

Contents

Figures	xv
Tables	xix
Preface	xxi
Acknowledgments	xxv
Part I	1
1 Security Risk Assessment and Management Process	3
1.1 Introduction	3
1.2 Security Risk Equation	6
1.3 Security Risk Assessment and Management Process	8
1.3.1 Facility Characterization	9
1.3.2 Threat Analysis	10
1.3.3 Consequence Analysis	11
1.3.4 System Effectiveness Assessment	13
1.3.5 Risk Estimation	16
1.3.6 Comparison of Estimated Risk Levels	17
1.3.7 Risk Reduction Strategies	17
1.4 Presentation to Management	18
1.5 Risk Management Decisions	18
1.6 Information Protection	19
1.7 Process Summary	19

1.8	References	20
1.9	Exercises	21
2	Screening Analysis	23
2.1	Introduction	23
2.2	Screening Analysis Methods	23
2.3	Summary	30
2.4	References	30
2.5	Exercises	30
3	Facility Characterization	31
3.1	Introduction	31
3.2	Undesired Events	32
3.3	Facility Description	33
3.3.1	Physical Details	33
3.3.2	Cyber-Information System	34
3.3.3	Facility Operations	34
3.3.4	Security Protection Systems	35
3.3.5	Workforce Description	38
3.3.6	Restrictions, Requirements, Limitations	39
3.4	Critical Assets	40
3.4.1	Generic Fault Tree	40
3.4.2	Identifying Critical Assets	42
3.5	Protection Objectives	44
3.6	Summary	45
3.7	References	46
3.8	Exercises	46
4	Threat Analysis	49
4.1	Introduction	49
4.2	Sources of Threat Information	50
4.2.1	Local and State Sources	51
4.2.2	National Sources	52

4.3	Adversary Spectrum	53
4.4	Adversary Capability	56
4.5	Threat Potential for Attack	58
4.5.1	Outsider Threat	62
4.5.2	Insider Threat	69
4.6	Summary	71
4.7	References	71
4.8	Exercises	72
5	Consequence Analysis	75
5.1	Introduction	75
5.2	Reference Table of Consequences	75
5.3	Consequence Values for Undesired Events	77
5.4	Summary	81
5.5	References	81
5.6	Exercises	81
6	Asset Prioritization	83
6.1	Introduction	83
6.2	Prioritization Matrix	84
6.3	Summary	85
6.4	References	85
6.5	Exercises	86
7	System Effectiveness	87
7.1	Introduction	87
7.2	Protection System Effectiveness	88
7.2.1	Adversary Strategies	88
7.2.2	Physical Protection System Effectiveness	90
7.2.3	Cyber-Protection System Effectiveness	106
7.3	Summary	116
7.4	References	117
7.5	Exercises	118

8	Estimating Security Risk	121
8.1	Introduction	121
8.2	Estimating Security Risk	121
8.2.1	Conditional Risk	122
8.2.2	Relative Risk	122
8.3	Summary	125
8.4	References	125
8.5	Exercises	125
9	Risk Reduction Strategies	127
9.1	Introduction	127
9.2	Strategies for Reducing Likelihood of Attack	127
9.3	Strategies for Increasing Protection System Effectiveness	129
9.3.1	Physical Protection System Upgrades	129
9.3.2	Cyber-Protection System Upgrades	129
9.3.3	Protection System Upgrade Package(s)	129
9.4	Strategies for Mitigating Consequences	132
9.4.1	Construction Hardening	133
9.4.2	Redundancy	141
9.4.3	Optimized Recovery Strategies	143
9.4.4	Emergency Planning	145
9.5	Combinations of Reduction Strategies	148
9.6	Summary	149
9.7	References	150
9.8	Exercises	151
10	Evaluating Impacts	153
10.1	Risk Level	153
10.2	Costs	157
10.3	Operations/Schedules	159
10.4	Public Opinion	160
10.5	Other Site-Specific Concerns	160
10.6	Review Threat Analysis	161

10.7	Summary	162
10.8	References	162
10.9	Exercises	163
11	Risk Management Decisions	165
11.1	Introduction	165
11.2	Risk Assessment Results	166
11.2.1	Executive Summary	167
11.2.2	Introduction	167
11.2.3	Threat Analysis	168
11.2.4	Consequence Analysis	168
11.2.5	System Effectiveness Assessment	169
11.2.6	Risk Estimation	169
11.2.7	Risk Reduction Strategies and Packages	170
11.2.8	Impact Analysis	170
11.2.9	Supporting Documentation	171
11.2.10	Report Overview	171
11.3	Risk Management Decisions	171
11.4	Establish Design Threat	173
11.5	Summary	174
11.6	References	174
11.7	Exercises	174
12	Summary	175
12.1	Facility Characterization	177
12.2	Threat Analysis	178
12.3	Consequence Analysis	180
12.4	System Effectiveness Assessment	180
12.5	Risk Estimation	182
12.6	Comparison of Estimated Risk Level to Threshold	183
12.7	Risk Reduction Strategies	183

12.8	Analysis of Impacts Imposed by Risk Reduction Upgrade Packages	184
12.9	Presentation to Management	185
12.10	Risk Management Decisions	185
Part II		187
13	Demonstration of the Security Risk Assessment and Management Process	189
13.1	Introduction	189
13.2	Security Risk Assessment and Management Process	190
13.3	Screening Analysis	192
13.4	Facility Characterization	195
13.5	Operations	196
13.6	General Description	198
13.7	Threat	214
13.8	Consequences	228
13.9	Prioritization Analysis	238
13.10	Protection System Effectiveness	243
	13.10.1 Physical Protection System Effectiveness	245
	13.10.2 Analysis of Blast Effects	264
13.11	Estimation of Risk	269
	13.11.1 Risk Summary	269
13.12	Risk Reduction Strategies	272
	13.12.1 Physical Protection System Upgrades	273
	13.12.2 Result of Physical Protection System Upgrades	276
	13.12.3 Cyber-Protection System Upgrades	280
	13.12.4 Results of Cyber-Protection System Upgrades	281

13.12.5	Consequence Mitigation Upgrades	281
13.12.6	Summary	284
13.13	Impact Analysis	285
13.13.1	Impacts of Upgrade Package	285
13.13.2	Impacts of Consequence Mitigation Package	288
13.14	Presentation to Management	288
13.14.1	Threat Description	289
13.14.2	Security Risk Estimates for the Baseline System	289
13.14.3	Risk Reduction Packages	290
13.14.4	Impact Analysis for Risk Reduction Package	294
13.15	Risk Management Decisions	295
	Appendix A: Generic Fault Tree for Buildings	297
	Appendix B: Adversary Sequence Diagrams	303
	Appendix C: Physical System Effectiveness Worksheets	309
	Appendix D: Insider Threat	329
	Acronyms	345
	Glossary	347
	Index	353

