1 Textbook Cyber Crises 1
1.1 Cyber Crisis Re-invented: Sony Pictures Entertainment 1
1.2 Dramaturgy of Inadequately Managed Cyber Crises 3

2 First Things First: The Human Factor in the Management of (Cyber) Crises 9
2.1 Decisions or the Essence of Crisis Management 9
2.2 Assessments, Behavioral Patterns and Stress 11
2.2.1 How People Perceive and Assess Situations 11
2.2.2 Behavioral Patterns and How They Manifest Themselves 12
2.2.3 Stress and How It Arises 13
2.2.4 Stress and What We Can Do About It 15
2.3 Requirements for the Members of the Emergency and Crisis Management Organization 17

3 Cyber Crisis Response 19
3.1 Alerting, Escalation, and Notification 19
3.1.1 Principles and Success Factors 19
3.1.2 Responsibilities and Processes 22
3.1.3 Availability or Stand-by Arrangements 25
3.1.4 Information Channels or: Alerting tools Vs. Telephone Cascades 26
3.1.5 Escalation Criteria Vs. Responsibility and Error Culture 29
3.2 Response at Strategic Level 30
3.2.1 Setting the Course: Initializing the Work of the Crisis Management Team 30
3.2.1.1 Before We Go into Action: The Get-Out-of-Jail-Free Card 32
3.2.1.2 Initial Analysis of the Situation or: What's Going On? 35
3.2.1.3 Affected Stakeholders or: Who Should We Expect? . . . 37

3.2.1.4 Thinking Negatively for a Change: What If? 44
3.2.1.5 From Identification to Assessment: Objective, Objective, and Objective Again 48
3.2.1.6 The Formal Establishment of the Crisis Case: Houston, We Have a Problem 52
3.2.2 Managing Cyber Crises in a Structured Way: Crisis Management Process 53
3.2.2.1 Variant A: Leadership Process 55
3.2.3 Variant B: FOR-DEC 62
3.2.4 Crisis Communication 63
3.2.4.1 Rules of Thumb for Crisis Communication 64
3.2.4.2 Starting Point: Stakeholder Needs and Distress in Cyber Crises 65
3.2.4.3 W-Questions of Crisis Communication 67
3.2.4.4 From Bloggers, YouTubers, and Journalists: Limits of German Press Law 73
3.2.5 From Practice: Strategies in Acute Cyber Crises 74
3.2.5.1 Victim Care Above All 75
3.2.5.2 We Ourselves Are Also Victims! 77
3.2.5.3 Attack Is the Best Defense 79
3.2.5.4 Putting the Cards on the Table Vs. Refusing to Communicate 81
3.2.5.5 Getting Out of the Line of Fire 82
3.2.5.6 Swapping a Scapegoat for an Identification Figure 84
3.2.5.7 When We Are Blackmailed 84
3.3 Reaction at Tactical-Operational Level 86
3.3.1 The Show Must Go on or: Restart of Processes and IT Systems 86
3.3.1.1 Restart: Critical (Business) Processes 88
3.3.1.2 Restart: IT Systems and Data 90
3.3.2 Cybersecurity Incident Response 94
3.3.2.1 Cybersecurity Incident Response Procedure 95
3.3.2.2 Rules of Thumb for Cybersecurity Incident Response 97

4 Cyber Crisis Preparation 99
4.1 Nothing for Regular Operations or: Emergency and Crisis Organization 99
4.1.1 The Rescue Team or: CMT 102
4.1.1.1 The Organizational Framework of the CMT 104
4.1.1.2 Manning of the CMT 105
4.1.1.3 The Crucial Question: Who Would Be Better (Not) to Be a Member of the CMT 109
4.1.2 Situation Center 111

4.1.3 Communications Staff 112
4.1.4 Emergency Bodies at the Tactical-Operational Level 113
4.2 Infrastructures and Tools 115
4.2.1 Crisis Manual 115
4.2.2 CMT Room 119
4.2.3 Templates and Posters 121
4.2.4 IT-Supported Crisis Management Tools 121
4.2.5 Alerting Tools 123
4.2.6 Governance Suites for BCM, IRBC, and ISM 124
4.2.7 IDS and SIEM Tools 125
4.3 Logistics Ensure Sustainability 126
4.4 Preparing for Crisis Communication 128
4.4.1 Communication Aids 129
4.5 Practice Creates Masters: Trainings and Exercises 134
4.5.1 Formats 134
4.5.2 Training Program 136
4.6 Create Conditions for the Continuation of Business Operations 139
4.6.1 Prepare Emergency Operation of (Business) Processes 139
4.6.1.1 Criticalities and Resources 139
4.6.1.2 Business Continuity Plans 142
4.6.2 Enable Restart of IT Systems 143
4.6.2.1 Technical Solutions 143
4.6.2.2 Organizational Preparations: Restart Plans and Restore Concepts 145
4.6.3 Creating a Framework for Cybersecurity Incident Response 147
4.7 What Works and What Does Not: Tests 147
4.8 Insurance of Cyber Risks 151

5 Cyber Crisis Prevention 155
5.1 Starting with an Analogy 155
5.2 Danger Recognized, Danger Averted: Awareness 157
5.3 Early Warning System: Risk Communication, Stakeholder Management, and Issue Management 158
5.3.1 Stakeholder and Issue Management 160
5.3.2 Risk Communication (And Its Pitfalls) 162
5.4 Not Sexy, but Fundamental: Asset Management and Structural Analysis 165
5.5 Indispensable: Information and IT Security Management 168
5.5.1 ISM in Fast Forward Mode 168
5.5.2 Fields of Action for Information Security 170
5.6 Focus Availability: Continuity Management 171
5.6.1 Business Continuity Management 171

5.6.2 IRBC/IT Service Continuity Management 173
5.7 Cyber Risk Management 176
5.7.1 Preliminary Work 177
5.7.2 Risk Assessment 177
5.7.2.1 Risk Identification 177
5.7.2.2 Risk Analysis 179
5.7.2.3 Risk Assessment 180
5.7.3 Risk Treatment 182
5.7.4 Acceptance of (Residual) Risks 183
5.8 Our Cyber Resilience and What It Is Like: Audits 185

6 Post Crisis Care: Follow Up 187
6.1 The View Outwards: Repairing Stakeholder Relationships 187
6.2 The View Inwards: People, Processes, and Technology 188
6.2.1 Human Factor 189
6.2.2 Alerting and Escalation 190
6.2.3 Interaction Between the Levels of the Emergency and Crisis Organization 190
6.2.4 Strategic Level 191
6.2.5 Operational Level: BCM and IRBC 192
6.2.6 Tactical Level: CSIRT and Cybersecurity Incident Response . . . 193
6.2.7 Crisis Communication 194

7 At a Glance: Seven Deadly Sins of Cyber Crisis Management 195

Appendix A: Read More 199

Appendix B: Abbreviations and Glossary 205

Index 217