

SOMMAIRE

NOTE DES AUTEURS	13
PRÉAMBULE : L'ENTREPRISE... OU LA CITADELLE ASSIÉGÉE.....	17
AVANT-PROPOS.....	23
<i>Pour une démarche globale de protection des entreprises</i>	25
<i>Le renseignement : une nécessité</i>	29
1. Trouver l'information stratégique non structurée.....	30
2. La maîtrise globale de l'information stratégique.....	35
3. La quête du renseignement économique.....	36
4. Les différents acteurs du renseignement économique.....	39
5. Le cycle du renseignement.....	43
6. Les catégories d'information sensible.....	45
<i>Pour une nouvelle définition de la notion de « risque »</i>	49
1. Le facteur humain.....	51
2. La cybercriminalité et le risque informatique.....	60
3. Le risque terrain.....	62
INTRODUCTION.....	67
<i>Géopolitique, géoéconomie, renseignement et autres complications...</i>	69
1. Une époque troublée.....	70
2. Une compétition farouche sur le terrain économique.....	72
3. Une entreprise sur quatre touchée par des actions d'espionnage.....	74
4. La confusion des pratiques de renseignement sur la sellette.....	76
5. L'intelligence économique, héritage des techniques des services d'État.....	80
6. Les armes de l'intelligence économique et du renseignement au service de la petite et moyenne entreprise.....	83

<i>Les nouvelles lois de l'hostilité économique</i>	85
1. Désignation de l'adversaire et contre-ingérence économique.....	87
2. Repenser les difficultés de l'action collective dans le cadre de l'entreprise.....	89
3. Face à la menace, les principes de réalité et de clairvoyance doivent prévaloir	91
4. L'information à haute valeur ajoutée et le savoir au cœur des luttes sauvages pour la recherche du profit.....	92
5. Des attaquants et des risques.....	93
<i>Des PME/PMI très pénalisées face aux menaces d'attaques subversives</i>	96
1. Les brevets sont-ils encore une arme dissuasive contre les attaquants ?.....	98
2. Propriété industrielle et droit des affaires : deux autres motifs d'inquiétude ?	100
3. La nécessité d'instaurer un nouveau mode de management par les hommes.....	100
4. La galaxie des PME/PMI : un terrain propice pour une nouvelle reconquête stratégique.....	103
5. Savoir répondre aux demandes concrètes de nos entreprises.....	104
<i>L'intelligence économique : il faut arrêter d'en parler et en faire !</i>	105
1. Au fond, qu'est-ce que l'« intelligence économique » ?.....	105
2. L'IE en France : un bilan contrasté.....	107
3. Changer d'état d'esprit et de regard pour mener des actions plus intelligentes.....	109
4. Le rouleau compresseur de l'approche anglo-saxonne : réellement imbattable ?.....	110
5. Et la France dans tout cela ?.....	111
<i>Vers un nouvel âge de la guerre économique en entreprise ?</i>	112
1. Les enjeux du renseignement économique « intelligent ».....	113
2. L'IE : quels coûts pour les petites et moyennes entreprises ?.....	116
LE PÔLE HUMAIN	119
<i>À l'école de la manipulation tactique : théorie et guide pratique</i>	121
1. Approches théoriques des processus communicationnels.....	126
2. Petite psychologie de la manipulation	137

3. Les situations de manipulation dans la vie courante.....	149
4. Les stratégies de manipulation.....	159
5. Les conditions de réussite d'une opération de manipulation.....	177
6. Identifier le profil psychologique d'un individu.....	184
<i>Identification et exploitation des faiblesses humaines par les prédateurs</i>	192
1. Débaucher chez son concurrent : cibler et convaincre.....	197
2. Organiser de faux entretiens : le renseignement conversationnel.....	199
3. Pratiquer la veille RH : le renseignement sans contact direct.....	200
4. Introduire un salarié « espion » : l'action clandestine d'infiltration...	201
5. <i>Social engineering</i> et manipulation des collaborateurs de l'entreprise cible.....	202
6. Recruter une « source » au sein des équipes adverses.....	216
7. Bilan récapitulatif : toutes les entreprises courent-elles le risque d'une faille humaine ?.....	229
8. Les suites à donner dans le cadre d'une enquête pénale conclusive.....	231
LE PÔLE NUMÉRIQUE	233
<i>La maîtrise des outils de recherche d'information</i>	244
1. Comprendre Google.....	244
2. Analyser une entreprise cible.....	254
3. Suivre les tribulations d'un individu sur la Toile.....	260
4. Parfaire sa veille.....	268
<i>Récupérer l'information souhaitée</i>	273
1. Préserver l'anonymat et la nature de l'attaque.....	274
2. Consulter la boîte mail d'un individu cible.....	278
3. Espionner un ordinateur à distance	285
4. Bénéficier d'un accès physique.....	292
5. S'infiltrer dans un réseau	300
<i>Se protéger</i>	319
1. Gérer sa présence sur Internet.....	321
2. La gestion des accès informatiques.....	328
3. La protection du poste de travail.....	333
4. La protection du réseau de l'entreprise.....	338
5. Empêcher les attaques	345
6. La sécurisation des échanges.....	348
7. Encadrer la mobilité.....	350
8. La politique de sécurité.....	356

LE PÔLE TERRAIN.....	377
<i>L'aspect physique et technique de l'action terrain</i>	379
1. Les intrusions physiques : vols avec effraction douce !.....	379
2. Les systèmes d'écoute.....	388
3. Autres méthodes pour obtenir de l'information.....	393
<i>Mesures de protection pour la sécurisation physique</i> <i>et topologique des entreprises</i>	400
1. L'environnement immédiat de l'entreprise.....	402
2. La gestion sécurisée des accès.....	404
3. La surveillance des locaux.....	406
4. La gestion des documents et correspondances.....	412
5. Pratiquer de fausses intrusions par mesure de prévention.....	413
CONCLUSION... <i>pour ne pas conclure !</i>	415
1. Pour un encadrement « intelligent » des collaborateurs.....	418
2. Considérer le facteur humain.....	419
3. La sensibilisation aux risques intrusifs.....	421
4. Quelques règles essentielles à respecter.....	422