LA BOÎTE À OUTILS

de la

Sécurité économique

Nicolas **MOINET**

DUNOD

Crédits iconographiques

Dossier 1 : © Adrien Roussel – Fotolia.com ; **Outil 9 :** © willypd – Fotolia.com

Dossier 2 : Outil 10 : © Andrey Popov – Fotolia.com ; **Outil 11 :** © Stephen Borengasser, © B. Agustín Amenábar Larraín, © Adam Heller, © Patrick Morrison, © iconoci, © Niels Gesquiere, © Raf Verbraeken, © Simple Icons, © Christelle Mozzati – The Noun Project ; **Outil 14 :** © Ben King – The Noun Project ; **Outil 17 :** © Margot Nadot, © Julieta Felix – The Noun Project ; **Outil 18 :** © momius – Fotolia.com ; **Outil 19 :** © Luis Prado, © Max Hancock – The Noun Project, © Daniel Schweinert – Fotolia.com, © aluxum – Fotolia.com

Dossier 3 : Outil 21 : © velazquez – Fotolia.com ; **Outil 22 :** © Wilson Joseph, © Martin Delin, © Arthur Schmitt, © Arthur Shlain – The Noun Project ; **Outil 29 :** © Luis Prado, © misirlou – The Noun Project

Dossier 4 : © Patrick Morrison – The Noun Project ; **Outil 35 :** © lekkyjustdoit – The Noun Project ; **Outil 36 :** © Andrej Kaprinay – Fotolia.com ; **Outil 37 :** © Juan Pablo Bravo, © 1974, © Fernando Vasconcelos – The Noun Project ; **Outil 38 :** © Simple Icons – The Noun Project ; **Outil 39 :** © Patrick Morrison, © Karthick Nagarajan, © Creative Stall, © Marek Polakovic, © Nick Kinling – The Noun Project ; **Outil 40 :** © Alexander Wiefel, © B. Agustín Amenábar Larraín – The Noun Project ; **Outil 41 :** © Stuart Miles – Fotolia.com ; **Outil 43 :** © Rohith M S – The Noun Project ; **Outil 44 :** © Sashkin – Fotolia.com, © Edward Boatman – The Noun Project ; **Outil 45 :** © lucadp – Fotolia.com

Dossier 5 : © Sergey Nivens – Fotolia.com ; **Outil 46 :** © misirlou – The Noun Project ; **Outil 51 :** © Wilson Joseph, © Lorenzo Baldini – The Noun Project ; **Outil 54 :** © Ted Grajeda, © iconsmind.com – The Noun Project.

Mise en page : Belle Page
Traduction : Stanley Hanks
Illustrations : Rachid Maraï

5 rue Laromiguière, 75005 Paris
www.dunod.com
ISBN 978-2-10-072846-6

Préface

Quelques années après la *Boîte à outils de l'intelligence économique*, il faut se réjouir de la sortie de ce livre collectif dans un domaine en pleine mutation.

La sécurité est restée longtemps au niveau du gardiennage et des risques d'incendie, ce qui en faisait un secteur délaissé des entreprises. Parallèlement à un service de sécurité généralement installé dans chaque site, on avait un *risk manager* dont l'objectif était de bien couvrir les risques par des assurances avec des primes raisonnables. Les problèmes majeurs résidaient dans la destruction partielle ou totale d'une usine, le vol par intrusion et le sabotage de machines. Ce fut une époque où le coût du risque et son impact sur l'entreprise étaient considérés comme très limités sauf erreur du management.

Récemment, on a découvert que les entreprises étaient amenées à rechercher le maximum d'informations sur leurs concurrents. Face au benchmarking adverse, il fallait apprendre à se protéger aussi bien au niveau des données que des process, de la stratégie ou des éléments de gestion. Face à des entreprises venues du monde entier et n'obéissant pas aux mêmes règles d'éthique, il a fallu sensibiliser l'ensemble du personnel face à des actions légales et illégales pouvant ruiner l'entreprise. Au-delà des procédures de protection, il a fallu changer d'état d'esprit.

L'arrivée du numérique et le cyber-espace avec le *big data*, l'Internet et les réseaux sociaux ont encore aggravé la situation. La sécurité se retrouve face à des attaques en tous genres contre lesquelles nos lois sont inadaptées et nos défenses balbutiantes. De l'escroquerie « au président », jusqu'à la menace de destruction de sites industriels, en passant par le détournement des formules de produits, le coût d'une agression dans le domaine de l'immatériel se révèle terriblement coûteux et parfois mortifère.

Face à cette évolution, le responsable de la sécurité doit en intégrer toutes les dimensions et le premier mérite de cet ouvrage est d'en faire une segmentation claire en 5 dossiers très différents et complémentaires. Dans chacun, on y trouve l'essentiel de ce qu'il faut savoir au niveau de la réalité et des actions à mener. Cela permet d'analyser objectivement toutes les situations pour construire des réponses adaptées aux problématiques. Je suis certain que cette boîte à outils va devenir indispensable à tous ceux en charge de ces activités et aux dirigeants qui veulent comprendre pourquoi la sécurité est en train de devenir une fonction essentielle de leur entreprise.

Enfin, il faut remercier les auteurs d'avoir ajouté en annexe le modèle d'analyse DIESE créé par la D2IE. Il permet de faire une analyse rapide de la situation sécuritaire de l'entreprise en la visualisant pour bâtir un programme d'amélioration et un plan d'action. Simple et efficace, son utilisation devrait être systématique dans toutes les petites et moyennes entreprises.

Alain Juillet
Président du Club des directeurs de sécurité des entreprises

Remerciements

Nous dédions cet ouvrage aux professionnels de la sécurité économique qui s'engagent au quotidien pour la protection du patrimoine scientifique, technologique et industriel, ainsi qu'à tous les citoyens qui se risquent à défendre nos intérêts dans un élan patriotique, synonyme d'ouverture au monde et non de repli sur soi.

Plus globalement, **nos pensées vont à celles et ceux qui ont risqué leur vie pour protéger les autres et c'est pourquoi nous avons souhaité reverser l'intégralité des droits d'auteurs de cet ouvrage à la fondation Maison de la gendarmerie**.

Nous tenons à remercier plus particulièrement :

› Alain Juillet, président du Club des directeurs de sécurité des entreprises.

› Claude Revel, déléguée interministérielle à l'Intelligence économique (D2IE – Premier ministre).

› Pascal Estève, lieutenant-colonel de gendarmerie, conseiller Sécurité économique et Intelligence territoriale à la D2IE, ainsi que Marie-Pierre Van Hoecke, conseiller senior, et Jérémy Jean-Jean, chargé de mission, créateurs de l'outil DIESE.

› Les généraux Christian Petit et Philippe Le Mouël, ainsi que le colonel Jean-Jacques Taché.

› Daniel Braud, président de la CCI Poitou-Charentes, ainsi que les membres du groupe technique national Intelligence économique (GTN IE) de CCI France, animé par Marc Giacomini et Pierre Batoche.

› Les initiateurs de l'antenne Intelligence économique de la région de gendarmerie Poitou-Charentes : Christian Vaury, Éric Fortin, David Girard et Laurent Beaulieu.

› Les dirigeants d'entreprises : Sandra Martin (Futuramat), Jean-Noël Pelletan (Tonnellerie JNP) et Michel Rousseau (SOS Data).

› IUT d'Angoulême : Thami Zeghloul, directeur, et Sébastien Soubie, responsable informatique.

› IUT de Poitiers : Pascal Martin, Lieutenant dans la réserve opérationnelle de la Gendarmerie nationale.

› Cécilia Rochefort et Arnault Varanne, journalistes.

Ainsi que tous ceux qu'il n'est pas possible de mentionner ici pour des raisons de sécurité nationale et notamment nos collègues de la DGSI…

Avant-propos

Mercredi matin, 8 h 30, au siège du MEDEF régional. La séance de sensibilisation à la sécurité économique va pouvoir commencer devant une trentaine de patrons de PME et une poignée d'institutionnels. Xavier, l'officier responsable de l'équipe de conférenciers de la Gendarmerie nationale, entre dans le vif du sujet : « Désormais, les attaques contre les entreprises se multiplient et aucune n'est à l'abri. Une entreprise française sur quatre en a été victime. Il est donc essentiel que vous ayez connaissance de l'ensemble des menaces existantes et des parades possibles. Tel est l'objectif de cette séance, qui pourra se poursuivre par un diagnostic de sécurité économique. » Le ton est donné.

Premier élément du décor : l'hyper-compétition et le défi de l'intelligence économique. Nicolas commence son exposé par le cas d'une PME empêchée de se développer sur un marché étranger en raison d'un mauvais usage de la propriété industrielle. Le patron de cette PME analyse comment il n'a pas su croiser l'information et la stratégie alors que son concurrent japonais a parfaitement su utiliser ses réseaux, pour se renseigner, puis faire un usage stratégique de la connaissance pour le paralyser. Dès lors, la sécurité doit être considérée de manière active, dans une dynamique d'ouverture, synonyme d'opportunités, et dans une prise en compte des risques liés à cette même ouverture.

C'est ensuite à Jacky d'intervenir sur le risque terrain qui correspond à l'attaque physique d'une entreprise. Des actions sous forme de sabotage de l'outil de production, de vol physique de données sensibles sur divers supports (dossiers, disques durs, ordinateurs portables…), de vol d'échantillons ou de prototypes, de pose de mouchards (micros, keyloggers…). Jean-Michel et Jérôme poursuivent sur le risque informatique, de plus en plus présent tant les attaques informatiques sont simples à concevoir et d'un coût peu élevé. Celles-ci visent à voler, exploiter, détruire, corrompre les données stratégiques, perturber voire bloquer le bon fonctionnement du réseau informatique d'un concurrent (déni de service). Chaque jour, on compte en France plusieurs millions de tentatives d'intrusion dans les systèmes d'information. Puis c'est à Éric d'aborder le risque humain qui englobe toutes les problématiques relatives à la vie des collaborateurs : débauchages opportuns, faux entretiens d'embauche, salariés espions, exploitation des faiblesses d'employés malléables (addictions), protestataires, démotivés… sans oublier les simples imprudences.

Enfin, François intervient sur la nécessité d'être en veille permanente et de mettre en œuvre un dispositif pour anticiper les mutations et transformer les risques en opportunités.

Marqués par les nombreux exemples donnés, parfois assortis de démonstrations d'attaques ou de petits films frappants, les chefs d'entreprise posent de nombreuses questions sur les bonnes pratiques à mettre en œuvre. Puis la séance est levée et chacun retourne à un quotidien très prenant.

Certains de la nécessité de ces séances de sensibilisation réalisées très régulièrement par les services de l'État dans chaque région de France, nos conférenciers de la gendarmerie savent que celles-ci ne sont pas suffisantes. En revenant de cette conférence, ils se disent qu'il manque un ouvrage pratique accessible à tous. C'est pourquoi ils vous proposent aujourd'hui cette *Boîte à outils de la sécurité économique*…

Les contributeurs

Cette *Boîte à outils de la sécurité économique* est une réalisation collective des membres de l'antenne Intelligence économique de la région de gendarmerie de Poitou-Charentes. Ont été en charge de la rédaction des dossiers et de la plus grande partie des outils :

Dossier 1

Jacky Sicard
Colonel dans la réserve citoyenne de la région de gendarmerie de Poitou-Charentes, il a effectué une carrière au sein de la gendarmerie d'active. Spécialiste Intelligence économique (conférences et audits d'entreprises), il est également « personne qualifiée » auprès de la commission de vidéosurveillance du département de la Vienne.

Dossier 2

Éric Gallot
Enseignant, chef d'escadron (ESR) de gendarmerie et diplômé d'État-major, spécialiste Intelligence économique (conférences et audits d'entreprises), il est affecté à l'antenne Intelligence économique de la région de gendarmerie de Poitou-Charentes. Il est auditeur de l'IHEDN.

Dossier 3 (et coordination de l'ouvrage)

Nicolas Moinet
Professeur des universités à l'institut d'administration des entreprises de Poitiers et lieutenant-colonel dans la réserve citoyenne de la Gendarmerie nationale, il est praticien-chercheur en intelligence économique. Directeur du master Intelligence économique et Communication stratégique du même IAE, il intervient depuis plus de vingt ans auprès des entreprises et des institutions publiques sur les questions touchant à la maîtrise et à la protection de l'information stratégique.

Dossier 4

Jean-Michel Lathiere
Adjudant-chef dans la Gendarmerie nationale, il est expert en cybercriminalité et spécialiste des systèmes d'information et de communication (SIC) auprès des entreprises. Il est titulaire du master Intelligence économique et Communication stratégique de l'IAE de Poitiers.

Jérôme Moreau
Maréchal de logis chef de réserve, il a passé 15 ans dans la sécurité informatique d'un groupe pharmaceutique. Il est maintenant directeur de whaller.com, plateforme de réseaux sociaux privatifs et sécurisés.

Dossier 5

François Baron
Responsable de l'intelligence économique au sein de la CCI Poitou-Charentes, il exerce le métier de conseil aux entreprises. Il a également exercé dans la formation et la recherche. Cet ouvrage s'inscrit dans le partenariat démarré en 2008 entre la CCI Poitou-Charentes et la région de gendarmerie de Poitou-Charentes.

Xavier Giloteaux
Officier de gendarmerie, en charge de l'intelligence économique au sein de la région de gendarmerie de Poitou-Charentes, il a exercé des responsabilités en matière de sécurité publique générale et de prévention de la délinquance sous toutes ses formes, au sein ou à la tête de compagnies de gendarmerie départementales. Il possède également des compétences dans les domaines de l'audit interne, du contrôle interne et de la prévention technique de la malveillance.

Au premier rang, de gauche à droite : François Baron, Xavier Giloteaux, Nicolas Moinet, Jacky Sicard
Au second rang, de gauche à droite : Jean-Michel Lathière, Jérôme Moreau, Éric Gallot

Autres contributeurs (par outil)

› Besnard Jean-Paul, référent sûreté affecté au groupement de gendarmerie de la Vienne (outils 4 et 5).

› Chardavoine Olivier, commandant de gendarmerie (outil 31).

› Maison Rouge (de) Olivier, avocat (texte réglementaire).

› Pascal Goubault, lieutenant de réserve de la gendarmerie nationale (outil 6).

Certaines fiches de cet ouvrage sont issues de la *Boîte à outils de l'intelligence économique* et ont été réécrites sur un mode plus sécuritaire. Ont donc également été sollicités les experts suivants : Camille Alloing (outil 33), Guilhem Armanet (outil 28), Pierre Breese (outil 49), Jean-Jacques Cambay (outil 32), Christophe Deschamps (outil 27), Pascal Junghans (outils 20 et 29), Terry Zimmer (outil 12).

Sommaire

La Boîte à outils, mode d'emploi

Les outils sont classés par dossier

DOSSIER 5

LA MAÎTRISE DES RISQUES ÉCONOMIQUES

« Les dangers visibles nous causent moins d'effroi que les dangers imaginaires. »
William Shakespeare

L'ouverture des frontières économiques, l'interdépendance croissante des acteurs économiques, la vitesse des changements, le développement exponentiel du numérique forment un environnement incertain et rendent la prise de décision et la conduite de l'entreprise de plus en plus complexes. Au cours de sa vie, l'entreprise fait face à, provoque ou rencontre de multiples événements intérieurs ou extérieurs qui présentent de nombreux risques pouvant nuire à ses intérêts. Identifier ces risques et les maîtriser est donc vital et stratégique pour nos entreprises, notamment les PME, PMI et ETI. Nos entreprises ne peuvent pas être compétitives sans une approche optimale des risques économiques dans leur globalité.

Ainsi, l'entreprise pour se développer doit « se connaître », c'est-à-dire identifier ses spécificités, ses savoir-faire, sa singularité (outil 50). Pour aider à construire sa stratégie, le chef d'entreprise et ses cadres peuvent entreprendre une démarche interne d'évaluation de la maîtrise des risques économiques (outil 46) auxquels elle s'expose. Cette démarche revêt un caractère stratégique et, pour cela, nécessite d'être renouvelée tous les 4 à 5 ans.

Afin d'identifier et de suivre les parties prenantes à l'intérieur de l'entreprise (organisation et ressources internes) ou à l'extérieur (concurrents, fournisseurs, partenaires, etc.), mettre en place une veille stratégique (outil 52) revêt un intérêt constant. En effet, les informations porteuses de rupture telles que les informations techniques, commerciales, légales et réglementaires, ou relatives aux modes et coutumes, vont alimenter le pilotage stratégique de l'entreprise.

Cette démarche de veille stratégique va également contribuer à alimenter une façon de faire spécifique : l'évaluation des profils et des intentions des parties prenantes. Cette démarche est essentielle. Elle permet par une consolidation et une analyse de multiples faits issus de la veille de construire des batteries de profils des acteurs clés et des scénarios d'intentions de ces acteurs. Ainsi se révèlent les stratégies en œuvre et les actions opérationnelles qui en découlent.

Sont également abordés dans ce dossier les points relatifs à la sécurisation des informations et des innovations de l'entreprise : de l'enveloppe Soleau (outil 48) qui date une création, au brevet (outil 49) qui « protège et rapporte à la fois », en passant par la confidentialité (outil 51).

Plus l'environnement est riche, mouvant et complexe, plus les risques économiques croissent, et les petites et moyennes entreprises en sont les premières victimes. Elles pourront solliciter les services de l'État dans leurs champs d'intervention présentés (outil 54). Sur l'information, le conseil et l'accompagnement, une entreprise pourra faire appel aux opérateurs de proximité que sont les structures de conseil et d'appui aux entreprises, comme les CCI (outil 55).

Enfin, cette démarche d'évaluation et de maîtrise des risques économiques, portée par le chef d'entreprise, doit être dans tous les esprits des collaborateurs.

Ces outils, sous forme de fiches non exhaustives, représentent un socle de travail sur lequel vous pourrez vous appuyer pour démarrer ou améliorer la mise en pratique de la maîtrise des risques économiques de votre entreprise.

LES OUTILS

L'intérêt de la thématique vu par un expert

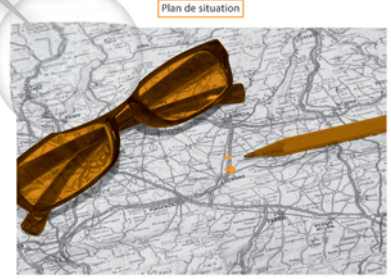
Un menu déroulant des outils

OUTIL 9

Le plan de contre-intrusion

SE PRÉPARER POUR MIEUX PARER

Plan de situation



➔ Emplacement de l'entreprise
Point d'observation

En résumé

Dans son plan de contre-intrusion, le chef d'entreprise doit viser deux objectifs. Tout d'abord la dissuasion avec, s'il échoue sur ce point, la mise en échec des intrus afin qu'ils ne puissent atteindre le but qu'ils se sont fixés, lequel risquerait de porter atteinte à son outil de production.

Insight

A CEO's counter-intrusion strategy should aim for two objectives. Dissuasion comes first. If it fails, intruders should at least be thwarted from achieving their goal, which would otherwise damage your firm's productive capacity.

La représentation visuelle de l'outil

L'outil en synthèse

L'essentiel en anglais

OUTIL 9

Pourquoi l'utiliser ?

Objectif

Le plan de contre-intrusion formalise l'ensemble des moyens que compte mettre en œuvre l'entreprise pour faire échec à toute intention de pénétration malveillante sur son site.

Contexte

Afin de s'approprier le savoir-faire d'une entreprise ou des informations devant rester confidentielles, plusieurs solutions s'offrent à ceux parés d'intentions malveillantes. Ils peuvent s'attaquer à l'entreprise de façon sournoise, en utilisant à distance les moyens techniques de communication (Internet) ou les faiblesses de personnels de l'entreprise, ou encore en profitant des entreprises extérieures venant réaliser des prestations sur son site. Mais ils peuvent aussi s'introduire en force sur son site pendant les moments de fermeture, en l'absence de tout personnel. Pour lutter contre cette seconde éventualité, le chef d'entreprise doit mener une réflexion sur les moyens à mettre en place pour dissuader de toute intrusion.

› un contrôle draconien des accès tel que conseillé dans l'outil 3 du présent ouvrage sur le contrôle d'accès ;
› la mise en place de barrières physiques comme précisé dans l'outil 2 sur les barrières physiques ;
› l'annonce dissuasive du dispositif en place pour lutter contre les intrusions, telle préconisée également dans l'outil 2.

Méthodologie et conseils

Avec ces atouts, il est certain que bon nombre de renoncements seront obtenus. Toutefois, ils ne suffiront pas à décourager des malfaiteurs très déterminés. Néanmoins, s'il ne parvient pas à empêcher l'intrusion, le dispositif doit rendre impossible, ou du moins particulièrement difficile, d'atteindre les différents points stratégiques de l'entreprise présentant peut-être une importance capitale pour son fonctionnement. Ce seront en effet les barrières physiques en place qui le permettront : sirène du système d'alarme, dispositifs équipés d'un générateur de brouillard, etc.

Le plan de contre-intrusion doit prévoir toutes les possibilités

Une signalétique claire

Les apports de l'outil et ses limites

Comment l'utiliser ?

Étapes

Cette réflexion doit porter sur deux possibilités : le dispositif de contre-intrusion destiné à dissuader ou à faire échec aux intrus la réaction face à une intrusion. Il convient s'appuyer sur le postulat que toute intrusion à des fins malveillantes et précises est généralement précédée d'un ou de plusieurs repérages pour définir le mode d'action à adopter et les risques encourus. En conséquence, une bonne dissuasion peut éviter l'intrusion. Un effort particulier doit donc être fait sur les points suivants :

Avantages

- Limiter au maximum les prises de risques suite au déclenchement du dispositif d'alarme.
- Réagir rapidement, efficacement et en sécurité en cas d'intrusion.

Précautions à prendre

- Les personnels chargés d'intervenir doivent parfaitement connaître le plan de contre-intrusion.
- Ne pas intervenir seul pour réaliser une levée de doute.
- Être doté d'un moyen de communication pour être en contact avec la direction ou un autre personnel non engagé.

SUITE OUTIL 9 ➔

OUTIL 11

L'ingénierie sociale ou « *social engineering* »

Comment être plus efficace ?

L'ingénierie sociale est aussi appelée **processus « d'élicitation »** (de « éliciter » : tirer, faire sortir de, susciter, terme souvent utilisé dans le jargon informatique pour désigner un **processus d'approche relationnel frauduleux** et qui définit plus globalement les méthodes mises en œuvre par certains hackers (catégorie des black hats), qui usent « d'élicitation » pour obtenir d'une personne manipulée un accès direct à un système informatique ou, plus simplement, pour satisfaire leur curiosité.

Pour l'attaquant, cette méthode reste peu [illegible] dont les résultats [illegible]ntis, elle ne sera [illegible] victimes étant peu [illegible] imprudence. [illegible]ce à ces attaques, [illegible]

[illegible]otentielles au sein

- le **support informatique** car on l'appelle pour lui demander de l'aide, souvent en cas de perte de mot de passe ;
- les **utilisateurs de services en ligne** qui ont, en général, une mauvaise connaissance des habitudes des sociétés ;
- les **utilisateurs réguliers des SI** qui connaissent l'organisation d'une société, les procédures. Cette cible permet à l'attaquant d'assembler un annuaire bien renseigné ;
- les **nouveaux utilisateurs ou utilisateurs occasionnels** (nouveaux employés, stagiaires) qui ne connaissent pas le fonctionnement de la société. Leur sensibilisation s'avère inexistante ou naissante ;
- les **personnels très actifs sur les réseaux sociaux** qui dévoilent facilement leur vie privée et celle de leurs collègues. De plus, le fait que nombre de sites Internet conservent des informations confidentielles sur les individus accroît aujourd'hui cette vulnérabilité.

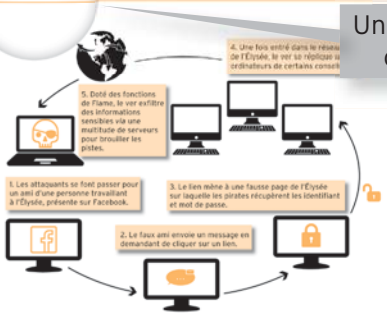
› **De connaître les différents leviers d'attaque possibles :**

- **Amitié et coopération :** l'empathie, la détresse, la culpabilité… Il faut pour cela connaître le contexte de la cible, ainsi que certains aspects personnels du sujet. Cette méthode est relativement discrète mais nécessite souvent plusieurs tentatives.
- **Usurpation d'identité et intimidation :** méthode un peu plus risquée que la précédente. Il faut disposer d'un annuaire bien renseigné sur la société, de son organigramme. Cette méthode est plus rapide puisque, dans la mesure où cette méthode est agressive, un seul essai est possible.
- **Sabotage :** vise les administrateurs. Il s'agit de se faire connaître comme l'interlocuteur adéquat en cas de problème du SI. L'attaquant profite alors de la confiance instaurée. Cette méthode est peu discrète mais efficace.
- De plus, **la vitesse du média utilisé est très importante :** le téléphone est le plus efficace ; le mail permet le *phishing* (fausses pages web incitant les victimes à cliquer sur un lien les entraînant sur un site infecté). Il faut aussi se méfier des pièces jointes qui, si on les ouvre, installent sur votre poste un cheval de Troie permettant de prendre la main sur celui-ci à distance et d'avoir accès à tous vos fichiers et au serveur de l'entreprise.

Un approfondissement pour être plus opérationnel

OUTIL 11

CAS de L'Élysée victime de l'ingénierie sociale[1]



En 2012, **les méthodes de l'ingénierie sociale (en particulier l'usurpation d'identité)** ont permis à des pirates d'entrer dans le réseau informatique de l'Élysée, c'est-à-dire au cœur du pouvoir politique français. Des notes secrètes, des plans stratégiques ont pu ainsi être récupérés par les attaquants.

Grâce à Facebook, ils ont pu reconstituer un organigramme assez complet des personnels travaillant à l'Élysée. Par le procédé du *phishing*, ils récupèrent l'identifiant et le mot du passe de la personne attaquée. Sous cette fausse identité, ils pénètrent dans le système informatique de l'Élysée et ont accès à l'ensemble du réseau. L'usurpation d'identité se fait grâce à un logiciel téléchargeable sur Internet.

Comment se protéger contre de telles attaques ?

› Ne pas ouvrir de pièces jointes d'origine douteuse (dont on ne connaît pas l'expéditeur).
› Si l'auteur du mail est connu, **la seule solution pour déjouer l'usurpation d'identité** est de demander un mail ou un SMS de confirmation. Éventuellement de mettre au point une question mémorable ou un mot de passe entre collègues. ■

Un cas pratique commenté

1 Cette offensive a été découverte entre les deux tours de l'élection présidentielle de 2012.

DOSSIER 1

LA **SÉCURITÉ PHYSIQUE** DES **LOCAUX** ET DES **MATÉRIELS**

« C'est terrible de se laisser prendre dans sa routine, on s'enlise, on se sent en sécurité. Et puis, tout à coup on s'éveille et il n'y a plus rien. »
Yves Thériault

Le chef d'entreprise doit constamment s'investir pour améliorer sa production afin de conquérir des marchés et améliorer son chiffre d'affaires. Ses activités et les études qu'il réalise pour se développer sont susceptibles de gêner les concurrents. Elles peuvent susciter des convoitises de leur part et le désir de se les approprier.
Si certaines attaques peuvent être réalisées de façon sournoise, en s'appuyant sur le facteur humain (interne et externe à l'entreprise) ou sur les nouvelles technologies (moyens informatiques, Internet, etc.), d'autres peuvent avoir lieu de manière brutale, avec une intrusion physique dans l'entreprise, le plus souvent à la faveur des moments de fermeture (nuit, week-ends, vacances...).
S'il veut se prémunir contre les intrusions, le chef d'entreprise doit se garantir en faisant un effort sur les différents points développés dans le présent dossier.
Il doit :

› tout d'abord réaliser **une auto-évaluation sur la sécurité physique** de son entreprise afin d'en dégager les points faibles ;

› mettre en place ou renforcer **les barrières physiques** pour au mieux dissuader voire, au pire, repousser les éventuelles tentatives d'intrusion avant que les auteurs n'aient pu atteindre leur objectif ;

› faire **contrôler les accès** de son entreprise, action constituant un critère de sérieux et de rigueur en matière de sécurité ;

› au besoin, ne pas hésiter à faire installer un dispositif de **vidéosurveillance**, pour renforcer son dispositif d'alarme et dissuader des éventuels projets d'intrusion et, au pire, faciliter l'identification des auteurs ;

› selon son type d'activité, réserver l'accès à certains lieux, ou locaux, aux personnels « sélectionnés » en se dotant de moyens modernes, s'appuyant sur leur **identification biométrique** ;

› savoir que le développement du **zéro papier,** s'il favorise l'activité d'une entreprise, n'en demeure pas pour autant sans risque ;

› assurer la meilleure protection des documents et/ou matériels sensibles en se dotant d'une **armoire forte** (ou d'un coffre-fort) et en l'installant au meilleur emplacement, afin de la rendre difficilement vulnérable ;

› se doter et faire utiliser une **broyeuse de documents** pour assurer la meilleure destruction possible de documents mis à la poubelle, dont on ne connaît pas toujours la destination ;

› mener enfin une réflexion et élaborer un **plan de contre-intrusion** à partir des mesures de protection mises en place dans l'entreprise pour se préparer à toute attaque et, si possible, y faire échec.

LES OUTILS

OUTIL 1

L'auto-évaluation de sécurité physique

C'EST EN CONNAISSANT SES FAIBLESSES QU'ON PEUT Y APPORTER DES SOLUTIONS

En résumé

Il est important pour une entreprise de prendre des mesures concernant la sécurité physique de son site (outils 1 à 9).

Le questionnaire proposé permet d'évaluer le niveau de protection physique de l'entreprise et surtout de faire prendre conscience de la nécessité de prendre des mesures si besoin.

Insight

Every company should adopt a series of measures to ensure its facilities' physical security (see tools 1 to 9).

The proposed questionnaire can help your company evaluate its degree of physical protection, and point out the need of taking additional steps if necessary.

OUTIL 1

Pourquoi l'utiliser ?

Objectif

L'outil présenté est un **questionnaire d'auto-diagnostic** destiné aux dirigeants souhaitant assurer la meilleure protection de leur entreprise, afin de préserver leur savoir-faire et leur outil de production. De nombreux aspects seront développés tout au long de ce dossier.

Contexte

De nombreuses entreprises subissent les conséquences d'une protection physique insuffisante. Quelles sont les dispositions matérielles et pratiques qu'il convient de mettre en œuvre pour l'améliorer ?

Comment l'utiliser ?

Étapes

Cet outil (voir grille ci-après) permet d'aborder le sujet des vulnérabilités physiques et de se poser un certain nombre de questions simples en évaluant de façon toute relative le niveau de protection ou de vulnérabilité de l'entreprise :

› Les **vulnérabilités physiques d'une entreprise** ont ici été numérotées de 1 à 12 en tournant dans le sens des aiguilles d'une montre.

› **À chaque question**, chacun choisira d'attribuer une note de 0 à 5. Plus le chiffre donné est élevé, plus l'entreprise est exposée au risque physique d'intrusion.

› **Le nombre total de points** indique le niveau de vulnérabilité de l'entreprise.

› **Si des vulnérabilités sont constatées avec ce premier outil**, il faudra se reporter aux autres outils du dossier 1 pour prendre les mesures qui s'imposent.

Méthodologie et conseils

› Sachant que les dirigeants d'entreprise ont peu de temps à consacrer à la sécurité de leur entreprise – bien que cela soit pourtant un enjeu majeur – ce questionnaire se doit d'être simple et rapide à compléter. De ce point de vue, l'utilisation de l'**outil DIESE**, développé sous l'égide de la délégation interministérielle à l'Intelligence économique est à recommander. Gratuit, il est présenté en annexe de cet ouvrage.

› Il peut être l'occasion, dans un second temps, de faire appel aux services de l'État compétents en la matière qui se déplaceront dans l'entreprise, examineront plus en détail les vulnérabilités (bilan de vulnérabilités) et proposeront des améliorations.

Vous assurerez la protection de votre outil de production en renforçant la sécurité de vos locaux industriels.

Avantages

- Donne un premier aperçu de son niveau de sécurité à l'abri des regards.
- Permet d'enclencher une prise de conscience de ses vulnérabilités.

Précautions à prendre

- Ce questionnaire n'a pas l'ambition d'être exhaustif. Il ne faut donc pas penser qu'on a fait le tour de la question en y répondant.
- Les mesures à prendre pour limiter les vulnérabilités humaines sont propres à chaque entreprise et doivent s'adapter et évoluer en fonction du contexte.

SUITE OUTIL 1 ➔