

TABLE DES MATIÈRES

Préface	5
Introduction	7

CHAPITRE 1

CADRE GÉNÉRAL DE LA SÉCURITÉ DU SYSTÈME D'INFORMATION

1.1. La révolution informatique pour les gens pressés	11
1.1.1. <i>L'ère précambrienne</i>	11
1.1.2. <i>L'informatique ouverte</i>	13
1.2. Histoire condensée de la sécurité du système d'information	14
1.2.1. <i>Les points cardinaux de la sécurité informatique</i>	14
1.2.2. <i>La sécurité vue sous l'angle réseau</i>	16
1.2.3. <i>La sécurité vue sous l'angle système</i>	17
1.3. Les nouveaux enjeux de la sécurité	18
1.4. Les dernières évolutions depuis 2012	19
1.4.1. <i>L'espionnage à grande échelle</i>	19
1.4.2. <i>La menace malware, plus que jamais</i>	20
1.4.3. <i>Le fractionnement à l'infini</i>	20

CHAPITRE 2

LES FONDAMENTAUX

2.1. Qu'est-ce qu'un système d'information (SI) ?	21
2.1.1. <i>Une définition standard</i>	21
2.1.2. <i>Le langage de l'entreprise</i>	22
2.1.3. <i>Un point de vue sur l'entreprise</i>	22
2.1.4. <i>Vision institutionnelle du SI</i>	23
2.2. La cartographie des processus	23
2.2.1. <i>Éléments théoriques</i>	23
2.2.2. <i>Cartographie des processus dans le monde de la santé</i>	24
2.3. Le modèle OSI	26
2.4. Concepts de maîtrise d'ouvrage et maîtrise d'œuvre	27
2.4.1. <i>Définitions</i>	27
2.4.2. <i>Complexité du concept</i>	28
2.4.3. <i>Position de la sécurité du système d'information dans le concept MOA/</i> <i>MOE</i>	29

2.5. Modèles de maturité	29
2.5.1. Les trois stades de réalisation	29
2.5.2. Le modèle de maturité COBIT	31
2.6. La sécurité du SI	33
2.6.1. Bases théoriques : DICP	33
2.6.2. Principe général de traitement du risque	34
2.6.3. Hiérarchie des besoins	35
2.6.4. Hiérarchie des besoins dans le monde de la santé	36
2.6.5. L'incident importe peu, seules comptent les conséquences	40
2.7. Le corpus juridique	41
2.7.1. La Commission nationale de l'informatique et des libertés (CNIL)	42
2.7.2. La loi du 4 mars 2002	44
2.7.3. Le décret confidentialité	45
2.7.4. Le décret hébergeur	45
2.7.5. La certification HAS	46
2.7.6. La certification des comptes	47
2.7.7. Le référentiel général de sécurité	48
2.7.8. Les politiques de sécurité du système d'information étatiques	49
2.7.9. Les autres décrets, arrêtés et circulaires	49
2.7.10. Le droit du travail	50
2.7.11. Prospectives	51
2.8. Le corpus normatif	51
2.9. Fondements cryptographiques	52
2.9.1. Des Incas à Kubrick	52
2.9.2. Le chiffrement symétrique	53
2.9.3. Chiffrement asymétrique	54
2.9.4. Infrastructure de gestion de clés	57
2.9.5. Prospectives	59
2.10. Les mots de passe	60
2.10.1. Un dernier rempart très friable	60
2.10.2. État des lieux technique	61
2.10.3. Prospectives	63

CHAPITRE 3

ÉLÉMENTS DE STRATÉGIE

3.1. Nouvelle approche de la sécurité	65
3.1.1. La sécurité, dernière des préoccupations	65
3.1.2. La culture du risque	66
3.1.3. Une démarche globale	68
3.1.4. Positionnement de la sécurité par rapport au modèle OSI	69
3.1.5. Des exigences sans cesse croissantes	69
3.2. Le responsable de la sécurité du système d'information (RSSI)	71
3.2.1. Les missions du RSSI	71
3.2.2. La position du RSSI dans l'organigramme	72
3.3. Les relations du RSSI	76
3.3.1. La contrainte	77
3.3.2. Le conseil	77
3.3.3. Cas particulier : les relations du RSSI avec la DSI	78
3.3.4. La MOA, « propriétaire » de ses risques	78
3.3.5. Les risques : jusqu'à quel point ?	79

3.4. Les instances internes	80
3.4.1. <i>Les instances de vigilance</i>	80
3.4.2. <i>Les instances d'arbitrage</i>	81
3.4.3. <i>Les instances de pilotage</i>	81
3.5. Les moyens	81
3.6. Mutualisation	83
3.6.1. <i>La fonction RSSI à l'aune des GHT</i>	83
3.6.2. <i>Le rôle des GCS</i>	83
3.6.3. <i>Vers la fin des GCS dans le domaine de la sécurité du système d'information ?</i>	85
3.7. La veille en sécurité du SI	85
3.7.1. <i>Les instances</i>	85
3.7.2. <i>Les formations</i>	86
3.7.3. <i>Les séminaires</i>	86
3.8. Vers un monde de contraintes normatives	87
3.9. Le découpage des projets	87

CHAPITRE 4

LE SYSTÈME DE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION (SMSI)

4.1. Le SMSI en bref : intérêt et limites	91
4.1.1. <i>La rencontre de deux mondes</i>	91
4.1.2. <i>Les enjeux majeurs</i>	93
4.1.3. <i>Les erreurs classiques</i>	93
4.1.4. <i>Le corpus normatif</i>	94
4.2. Descriptif général de la méthode	96
4.2.1. <i>Organisation</i>	96
4.2.2. <i>Le socle</i>	97
4.2.3. <i>Le moteur</i>	97
4.2.4. <i>Les contraintes exogènes</i>	100
4.2.5. <i>Les indicateurs et rapports</i>	100
4.2.6. <i>Les actions et projets</i>	101
4.2.7. <i>Le corpus documentaire</i>	102
4.3. Le projet de certification ISO 27 001	106
4.3.1. <i>Périmètre</i>	107
4.3.2. <i>Gouvernance</i>	107
4.3.3. <i>Découpage et livrables</i>	108
4.3.4. <i>Phase 1 : état des lieux technique et organisationnel</i>	108
4.3.5. <i>Phase 2 : appréciation générale des risques</i>	110
4.3.6. <i>Phase 3 : mise en œuvre du socle de base de la gouvernance</i>	115
4.4. Le maintien de la démarche	124
4.5. Conclusion	125

CHAPITRE 5

LES PROJETS

5.1. Les plans de continuité et reprise d'activité (PCA-PRA)	128
5.1.1. Contexte et enjeux.....	128
5.1.2. Cadrage	131
5.1.3. Démarche générale	133
5.1.4. La question des besoins des métiers	133
5.1.5. Sécurisation des réseaux et impact sur le bâti	135
5.1.6. Architecture technique pour un PCA-PRA.....	139
5.1.7. Les composants critiques d'un SI.....	141
5.1.8. Exemple 1 : appréciation des risques aux urgences	145
5.1.9. Exemple 2 : sécurisation de la stérilisation	146
5.1.10. Plan de repli des informaticiens	147
5.1.11. Plans de tests	148
5.1.12. Éléments managériaux	149
5.1.13. Conclusion.....	153
5.2. Le projet Identity Access Management (IAM)	154
5.2.1. Contexte et enjeux.....	154
5.2.2. Rappel sur les cartes CPX	155
5.2.3. Architecture générale d'une infrastructure CPX.....	155
5.2.4. Objectifs généraux.....	157
5.2.5. Service de gestion des cartes	158
5.2.6. Service aux utilisateurs	161
5.2.7. Sources des identités	161
5.2.8. Service de gestion des habilitations.....	166
5.2.9. Service de gestion des accès	168
5.2.10. Les autorités de certification (AC).....	170
5.2.11. Éléments de planning.....	171
5.2.12. Cas particulier : confidentialité des données vis-à-vis des informaticiens	171
5.2.13. Aspects financiers.....	173
5.2.14. Le cas des GHT.....	173
5.2.15. Impact du décret sur l'externalisation de la saisie des comptes rendus médicaux	174
5.2.16. Impact du décret sur les règles d'accès au dossier médical local	176
5.2.17. Conclusion.....	179
5.3. La sauvegarde et la restauration	180
5.3.1. Contexte et enjeux.....	180
5.3.2. Cadrage	182
5.3.3. Déroulement	184
5.3.4. Aspects organisationnels	191
5.3.5. Aspects financiers	192
5.3.6. Externalisation et sous-traitance.....	192
5.3.7. Conclusion.....	193
5.4. Le bloc d'accès	194
5.4.1. Contexte et enjeux.....	194
5.4.2. Cadrage	194
5.4.3. Phases préparatoires.....	195
5.4.4. Composants de base du bloc d'accès	196
5.4.5. Éléments additionnels	198
5.4.6. Aspects juridiques	200
5.4.7. DSI et fournisseur d'accès Internet	202

5.4.8. Les accès extérieurs	203
5.4.9. Aspects financiers	206
5.4.10. L'externalisation	206
5.4.11. La dimension GHT	207
5.4.12. Conclusion	207
5.5. La sécurisation du parc	208
5.5.1. Contexte et enjeux	208
5.5.2. Cadrage	208
5.5.3. Éléments de politique	209
5.5.4. Les dispositifs techniques	213
5.5.5. Questions diverses	219
5.5.6. Conclusion	221
5.6. La gestion des traces	221
5.6.1. Contexte et enjeux	221
5.6.2. Cadrage	222
5.6.3. Nature des traces applicatives	223
5.6.4. Respect de la réglementation	223
5.6.5. Accès aux logs de consultation d'un dossier médical local	224
5.6.6. Centralisation du système	225
5.6.7. Étendue des besoins	226
5.6.8. État du marché	226
5.6.9. Conclusion	227
5.7. Le décret hébergeur	227
5.7.1. Contexte et enjeux	227
5.7.2. Aspects managériaux	227
5.7.3. Dépôt d'un agrément d'hébergeur	230
5.7.4. L'agrément version 2	233
5.7.5. Aspects financiers	234
5.7.6. Conclusion	234
5.8. Les audits	236
5.8.1. SMSI	236
5.8.2. PCA-PRA	236
5.8.3. Décret confidentialité	237
5.8.4. Sauvegarde	237
5.8.5. Bloc d'accès	237
5.8.6. Sécurisation du parc	238
5.8.7. Hébergement de données de santé	239
5.8.8. Protection antivirale	239
5.8.9. Réseau	239
5.8.10. Conformité	239
5.8.11. Conclusion	239
5.9. Archivage	240
5.9.1. Contexte et enjeux	240
5.9.2. Cadrage	240
5.9.3. Éléments techniques	242
5.9.4. Dimension juridique	244
5.9.5. Impact des GHT	244
5.9.6. Conclusion	245
5.10. Protection antivirale	245
5.10.1. Contexte et enjeux	245
5.10.2. Objectifs généraux	246
5.10.3. Aspects financiers	247

5.10.4. Le cas des GHT	247
5.10.5. Conclusion	247
5.11. Sécurisation du réseau	247
5.11.1. Contexte et enjeux	247
5.11.2. Objectifs généraux	248
5.11.3. Le cas des GHT	249
5.11.4. Conclusion	249
5.12. Chiffrement	250
5.12.1. Contexte et enjeux	250
5.12.2. Objectifs généraux	250
5.12.3. Aspects techniques	250
5.12.4. Conclusion	252
5.13. Conformité	252
5.13.1 Contexte et enjeux	252
5.13.2. Objectifs généraux	252
5.13.3. Aspects financiers	257
5.13.4. Le cas des GHT	257
5.13.5. Conclusion	257
5.14. Protection du Cloud	258
5.14.1. Contexte et enjeux	258
5.14.2. Objectifs généraux	258
5.14.3. Le cas des GHT	259
5.14.4. Conclusion	259
5.15. Prospectives	259
5.15.1. Data Loss Prevention (DLP)	259
5.15.2. Sondes Intrusion Detection System (IDS)	260

CHAPITRE 6

LES ASPECTS FINANCIERS DE LA SÉCURITÉ

6.1. Limites inhérentes de l'estimation	261
6.2. Méthode	262
6.3. Analyse	262
6.3.1. Généralités	262
6.3.2. Projet SMSI	263
6.3.3. Projet PCA-PRA	263
6.3.4. Projet IAM	263
6.3.5. Sauvegarde-restauration	264
6.3.6. Bloc d'accès	264
6.3.7. Sécurisation du parc	264
6.3.8. La gestion des traces	265
6.3.9. Le décret hébergeur	265
6.3.10. Les audits	266
6.3.11. L'archivage numérique	266
6.3.12. La protection antivirale	266
6.3.13. La protection réseau	266
6.3.14. Le chiffrement	266
6.3.15. La conformité	267
6.3.16. Le Cloud	267
6.4. Synthèse	267

CHAPITRE 7

DOMAINES CONNEXES

7.1. La sécurisation des achats	269
7.2. La sécurisation du mode projet	271
7.3. La sécurisation de l'externalisation	272
7.4. Les infrastructures spontanées	273
7.5. Le droit de la sécurité du système d'information	274

CHAPITRE 8

LE CAS DES GHT

8.1. Éléments de stratégie	276
8.1.1. Les textes comme source de légitimité	276
8.1.2. La sécurité du système d'information comme catalyseur ou frein	276
8.1.3. Les leviers stratégiques	277
8.2. La tactique	278
8.3. La mise en œuvre	279
8.4. Exemples de projets à l'aune des GHT	280
8.4.1. Le projet PCA-PRA	280
8.4.2. Le projet bloc d'accès	280
8.4.3. La protection antivirale	281
8.5. Conclusion	281

CHAPITRE 9

**LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
À TRAVERS LE TEMPS**

9.1. Retour sur 2002	283
9.2. État des lieux 2017-2018	285
9.2.1. Le verre à moitié vide	285
9.2.2. Le verre à moitié plein	286
9.3. Perspectives 2030	287
9.3.1. Évolution de l'informatique de santé	287
9.3.2. Évolution des menaces	289
9.3.3. Quels impacts ?	291
9.4. Les invariants	292
9.4.1. Développer la culture de la procédure	292
9.4.2. Déployer la sécurité totale en continu	293
9.4.3. Faire face aux enjeux techniques	293
9.4.4. Aller vers la certification	293
9.4.5. Croissance des budgets SI et de sécurité du système d'information	294
9.5. Conclusion	294

Conclusion	295
Tirer les leçons des erreurs des autres	295
Prioriser les projets	296
Revenir aux fondamentaux	297
Annexes	
1. Principales jurisprudences et textes réglementaires	301
2. Cellule de crise	305
3. Exemple de cartographie applicative catégorisée	307
4. Exemple de tableau de bord sécurité	313
5. Exemple de métriques pour le calcul des risques	319
6. Exemple d’affiche sur les bonnes pratiques quotidiennes	321
Références	323
Liste des sigles	325

Maquette couverture: V. Hélye
 Conception: Presses de l’EHESP
 Réalisation: PCA-CMB Graphic - Rezé
 Achevé d’imprimer en janvier 2018
 sur les presses de Sepec numérique
 N° d’impression: N10715171206
 IMPRIMÉ EN FRANCE