

Table des matières

Avant-propos	1
Introduction	5
Partie 1. Le système d'information : des technologies et des personnes	9
Chapitre 1. Des composants aux fins connues : les technologies	11
1.1. Jusqu'à la fin du XIX ^e siècle : diminuer les temps de transmission	12
1.2. À partir de la fin du XIX ^e siècle : diminuer les temps de traitement	19
1.3. À partir de la fin du XX ^e siècle : faire face à la massification	26
Chapitre 2. Des composants interprétants : les personnes	29
2.1. Le <i>tacit knowing</i> ou comment sait-on ?	30
2.1.1. Il existe des connaissances tacites.	30
2.1.2. <i>Sense-giving</i> et <i>sense-reading</i> : les connaissances sont tacites	31
2.2. Le schéma d'interprétation, filtre au travers duquel nous créons nos connaissances.	34

2.2.1. Un outil de <i>tacit knowing</i>	34
2.2.2. Les différents modes de schémas d'interprétation.	36
2.2.2.1. La croyance sur l'analysabilité de l'environnement	36
2.2.2.2. L'intrusion dans l'environnement pour le comprendre.	37
2.2.3. La commensurabilité des schémas d'interprétation.	39
2.3. Le concept d'incommensurabilité	41
2.3.1. De la communication partielle à l'incommensurabilité	41
2.3.2. Le langage : relier les mots à la nature.	42
2.3.3. La révolution : changer le sens des mots	44
2.4. Les modèles mentaux, représentations de la réalité	46
2.4.1. Des représentations incomplètes	47
2.4.2. Des représentations cognitives.	48
2.4.3. Les modèles mentaux partagés	49
2.4.4. Expliciter les modèles mentaux	51
2.4.4.1. Explicitation directe	51
2.4.4.2. Explicitation indirecte.	54
Partie 2. La menace intérieure	57
Chapitre 3. Les trois catégories de menace intérieure	59
Chapitre 4. Le non-intentionnel.	65
4.1. La qualité des informations dérobées	69
4.2. Le cas de l'information apparemment anodine, mais à valeur cachée	70
4.3. Le cas de l'information qu'il suffit de demander.	73
4.4. Le cas de l'information qui va vous aider	75
Chapitre 5. L'intentionnel non malveillant	77
5.1. Du conflit entre productivité et sécurité	79
5.2. Les contournements, facteur d'innovation ou de risque	82
5.2.1. Contourner, c'est innover	82
5.2.2. Contourner, c'est risqué	83

5.3. Sur les violations non malveillantes	83
5.3.1. Comportement intentionnel	84
5.3.2. Bénéfice personnel sans intention malveillante	85
5.3.3. Rupture volontaire des règles	85
5.3.4. Possibles dommages ou risques de sécurité	86
Chapitre 6. L'intentionnel malveillant	87
6.1. L'information est connue, pourquoi ne pas l'exploiter ?	88
6.2. Contexte organisationnel et processus cognitifs du passage à l'acte	91
6.2.1. Pour l'organisation, la dissuasion empêche la malveillance	91
6.2.2. Pour l'employé, le désengagement moral justifie la malveillance	94
6.3. Facilité de dissuasion	96
Conclusions et perspectives	101
Liste des figures	105
Liste des scénarios d'attaque	109
Bibliographie	111
Index	119