Contents

Foreword xi

Preface xiii

Introduction xvii

Chapter 1. An Increasingly Vulnerable World 1

1.1. The context 1
1.1.1. Technological disruptions and globalization 1
1.1.2. Data at the heart of industrial productivity 3
1.1.3. Cyberspace, an area without boundaries 3
1.1.4. IT resources 4
1.2. Cybercrime 4
1.2.1. The concept of cybercrime 4
1.2.2. Five types of threats 6
1.2.3. Five types of attackers 9
1.3. The cybersecurity market. 15
1.3.1. The size of the market and its evolution 15
1.3.2. The market by sector of activity 15
1.3.3. Types of purchases and investments. 16
1.3.4. Geographical distribution 17
1.4. Cyber incidents 17
1.4.1. The facts 17
1.4.2. Testimonials versus silence 24
1.4.3. Trends 25
1.4.4. Examples. 27

1.5. Examples of particularly exposed sectors of activity 30
1.5.1. Cinema 30
1.5.2. Banks 31
1.5.3. Health 34
1.5.4. Tourism and business hotels 35
1.5.5. Critical national infrastructure 36
1.6. Responsibilities of officers and directors 37

Chapter 2. Corporate Governance and Digital Responsibility 39

2.1. Corporate governance and stakeholders 39
2.2. The shareholders 40
2.2.1. Valuation of the company 41
2.2.2. Cyber rating agencies 42
2.2.3. Insider trading 43
2.2.4. Activist shareholders 44
2.2.5. The stock exchange authorities 45
2.2.6. The annual report 45
2.3. The board of directors. 47
2.3.1. The facts 47
2.3.2. The four missions of the board of directors. 47
2.3.3. Civil and criminal liability 49
2.3.4. The board of directors and cybersecurity 50
2.3.5. The board of directors and data protection 53
2.3.6. The statutory auditors 54
2.3.7. The numerical responsibility of the board of directors. 55
2.4. Customers and suppliers 56
2.5. Operational management 58
2.5.1. The impacts of digital transformation 58
2.5.2. The digital strategy 59
2.5.3. The consequences of poor digital performance 62
2.5.4. Cybersecurity 63
2.5.5. Merger and acquisition transactions 65
2.5.6. Governance and data protection, cybersecurity 66

Chapter 3. Risk Mapping 69

3.1. Cyber-risks 69
3.2. The context 71
3.3. Vulnerabilities 72
3.3.1. Fraud against the president 73

3.3.2. Supplier fraud 73
3.3.3. Other economic impacts 74
3.4. Legal risks 76
3.4.1. Class actions 76
3.4.2. Sanctions by the CNIL and the ICO 77
3.5. The objectives of risk mapping 78
3.6. The different methods of risk analysis 79
3.7. Risk assessment (identify) 81
3.7.1. The main actors 81
3.7.2. The steps 82
3.8. Protecting 83
3.9. Detecting 83
3.10. Reacting 84
3.11. Restoring 85
3.12. Decentralized mapping 85
3.12.1. The internal threat 85
3.12.2. Industrial risks 87
3.12.3. Suppliers, subcontractors and service providers 88
3.12.4. Connected objects 89
3.13. Insurance 94
3.14. Non-compliance risks and ethics 96

Chapter 4. Regulations 99

4.1. The context 99
4.1.1. Complaints filed with the CNIL 100
4.1.2. Vectaury 101
4.1.3. Optical Center 102
4.1.4. Dailymotion 103
4.2. The different international regulations (data protection) 103
4.2.1. The United States 104
4.2.2. China 104
4.2.3. Asia 105
4.2.4. Europe 105
4.3. Cybersecurity regulations, the NIS Directive 105
4.4. Sectoral regulations 106
4.4.1. The banking industry 106
4.4.2. Health 108
4.5. The General Data Protection Regulation (GDPR) 109
4.5.1. The foundations 110
4.5.2. Definition of personal data 110
4.5.3. The so-called “sensitive” data 111

4.5.4. The principles of the GDPR 112
4.5.5. The five actions to be in compliance with the GDPR 113
4.5.6. The processing register 113
4.5.7. The five actions to be carried out 113
4.5.8. Cookies 116
4.6. Consequences for the company and the board of directors 117

Chapter 5. Best Practices of the Board of Directors 119

5.1. Digital skills 120
5.2. Situational awareness 121
5.2.1. The main issues 121
5.2.2. Insurance 125
5.3. Internal governance 126
5.3.1. The CISO 126
5.3.2. The CISO and the company 127
5.3.3. Clarifying responsibilities 131
5.3.4. Streamlining the supplier portfolio 133
5.3.5. Security policies and procedures 134
5.3.6. The human being 137
5.4. Data protection 138
5.4.1. Emails 139
5.4.2. The tools 141
5.4.3. Double authentication: better, but not 100% reliable 142
5.5. Choosing your service providers 142
5.6. The budget 143
5.7. Cyberculture 144
5.8. The dashboard for officers and directors 145

Chapter 6. Resilience and Crisis Management 147

6.1. How to ensure resilience? 147
6.2. Definition of a CERT 149
6.3. Definition of a SOC 149
6.4. The role of ENISA 150
6.5. The business continuity plan 150
6.6. Crisis management 151
6.6.1. The preparation 151
6.6.2. Exiting the state of sideration 152
6.6.3. Ensuring business continuity 153
6.6.4. Story of the TV5 Monde attack 154
6.6.5. Management of the first few hours 159
6.7. Crisis simulation 163

Conclusion. The Digital Committee 165

Appendices 167

Appendix 1. Cybersecurity Dashboard 169

Appendix 2. Ensuring Cybersecurity in Practice and on a Daily Basis 173

Appendix 3. Tools to Identify, Protect, Detect, Train, React and Restore 175

Glossary 179

References 183

Index 187