Table des matières

Préface 1
Hervé GUILLOU

Avant-propos 3

Introduction. Performance financière et performance cyber 7

Chapitre 1. Un monde de plus en plus vulnérable 13

1.1. Le contexte 13
1.1.1. Les ruptures technologiques et la globalisation 13
1.1.2. La donnée au cœur de la productivité industrielle 15
1.1.3. Le cyberespace, un espace sans frontières 15
1.1.4. Les moyens informatiques 16
1.2. La cybercriminalité 16
1.2.1. Le concept de cybercriminalité 16
1.2.2. Cinq types de menaces 18
1.2.2.1. Le cyberespionnage 19
1.2.2.2. Les attaques indirectes 20
1.2.2.3. Le sabotage 20
1.2.2.4. Le *cryptojacking* ou minage de cryptomonnaie 20
1.2.2.5. Fraudes en ligne et cybercriminalité 21
1.2.3. Cinq types d'attaquants 21
1.2.3.1. À la recherche d'argent facile 21
1.2.3.2. Les cyberactivistes/hacktivistes 21
1.2.3.3. Les concurrents (ou les États) dans un but d'espionnage ou de sabotage 22

1.2.3.4. Les employés : la menace la plus fréquente 23
1.2.3.5. Les États 24
1.3. Le marché de la cybersécurité 26
1.3.1. La taille du marché et son évolution 26
1.3.2. Le marché par secteur d'activité 27
1.3.3. Les types d'achats et d'investissements 28
1.3.4. La répartition géographique 28
1.4. Les incidents cyber 28
1.4.1. Les faits 28
1.4.1.1. Les informations sur la cybercriminalité 29
1.4.1.2. L'origine des menaces 30
1.4.1.3. Leur mise en œuvre 31
1.4.1.4. Les cibles 33
1.4.1.5. Les cordonniers les plus mal chaussés 34
1.4.2. Témoignages *versus* omerta 35
1.4.3. Les tendances 36
1.4.3.1. Les méthodes cybercriminelles 36
1.4.3.2. Les attaquants 36
1.4.3.3. Les objets connectés 36
1.4.3.4. La cyberguerre 37
1.4.4. Des exemples 37
1.4.4.1. Les fuites d'informations 37
1.4.4.2. Quelques exemples d'attaques célèbres 38
1.5. Exemples de secteurs d'activité particulièrement exposés 41
1.5.1. Le cinéma 41
1.5.2. La banque 42
1.5.3. La santé 45
1.5.4. Le tourisme et l'hôtellerie d'affaires 46
1.5.5. Les opérateurs d'importance vitale (OIV) 46
1.5.5.1. Loi de programmation militaire 46
1.5.5.2. Les enjeux pour les dirigeants et les administrateurs 47
1.6. Les responsabilités des dirigeants et administrateurs 48

Chapitre 2. Gouvernance d'entreprise et responsabilité numérique 49

2.1. Gouvernance d'entreprise et parties prenantes 49
2.2. Les actionnaires 50
2.2.1. La valorisation de l'entreprise 50
2.2.2. Les agences de notation cyber 52
2.2.3. Les délits d'initiés 52
2.2.4. Les actionnaires activistes 53

2.2.5. Les autorités boursières 54
2.2.6. Le rapport annuel 55
2.3. Le conseil d'administration 56
2.3.1. Les faits 56
2.3.2. Les quatre missions du conseil d'administration 57
2.3.3. Les responsabilités civiles et pénales 58
2.3.4. Le conseil d'administration et la cybersécurité 60
2.3.4.1. La prise en main du destin numérique de l'entreprise 61
2.3.4.2. Réinventer le conseil d'administration ? 61
2.3.5. Le conseil d'administration et la protection des données 62
2.3.6. Les commissaires aux comptes 64
2.3.7. La responsabilité numérique du conseil d'administration 64
2.4. Les clients et les fournisseurs 65
2.5. La direction opérationnelle 67
2.5.1. Les impacts de la transformation numérique 67
2.5.2. La stratégie numérique 68
2.5.2.1. Plusieurs réponses possibles et complémentaires 69
2.5.3. Les conséquences d'une mauvaise performance numérique 71
2.5.4. La cybersécurité 72
2.5.5. Les opérations de fusion-acquisition 74
2.5.6. Gouvernance et protection des données, cybersécurité 75
2.5.6.1. Les données internes 75
2.5.6.2. Les données clients 75
2.5.6.3. Open Data et protection des données personnelles 76
2.5.6.4. Les données publiques – L'espionnite aiguë ? 76

Chapitre 3. La cartographie des risques 79

3.1. Les cyberrisques 79
3.2. Le contexte 81
3.3. Les vulnérabilités 82
3.3.1. La fraude au président 83
3.3.2. La fraude au fournisseur 83
3.3.3. Autres impacts économiques 84
3.4. Les risques juridiques 86
3.4.1. Les recours collectifs ou *class actions* 86
3.4.2. Les sanctions de la CNIL et de l'ICO 87
3.5. Les objectifs de la cartographie des risques 88
3.6. Les différentes méthodes d'analyse des risques 89
3.7. L'évaluation des risques (identifier) 91
3.7.1. Les principaux acteurs 91
3.7.2. Les étapes 92

3.8. Protéger . . . 93
3.9. Détecter . . . 93
3.10. Réagir . . . 94
3.11. Restaurer. . . . 95
3.12. La cartographie décentralisée . . . 95
3.12.1. La menace interne . . . 95
3.12.2. Les risques industriels . . . 96
3.12.3. Les fournisseurs, sous-traitants et prestataires de services . . . 98
3.12.4. Les objets connectés . . . 99
3.12.4.1. Les jouets connectés . . . 101
3.12.4.2. Les assistants vocaux . . . 101
3.12.4.3. Les mesures de sécurité pour objets connectés. . . . 102
3.13. L'assurance . . . 103
3.14. Les risques de non-conformité et l'éthique . . . 105

Chapitre 4. Les règlementations . . . 107

4.1. Le contexte . . . 107
4.1.1. Les plaintes déposées à la CNIL . . . 108
4.1.2. Vectaury . . . 109
4.1.3. Optical Center . . . 110
4.1.4. Dailymotion . . . 110
4.2. Les différentes règlementations internationales (protection des données) . . . 111
4.2.1. Les États-Unis . . . 111
4.2.2. La Chine . . . 112
4.2.3. L'Asie. . . . 113
4.2.4. L'Europe . . . 113
4.3. Les règlementations relatives à la cybersécurité, la directive NIS . . . 113
4.4. Les règlementations sectorielles. . . . 114
4.4.1. L'industrie bancaire . . . 114
4.4.2. La santé . . . 115
4.5. Le Règlement général sur la protection des données (RGPD) . . . 116
4.5.1. Les fondements . . . 118
4.5.2. Définition d'une donnée personnelle . . . 118
4.5.3. Les données dites « sensibles » . . . 119
4.5.4. Les principes du RGPD . . . 119
4.5.4.1. La transparence . . . 119
4.5.4.2. La minimisation . . . 120
4.5.4.3. La sécurisation des données . . . 120
4.5.4.4. L'*accountability* . . . 120
4.5.5. Les cinq actions pour être en conformité au RGPD . . . 120

4.5.6. Le registre des traitements . . . 121
4.5.7. Les cinq actions à mener . . . 121
4.5.7.1. Nomination d'un DPO . . . 121
4.5.7.2. Plan de mise en conformité . . . 122
4.5.7.3. Produire/actualiser le traitement des données personnelles . . . 122
4.5.7.4. Actualiser les sites web/les documents . . . 123
4.5.7.5. Écrire aux sous-traitants et partenaires impactés . . . 123
4.5.8. Les cookies . . . 124
4.6. Les conséquences pour l'entreprise et le conseil d'administration . . . 124

Chapitre 5. Les bonnes pratiques du conseil d'administration . . . 127

5.1. Les compétences numériques . . . 127
5.2. La connaissance de la situation . . . 129
5.2.1. Les principales questions . . . 129
5.2.1.1. *It starts with the CEO ! – Tone from the top* . . . 129
5.2.1.2. Éviter la méthode consistant à cocher les listes de points de contrôle . . . 130
5.2.1.3. Attribuer des responsabilités de supervision claires au niveau du conseil . . . 130
5.2.1.4. Exiger des évaluations, tests et rapports . . . 131
5.2.1.5. Rester vigilant en permanence . . . 131
5.2.1.6. Être informé et comprendre les incidents . . . 132
5.2.1.7. Anticiper . . . 132
5.2.2. L'assurance . . . 133
5.3. La gouvernance interne . . . 134
5.3.1. Le RSSI . . . 134
5.3.2. Le RSSI et l'entreprise . . . 135
5.3.3. Clarifier les responsabilités . . . 139
5.3.4. Rationaliser le portefeuille de fournisseurs . . . 140
5.3.5. Les politiques de sécurité et les procédures . . . 141
5.3.5.1. La stratégie *Cloud* . . . 142
5.3.5.2. La stratégie *bring your own device* (BYOD) . . . 143
5.3.6. L'humain . . . 144
5.4. La protection des données . . . 145
5.4.1. Les e-mails . . . 146
5.4.2. Les outils . . . 147
5.4.3. La double authentification : mieux, mais pas fiable à 100 % . . . 149
5.5. Choisir ses prestataires . . . 149
5.6. Le budget . . . 149
5.7. La cyberculture . . . 150
5.8. Le tableau de bord pour les dirigeants et administrateurs . . . 152

Chapitre 6. La résilience et la gestion de crise 153

6.1. Comment assurer la résilience ?. 153
6.2. Définition d'un CERT 155
6.3. Définition d'un SOC 155
6.4. Le rôle de l'AESRI 156
6.5. Le plan de continuité d'activité 156
6.6. La gestion de crise. 157
6.6.1. La préparation 157
6.6.2. Sortir de l'état de sidération 158
6.6.3. Assurer la continuité d'exploitation 159
6.6.4. Récit de l'attaque de TV5 Monde 160
6.6.5. La gestion des premières heures 165
6.6.5.1. Les mesures d'urgence 165
6.6.5.2. Le paiement de la rançon 167
6.6.5.3. La gestion du moyen terme 168
6.6.5.4. La gestion du long terme 168
6.7. La simulation de crise. 168

Conclusion. Le comité numérique 171

Annexe 1. Tableau de bord sur la cybersécurité. 173

Annexe 2. Assurer, en pratique et au quotidien, sa cybersécurité 177

Annexe 3. Les outils pour identifier, protéger, détecter, former, réagir, restaurer 179

Glossaire 183

Bibliographie 187

Index 191