6.17	Within the Contracting Process	117
4.3	The P3 Spectrum.....	60	6.18	Enforcement of Source Selection Data.....	118
4.4	Establishment of New Capacity.....	62	6.19	Privacy Information.....	119
4.5	Maintenance of Existing Capacity.....	64	6.20	Enforcement of Privacy Information	120
4.6	The Coming Financial Crisis.....	65	6.21	Unclassified Controlled Nuclear Information	121
4.7	Other Forms of Public-Private Cooperation and the Erosion of Governance	67	6.22	Enforcement of UCNI.....	122
4.8	Balancing Points.....	69	6.23	Critical Energy Infrastructure Information	122
4.9	Authors' Notes.....	71	6.24	Enforcement of CEII.....	123
5	The Reinvention of Information Sharing and Intelligence.....	73	6.25	Controlled Unclassified Information	123
5.1	Introduction	73	6.26	Lessons Learned Programs.....	125
5.2	Data vs. Information vs. Intelligence	74	6.27	Infragard	125
5.3	The Importance of Background to Context	75	6.28	Sensitive Unclassified Nonsafeguards Information (SUNSI)	126
5.4	Context Affecting Sensitivity.....	78	6.29	Safeguards Information (SGI)	127
5.5	Enter the Cloud.....	82	6.30	Authors' Notes.....	127
			7	Supervisory Control and Data Acquisition	129
			7.1	Introduction	129
			7.2	What Are Control Systems?.....	129

7.3	Types of Control Systems	131
7.4	Components of Control Systems	131
7.5	Vulnerability Concerns about Control Systems	132
7.6	Adoption of Standardized Technologies with Known Vulnerabilities	133
7.7	Connectivity of Control Systems to Unsecured Networks	134
7.8	Implementation Constraints of Existing Security Technologies	134
7.9	Insecure Connectivity to Control Systems	136
7.10	Publicly Available Information about Control Systems	136
7.11	Control Systems May Be Vulnerable to Attack	137
7.12	Consequences Resulting from Control System Compromises	138
7.13	Wardialing	138
7.13.1	Goals of Wardialing	139
7.13.2	Threats Resulting from Wardialing	140
7.14	Wardriving	140
7.15	Warwalking	141
7.16	Threats Resulting from Control System Attacks	141
7.17	Issues in Securing Control Systems	142
7.18	Methods of Securing Control Systems	143
7.19	Technology Research Initiatives of Control Systems	145
7.20	Security Awareness and Information Sharing Initiatives	146
7.21	Process and Security Control Initiatives	147
7.22	Securing Control Systems	149
7.23	Implement Auditing Controls	149
7.24	Develop Policy Management and Control Mechanisms	150
7.25	Control Systems Architecture Development	150
7.26	Segment Networks between Control Systems and Corporate Enterprise	150
7.27	Develop Methodologies for Exception Tracking	151
7.28	Define an Incident Response Plan	151
7.29	Similarities between Sectors	152
7.30	US Computer Emergency Readiness Team CSSP	152
7.31	Control Systems Cyber Security Evaluation Tool (CSET)	154
7.32	SCADA Community Challenges	156
7.33	The Future of SCADA	157
7.34	SCADA Resources	158
7.34.1	Blogs	158
7.34.2	SCADASEC Mailing List	158
7.34.3	Online SCADA and SCADA Security Resources	159
7.35	Authors' Notes	159

8	The Evolution of Physical Security	161
8.1	Introduction	161
8.2	Core Offices Tested	162
8.3	First Responder	168
8.4	First Responder Classifications	170
8.5	Guideline Classifications	170
8.6	Example: North American Emergency Response Guidebook	171
8.7	Awareness-Level Guidelines	172
8.7.1	Recognize Incidents	173
8.7.2	Basic Protocols	173
8.7.3	Know Self-Protection Measures	174
8.7.4	Know Procedures for Protecting Incident Scenes	175
8.7.5	Know Scene Security and Control Procedures	176
8.7.6	Know How to Use Equipment Properly	177
8.8	Performance-Level Guidelines	178
8.9	Operational Levels Defined	178
8.10	Level A: Operations Level	179
8.10.1	Have Successfully Completed Awareness-Level Training	179
8.10.2	Know ICS Awareness Procedures	180
8.10.3	Know Self-Protection and Rescue Measures	181
8.11	Level B: Technician Level	182
8.11.1	Know WMD Procedures	182
8.11.2	Have Successfully Completed Awareness and Performance-Level Training	183
8.11.3	Know Self-Protection, Rescue, and Evacuation Procedures	184
8.11.4	Know and Follow Procedures for Performing Specialized Tasks	186
8.11.5	Know ICS Performance Procedures	188
8.11.6	Planning and Management-Level Guidelines	189
8.11.7	Successfully Completed Awareness, Performance, and Management Training	190
8.11.8	Know ICS Management Procedures	190
8.12	Know Protocols to Secure, Mitigate, and Remove HAZMAT	191
8.13	Additional Protective Measures	193
8.14	Understand the Development of the IAP	193
8.15	Know and Follow Procedures for Protecting a Potential Crime Scene	194
8.16	Know Department Protocols for Medical Response Personnel	195
8.17	National Fire Prevention Association 472	195

8.18	Osha Hazardous Waste Operations and Emergency Response	196	10.2	Focusing the Control (Asset)	224
8.19	Skilled Support Personnel	197	10.2.1	The Threat Outcome	224
8.20	Specialist Employee	197	10.2.2	Aligning Outcomes to Assets	225
8.21	DOT HAZMAT Classifications	198	10.3	Risk Management	227
8.21.1	DOT HAZMAT Class 1: Explosives	199	10.3.1	Concentrating the Control	228
8.21.2	DOT HAZMAT Class 2: Gases	199	10.4	Control Design	228
8.21.3	DOT HAZMAT Class 3: Flammable Liquids	199	10.4.1	Aligning Risk Management and Controls	228
8.21.4	DOT HAZMAT Class 4: Flammable Solids	199	10.4.2	Integration of the Harmonized Model	232
8.21.5	DOT HAZMAT Class 5: Oxidizers	199	10.5	Authors' Note	234
8.21.6	DOT HAZMAT Class 6: Toxic Materials	200			
8.21.7	DOT HAZMAT Class 7: Radioactive Materials	200	11	Challenges in Regulatory Oversight	235
8.21.8	DOT HAZMAT Class 8: Corrosive Materials	200	11.1	The Role of Regulatory Oversight	235
8.22	Importance of Implementing an Emergency Response Plan	201	11.2	Balancing Public Safety and Business Operations	237
8.23	Authors' Notes	201	11.3	A Critical Challenge in the Regulatory Development Process	240
9	The Insider Threat	203	11.4	Consultation, Cooperation, or Coercion	241
9.1	Defining the Insider Threat	203	11.5	Critical Capacities for Regulators	244
9.2	Intent and Commitment	204	11.6	Balancing Resilience and Financial Responsibility	246
9.2.1	What Motivates the Insider Threat?	204	11.7	Picking the Right Mechanisms	248
9.2.2	The Changing Attitude Towards Employment	205	11.8	The Emerging Role of Private Associations and Membership	249
9.2.3	The Impact on Intent and Commitment	205	11.9	Membership versus Competition?	249
9.3	Knowledge, Skills, Abilities, and Resources	206	11.10	Authors' Note	250
9.3.1	The Ability to Target	207	12	Interdependencies	251
9.3.2	The Ability to Lengthen the Breach	207	12.1	Looking at the World—A Community	251
9.3.3	The Ability to Abuse Processes	208	12.2	Current Trends in Business	252
9.4	Proximity and Mobility	208	12.3	The Shift and Change Government and Regulation	254
9.4.1	Proximity to the Community	208	12.4	The Blurred Line between Government and Business	255
9.4.2	Mobility within the Community	209	12.5	The Rise of the Networked Machines—The Internet of Things (IoT)	256
9.4.3	The Ability to Camouflage Activities	210	12.6	Trends in the Alignment of Interdependencies	256
9.5	The Need for Organizations to Listen, Adapt and Control	210	12.7	The Emergence of the Key Sectors – Energy, Transportation, Telecommunications, and Financial	259
9.5.1	Observing	212	12.8	Comparing the Topography of Interdependencies with Flat/Hierarchical Networks	261
9.5.2	Listening	212	12.9	Conditions for the Perfect Storm	265
9.5.3	Adapting	213	12.10	Authors' Note	266
9.5.4	Controlling	214	13	Climate Change	267
9.6	The Alternative Approach to Staffing and Resource Management	215	13.1	The Challenge of a Changing Climate	267
9.7	Authors' Notes	216	13.2	Christening the Ground—The Basic Concepts of CIP	269
10	Safeguard Design	217	13.3	Responding to Longer-Termed Issues	271
10.1	Responding to the Threat	217	13.4	Integrating Shorter-Termed Challenges of a Changing Climate	277
10.1.1	Understanding Intent	218	13.5	Authors' Note	292
10.1.2	Understanding Capacity, Opportunity and Resources	220			
10.1.3	Understanding Proximity and Mobility	222			