

Contents

1	Introduction	1
1.1	Aim and Emphasis	2
1.2	Policy of Writing and Presentation	2
1.3	Structure and Organization	3
1.3.1	Part I: Conceptual Introduction	3
1.3.2	Part II: Cyber-risk Assessment Exemplified	4
1.3.3	Part III: Known Challenges	4
1.4	Intended Readers and Ways to Read	5
1.5	Relevant Standards	6
 Part I Conceptual Introduction		
2	Risk Management	9
2.1	What is Risk?	9
2.2	What is Risk Management?	12
2.3	Communication and Consultation	13
2.3.1	Establish a Consultative Team	14
2.3.2	Define a Plan for Communication and Consultation	14
2.3.3	Ensure Endorsement of the Risk Management Process	14
2.3.4	Communicate Risk Assessment Results	15
2.4	Risk Assessment	15
2.4.1	Context Establishment	15
2.4.2	Risk Identification	18
2.4.3	Risk Analysis	20
2.4.4	Risk Evaluation	21
2.4.5	Risk Treatment	21
2.5	Monitoring and Review	22
2.5.1	Monitoring and Review of Risks	23
2.5.2	Monitoring and Review of Risk Management	23
2.6	Further Reading	24

3	Cyber-systems	25
3.1	What is a Cyberspace?	25
3.2	What is a Cyber-system?	26
3.3	Further Reading	26
4	Cybersecurity	29
4.1	What is Cybersecurity?	29
4.2	How Does Cybersecurity Relate to Information Security?	30
4.3	How Does Cybersecurity Relate to Critical Infrastructure Protection?	30
4.4	How Does Cybersecurity Relate to Safety?	31
4.5	Further Reading	32
5	Cyber-risk Management	33
5.1	What is Cyber-risk?	33
5.2	Communication and Consultation of Cyber-risk	34
5.3	Cyber-risk Assessment	35
5.3.1	Context Establishment for Cyber-risk	37
5.3.2	Identification of Malicious Cyber-risk	37
5.3.3	Identification of Non-malicious Cyber-risk	40
5.3.4	Analysis of Cyber-risk	42
5.3.5	Evaluation of Cyber-risk	43
5.3.6	Treatment of Cyber-risk	44
5.4	Monitoring and Review of Cyber-risk	45
5.4.1	Monitoring and Review of Cyber-risk	46
5.4.2	Monitoring and Review of Cyber-risk Management	46
5.5	Further Reading	47

Part II Cyber-risk Assessment Exemplified

6	Context Establishment	51
6.1	Context, Goals, and Objectives	51
6.1.1	External Context	52
6.1.2	Internal Context	52
6.1.3	Goals and Objectives	52
6.2	Target of Assessment	53
6.2.1	Electricity Customer	54
6.2.2	Distribution System Operator	54
6.2.3	Communication Channels Between Components	55
6.3	Interface to Cyberspace and Attack Surface	55
6.4	Scope, Focus, and Assumptions	56
6.4.1	Scope	56
6.4.2	Focus	56
6.4.3	Assumptions	57
6.5	Assets, Scales, and Risk Evaluation Criteria	57
6.5.1	Assets	57
6.5.2	Likelihood Scale	58

6.5.3	Consequence Scales	58
6.5.4	Risk Evaluation Criteria	59
6.6	Further Reading	60
7	Risk Identification	61
7.1	Risk Identification Techniques	61
7.2	Malicious Risks	64
7.2.1	Threat Source Identification	65
7.2.2	Threat Identification	66
7.2.3	Vulnerability Identification	68
7.2.4	Incident Identification	70
7.3	Non-malicious Risks	73
7.3.1	Incident Identification	75
7.3.2	Vulnerability Identification	76
7.3.3	Threat Identification	77
7.3.4	Threat Source Identification	79
7.4	Further Reading	80
8	Risk Analysis	81
8.1	Threat Analysis	81
8.1.1	Malicious Threats	82
8.1.2	Non-malicious Threats	83
8.2	Vulnerability Analysis	84
8.2.1	Malicious Threat Vulnerabilities	85
8.2.2	Non-malicious Threat Vulnerabilities	85
8.3	Likelihood of Incidents	86
8.4	Consequence of Incidents	88
8.5	Further Reading	89
9	Risk Evaluation	91
9.1	Consolidation of Risk Analysis Results	91
9.2	Evaluation of Risk Level	92
9.3	Risk Aggregation	92
9.4	Risk Grouping	95
9.5	Further Reading	96
10	Risk Treatment	97
10.1	Risk Treatment Identification	97
10.1.1	Malicious Risks	97
10.1.2	Non-malicious Risks	99
10.2	Risk Acceptance	101
10.3	Further Reading	103

Part III Known Challenges and How to Address Them in Practice

11 Which Measure of Risk Level to Use?	107
11.1 Two-factor Measure	107
11.2 Three-factor Measure	108
11.3 Many-factor Measure	109
11.4 Which Measure to Use for Cyber-risk?	110
11.5 Further Reading	110
12 What Scales Are Best Suited Under What Conditions?	111
12.1 Classification of Scales	111
12.2 Qualitative Versus Quantitative Risk Assessment	112
12.3 Scales for Likelihood	114
12.4 Scales for Consequence	115
12.5 What Scales to Use for Cyber-risk?	115
12.6 Further Reading	116
13 How to Deal with Uncertainty?	117
13.1 Conceptual Clarification	117
13.2 Kinds of Uncertainty	118
13.3 Representing Uncertainty	119
13.4 Reducing Uncertainty	120
13.5 How to Handle Uncertainty for Cyber-risk?	121
13.6 Further Reading	121
14 High-consequence Risk with Low Likelihood	123
14.1 Dealing with Black Swans	123
14.2 Identifying Gray Swans	124
14.3 Communicating Gray Swans	125
14.4 Dealing with Gray Swans	126
14.5 Recognizing Gray Swans in Cyberspace	126
14.6 Further Reading	127
15 Conclusion	129
15.1 What We Have Put Forward in General	129
15.2 What We Have Put Forward in Particular	130
15.3 What We Have not Covered	131
Glossary	133
References	137
Index	141

Cyber-Risk Management

Refsdal, A.; Solhaug, B.; Stolen, K.

2015, XI, 145 p. 32 illus., Softcover

ISBN: 978-3-319-23569-1