©angus

SÉCURITÉ ÉCONOMIQUE : l'indiscrétion et la malveillance guettent...

Interview de Jérôme Saiz, consultant au sein de la société OPFOR Intelligence*
Par Marc Jacob et Emmanuelle Lamandé

Garder la maîtrise de son information stratégique et de ses savoir-faire quand on est une entreprise n'est pas de tout repos, d'autant que l'indiscrétion et la malveillance guettent de toutes parts. Comment s'assurer que le savoir et le savoir-faire qui font la valeur de son organisation ne tombent pas entre les mains de ses concurrents ou de toutes personnes mal intentionnées ? Quelles sont les clés d'une sécurité économique efficiente ?

Global Security Mag : Comment définiriez-vous la sécurité économique aujourd'hui et ses champs d'action ?

Jérôme Saiz : Si l'on ne parle que de sécurité économique, il s'agit alors avant tout de la maîtrise de l'information stratégique. S'assurer, sur tous les plans (humains, technologiques, juridiques) et de manière coordonnée, que le savoir et le savoir-faire qui font la valeur de l'entreprise ne sont pas aisément accessibles à ses concurrents, y compris s'ils décident d'avoir recours à des moyens illégaux.
Si l'on étend la définition au concept d'Intelligence Économique, il s'agit alors dans le même temps d'organiser l'entreprise afin qu'elle soit en mesure, par des moyens légaux, de mieux lire la carte du champ de bataille économique, qu'elle soit mieux informée des risques inhérents à ses projets, des intentions de ses concurrents, et globalement, qu'elle soit mieux équipée dans sa prise de décisions stratégiques, afin, par exemple, d'aborder plus sereinement un nouveau marché ou un nouveau partenariat.

Du vol d'informations et de savoir-faire aux tentatives d'influence et de sabotage

GS Mag : Quelles sont les principales menaces auxquelles les administrations et les entreprises françaises doivent faire face dans ce domaine ?

Jérôme Saiz : Il s'agit évidemment avant tout du vol d'informations propriétaires et du savoir-faire, qui peut prendre de très nombreuses formes, et que j'aborderai ultérieurement.
Mais il ne faut pas négliger pour autant toutes les manœuvres qui peuvent être menées par un adversaire pour s'offrir une position avantageuse de manière illégale, dissimulée ou irrégulière.
En fonction des enjeux et des moyens dont dispose l'adversaire, cela peut passer par de l'influence lors de la définition de normes (européennes, notamment), du harcèlement juridique, du sabotage (par exemple pour empêcher de déposer une proposition dans les délais impartis), du vol d'informations au sujet d'une négociation en cours, de l'organisation de campagnes de dénigrement (en particulier sur les réseaux sociaux, devenus un incroyable terrain de jeu en la matière), et jusqu'à des actions physiques menées contre les négociateurs afin de perturber une négociation commerciale importante et, là aussi, faire rater des échéances ou des rendez-vous cruciaux.
L'une des principales difficultés tient au fait que ces menaces portent en définitive sur tous les domaines : informationnels, technologiques, humains, juridiques. Et l'attaquant ne se prive pas de les exploiter indifféremment ou successivement, lançant une attaque dans l'un de ces domaines afin de faciliter la suivante, qui portera sur un autre (je pense en particulier à une intrusion physique par ruse qui facilitera grandement un piratage numérique). Malheureusement, les entreprises sont quant à elles encore trop souvent organisées en silos, ce qui ne facilite pas l'articulation de la défense sur le même modèle.
Il me semble donc important de souligner, au-delà des principales menaces exogènes que nous venons de décrire, cette menace endogène, liée à la manière dont l'entreprise structure sa défense, et qui demande de sa part une véritable évolution culturelle. Les choses ont heureusement tendance à avancer en la matière, mais ce n'est malheureusement pas encore la norme.

GS Mag : Quels impacts l'essor du numérique a-t-il eu sur les risques et enjeux inhérents à cette sécurité économique ?

Jérôme Saiz : Quelle valeur de l'entreprise n'est à aucun moment touchée par du numérique ? Aucune. Le numérique irrigue l'entreprise

à tous les étages, dans toutes ses activités et dans toutes ses relations. Et cela ne va pas aller en diminuant ! L'impact du numérique est donc évidemment profond et durable.
C'est pourquoi en matière de sécurité, le numérique, qui véhicule toute la valeur de l'entreprise, sa connaissance, ses projets et ses secrets, devient naturellement un élément critique à protéger et à surveiller activement.

Quiconque a accès à l'information recherchée est susceptible d'être le vecteur d'une action malveillante

GS Mag : Quels sont généralement les profils des acteurs malveillants qui tentent de mettre à mal aujourd'hui cette protection des actifs et informations stratégiques en entreprise ?

Jérôme Saiz : Très variés ! Mais il convient d'abord de distinguer les commanditaires des exécutants. Les commanditaires sont plus rarement identifiés, mais l'on peut évidemment citer des États étrangers ou des entreprises privées concurrentes.
Concernant les exécutants, en revanche, tout est possible, et c'est bien ce qui rend la prévention si délicate. En généralisant, on peut dire que l'on peut avoir affaire à tout le spectre des compétences, depuis les professionnels d'un service de renseignement étranger jusqu'au voyou recruté pour une effraction pas très fine.
Et entre les deux, on peut trouver de tout : des avocats, des sociétés de sécurité ou des enquêteurs privés (dans les deux cas, peu scrupuleux), des voyous, et ensuite tous ceux qui ont accès à l'information recherchée, chez la victime ou ailleurs : un comptable, des commerciaux, l'employé d'un opérateur téléphonique (lorsqu'il s'agit de se procurer la facture détaillée d'une cible, un grand classique), etc.
En bref : quiconque a accès à l'information recherchée et souffre d'une vulnérabilité (une faiblesse personnelle) connue de l'adversaire est susceptible d'être le vecteur d'une action malveillante. Y compris malgré lui !
Mais si l'on cherche un cas d'école plausible, on peut mentionner le mille-feuille bien connu : l'avocat du commanditaire va servir d'intermédiaire avec une société de sécurité privée, qui va elle-même sous-traiter à des « freelances » aux expertises diverses (eux-mêmes n'hésitant pas à embarquer d'autres freelances dans la mission). Et les discussions entre le commanditaire et son avocat passeront préférablement par le responsable de son service de sécurité interne. En cas de poursuites judiciaires, cela permet à chaque niveau de nier avoir eu connaissance du détail des pratiques de l'étage inférieur et, bien entendu, de les désapprouver.
Attention toutefois à préciser que nous sommes ici dans le cadre de la malveillance, qui repose donc sur des pratiques illégales. Ce ne sont évidemment pas les méthodes de travail des nombreux cabinets d'Intelligence Économique respectueux des lois, qui se sont d'ailleurs organisés en un syndicat chargé d'élaborer une charte de déontologie pour la profession (le SYNFIE).

La sécurité économique va de pair avec le patriotisme économique

GS Mag : Quel état faites-vous du niveau de maturité actuel de la France en la matière ? Quels sont les pays les plus en avance sur ces sujets ?

Jérôme Saiz : À l'échelle d'un pays, la sécurité économique va de pair avec le patriotisme économique. Les pays les plus « économiquement patriotes » (tout simplement ceux dont les citoyens ne se sentent pas déconnectés de la vie économique, mais ont conscience de participer activement à sa réussite) sont mécaniquement plus avancés que nous. Je pense notamment à l'Allemagne ou au Japon, qui sont deux cas d'école régulièrement étudiés durant les formations en Intelligence Économique.
Ensuite, les pays anglo-saxons sont eux aussi naturellement avantagés. La culture du renseignement y est moins taboue que chez nous et fait l'objet d'études universitaires, et les liens avec le privé sont plus poreux.
Mais cela ne signifie pas pour autant que la France est mauvaise élève ! Certes, les pérégrinations de « l'Intelligence Économique à la Française » ne sont pas de tout repos : changement de tutelle, changement de nom (l'on devrait d'ailleurs désormais plutôt parler « *d'information stratégique et de sécurité économique* »), et sentiment qu'il a pu parfois manquer d'un pilote. Mais nous avons aussi la chance de nous appuyer sur plusieurs rapports fondateurs (Martre, dès 1994, Carayon, en 2003…) qui ont marqué l'effort de l'État en la matière. Un effort qui se poursuit aujourd'hui sous l'égide de la Direction Générale des Entreprises, à Bercy. Nous bénéficions aussi d'un maillage territorial fort, notamment grâce à la Gendarmerie Nationale, qui œuvre à la fois dans le domaine de la sécurité économique et de la sûreté au profit des entreprises locales. Sans oublier non plus l'action des CCI sensibilisées sur le sujet, et du Ministère de l'Intérieur.
Enfin, nous avons la chance de bénéficier de très bonnes formations en la matière, telles que celle de l'INHESJ (Institut national des hautes études de la sécurité et de la justice) basée à l'École Militaire, ou encore celle de l'EGE (École de Guerre Économique), ainsi que d'auteurs prolifiques qui contribuent à alimenter la réflexion sur le sujet (Christian Harbulot, Nicolas Moinet, Éric Delbecque…).
Bref, la matière et la réflexion ne manquent pas. Mais peut-être, et comme souvent en France, nous manque-t-il juste un peu de pragmatisme pour décliner tout cela de manière vraiment opérationnelle au sein des entreprises !

Thema
ECONOMIC SECURITY

Economic security: gaffes and grudges lying in wait ...

*Interview with Jérôme Saiz, consultant at OPFOR Intelligence **
By Marc Jacob and Emmanuelle Lamandé

Keeping control of strategic enterprise information and know-how is not easy, especially with the risk of gaffes and grudges lying in wait inside and out. How can you ensure that the knowledge and skills that make up the value of your organisation do not fall into the hands of your competitors or those who would do harm? What are the keys to efficient economic security?

©angus

GS Mag : Quels sont généralement les points sensibles que les entreprises françaises tendent à négliger ?

Jérôme Saiz : Ils seront très différents d'une entreprise à l'autre, car très dépendants de son activité et de son niveau de maturité. Et c'est d'ailleurs justement le rôle du consultant sécurité/sûreté que d'adapter les évidences à la réalité de son client. Je me contenterai donc plutôt de citer les points de vigilance les plus communément oubliés ou mal mis en œuvre.

Ce sont là de grands classiques de l'IE, sans grande originalité, et la liste n'est évidemment pas exhaustive !

- L'accueil des visiteurs ;
- L'encadrement des stagiaires (dont la relecture de leur rapport avant publication) ;
- L'accueil des délégations étrangères ;
- Les déplacements à l'étranger, en particulier le passage de frontières ;
- Les discussions entre collègues dans un lieu public (le train, le restaurant-cantine du midi à proximité des locaux, etc.) ;
- La participation aux salons professionnels (une hécatombe !) ;
- L'utilisation de locaux en coworking pour les startups innovantes ;
- La sensibilisation des collaborateurs aux faux entretiens de recrutement (un salarié qui n'a pas été sensibilisé est quasiment assuré de tomber dans le piège) ;
- La politique de gestion des équipements informatiques en déplacement (non, un coffre d'hôtel n'est pas une protection suffisante, et non, tant que l'ordinateur n'est pas totalement éteint, on ne peut compter sur le chiffrement intégral du disque dur) ;
- Les concours internationaux montés de toutes pièces par un adversaire et qui exigent, pour participer, de communiquer beaucoup trop d'informations.

Évidemment, il est absolument nécessaire de commencer par une analyse des risques, afin d'identifier les points faibles à corriger en priorité.

GS Mag : Quels sont les acteurs et organismes français qui peuvent accompagner les entreprises aujourd'hui dans leurs démarches ? De quelles manières ?

Jérôme Saiz : Le dispositif français d'Intelligence Économique est aujourd'hui piloté par la Direction Générale des Entreprises, au sein du ministère des Finances, à travers le SISSE (Service de l'Information Stratégique et de Sécurité Économique). Un Commissaire à l'Information Stratégique et à la Sécurité Économiques veille au « *pilotage interministériel de la politique publique en matière de protection et de promotion des intérêts économiques, industriels et scientifiques de la Nation* », selon la formule officielle.

Sur le terrain, et en particulier localement, la Gendarmerie Nationale est un acteur de proximité incontournable car au contact des PME (qui constituent l'essentiel de notre tissu économique), qu'elle informe, sensibilise et alerte en matière d'IE et de sûreté. Évidemment, cela est très dépendant de la disponibilité d'effectifs formés, qui n'est hélas pas toujours suffisante pour permettre de suivre les PME locales avec autant d'application que l'institution ne le souhaiterait. Mais le territoire est vaste !

Si la Gendarmerie s'adresse essentiellement aux PME en régions, au sein du ministère de l'Intérieur, la DGSI entretient des contacts étroits avec les grands groupes français du CAC 40 et dispose d'une section de conférenciers dédiés dont les interventions de sensibilisation sont réputées pour leur efficacité (ce qui, au demeurant, n'empêche évidemment pas les antennes régionales de la DGSI d'identifier et de soutenir de petites PME innovantes à protéger de manière plus ciblée).

Enfin, tout ce petit monde se retrouve à l'occasion de nombreux événements, organisés partout en France par des CCI, des préfectures ou la DIRECCTE locale (Direction régionale des entreprises, de la concurrence, de la consommation, du travail et de l'emploi).
Là encore, il s'agit avant tout de sensibiliser les chefs d'entreprise et leurs cadres aux risques, bien réels, d'ingérence économique.

Enfin, des organisations, telles que la CPME, le MEDEF ou d'autres associations professionnelles verticales, adressent régulièrement la question auprès de leurs membres.

Avant tout, sachez où vous mettez les pieds !

GS Mag : Quelles sont les étapes essentielles à mettre en œuvre, selon vous, dans toute démarche de sécurité économique et quelles sont vos recommandations en la matière ?

Jérôme Saiz : Avant tout, savoir où l'on met les pieds ! Une démarche de sécurité économique n'a rien d'anodin : elle doit parvenir à faire converger une volonté forte de la Direction avec les capacités d'une organisation pour atteindre des objectifs opérationnels qui se traduiront de manière très concrète par, évidemment, une réduction de son exposition aux risques d'ingérence et de vol d'informations, notamment lors de l'approche de nouveaux marchés ou de nouveaux partenaires. Mais également, si l'on se place dans une optique plus large d'Intelligence Économique, une plus grande agilité, une meilleure réactivité et une capacité de prise de décision améliorée (plus rapide, plus rationnelle).
Il s'agit donc de plonger au cœur de l'organisation (parce que l'IE n'est pas seulement le travail d'une équipe en vase clos) et de sa culture. Et pour tout cela, il faut de la visibilité sur ce que celle-ci fait déjà en matière de veille, de partage, d'exploitation et de protection (ou non !) de l'information. Et ce que ses décideurs en attendent réellement !
En outre, un certain nombre d'entreprises appliquent déjà sans le savoir certaines pratiques de l'Intelligence Économique, mais de manière non structurée. Il convient donc d'abord d'avoir une bonne visibilité sur l'existant et sur la culture maison vis-à-vis de l'information. Et cela passe forcément par beaucoup d'entretiens.

Le reste est une démarche de structuration et d'outillage de la collecte, de l'analyse et de la diffusion (je préfère même parler d'appropriation) de l'information. C'est généralement un travail de consultant au contact de la direction générale, des décideurs et des différentes parties prenantes qui auront à exploiter l'outil ou à en « consommer » le produit fini.

Plan de sûreté : tout repose sur la force de l'ensemble

GS Mag : Quelles sont vos préconisations en matière de sécurité physique et de protection bâtimentaire ?

Jérôme Saiz : La définition d'un plan de sûreté est un exercice

complexe qui dépasse le cadre de ces lignes et ne saurait être générique. Mais je mettrai l'accent sur trois points essentiels.

En premier lieu, être cohérent et réaliste. Par exemple, les meilleurs blocs-portes du marché résisteront en moyenne 15 minutes face à un attaquant confirmé et bien équipé. À moins de vouloir sécuriser la salle des coffres d'une banque, on ne trouvera pas mieux.
Cela peut sembler faible, et bien loin des résistances affichées par certains catalogues grand public peu sérieux, qui peuvent atteindre des heures. Mais contrairement aux annonces purement marketing, il s'agit là d'une résistance éprouvée en laboratoire (et qui sera, évidemment, bien meilleure face à un adversaire moins compétent).
Et puis, surtout, ces 15 minutes ne doivent pas être considérées de manière isolée. Elles font partie d'un plan de protection plus global. Ainsi, peut-être qu'en amont un détecteur sismique sensible aux mouvements et intégré à une clôture intérieure a permis de donner silencieusement l'alerte. Une alerte qui a été confirmée grâce à un réseau de capteurs (optiques ou sonores) bien pensé. Et qu'il faut à partir de ce moment précis moins de 20 minutes à un équipage de sécurité pour être dépêché sur les lieux. Dans ce cas, la résistance mécanique de la porte est adéquate.
Ou peut-être que derrière cette porte se trouve en outre un dispositif fumigène qui empêchera les intrus de mettre la main sur ce qu'ils sont venus chercher ou les retardera plus encore, tandis que les forces de l'ordre seront déjà en route après confirmation de l'intrusion par des moyens électroniques.
En réalité, le moment de la première détection (le plus en amont possible), le temps de résistance mécanique et le temps d'intervention sont trois paramètres liés. Ils composent une équation globale qui doit être équilibrée et cohérente. Pris de manière isolée, aucun de ces éléments n'est véritablement suffisant. Mais c'est leur bonne association, dans une stratégie cohérente, qui fait la force de l'ensemble.

En second lieu, j'insisterai sur l'importance du zonage à l'intérieur des locaux et de l'accueil des visiteurs. Une bonne politique d'accueil et d'accompagnement des visiteurs, avec une définition claire et intelligente des différentes zones, associée à des listes de contrôle d'accès cohérentes, permettra de réduire considérablement la marge de manœuvre d'un éventuel visiteur égaré (et cela va de pair avec la sensibilisation des collaborateurs qui découvriraient un « externe » dans de telles zones privées, et dans certains cas d'une politique de « bureaux propres » régulièrement testée).
À titre d'exemple, j'ai rencontré une société dont la salle d'attente des visiteurs servait également à stocker provisoirement le courrier sortant. C'est une faute de zonage qui peut avoir des conséquences graves.

Enfin, il me semble indispensable de former les personnels de la sûreté aux nouveaux risques numériques. Il est par exemple devenu excessivement simple de contourner l'essentiel des protections numériques périmétriques mises en œuvre par l'entreprise en introduisant frauduleusement un équipement de type Raspberry Pi ou Teensy spécialement modifié (ou même d'autres, dédiés au hacking, disponibles clés en main sur Internet pour moins d'une centaine d'euros).
Il est donc important que les agents de sûreté (mais aussi d'entretien !) sachent à quoi cela peut ressembler et comment réagir s'ils découvrent un tel équipement dans un recoin de bureau, une salle machines ou lors d'une inspection visuelle des sacs (ce qui est d'ailleurs déjà arrivé avec un équipement d'interception radio).

Vos collaborateurs constituent des « capteurs » d'informations idéaux

GS Mag : Quels acteurs doivent être impliqués au sein de l'entreprise ?

Jérôme Saiz : Tous ! À des degrés divers, bien entendu, mais il est important que l'entreprise sensibilise largement à ces thématiques. Les collaborateurs, par exemple, sont en première ligne et constituent des « capteurs » d'informations idéaux (ce sont bien souvent eux qui sont les premières victimes des diverses tentatives de manipulation, ou qui sont les mieux placés pour observer quelque chose d'inhabituel). Mais ils ne bénéficient pas toujours des moyens adéquats pour remonter cette information aisément et rapidement.

Ensuite, je suis un fervent défenseur d'une approche pluridisciplinaire de la protection de l'entreprise, et donc très favorable à la création d'une Direction Sécurité Groupe, qui permet de faire travailler de manière très horizontale des compétences SSI, sûreté, juridique et de communication, tout en permettant d'orchestrer une stratégie globale. Ce n'est évidemment pas toujours possible, notamment en fonction de cultures d'entreprises très diverses ou d'activités particulières. D'autres organisations sont alors évidemment possibles, tant que l'on parvient, à mon sens, à favoriser cet aspect pluridisciplinaire de la protection.

Le cliché de l'opposition entre un RSSI geek d'un côté et de l'autre un service de sûreté dirigé par un ancien gendarme hermétique aux nouvelles technologies a clairement vécu. Aujourd'hui, un bon mélange de profils est indispensable pour identifier, détecter et traiter les menaces forcément globales qui ciblent l'entreprise (des profils civils et militaires, issus des services de renseignement ou universitaires, consultants techniques et organisationnels, juristes et communicants, internes et externes, etc.). Pour cela, une direction unique est un atout. Mais évidemment, orchestrer efficacement tout ce petit monde est une autre histoire !

GS Mag : Quels outils (techniques, organisationnels, juridiques…) peuvent aider les organisations ?

Jérôme Saiz : Plutôt qu'une liste de courses forcément périmée dans quelques mois, je ferai l'énumération des conditions idéales à rechercher dans l'élaboration de toute stratégie de défense, qu'elle soit économique ou de sûreté.

- Le soutien sans faille de la direction générale ;
- Des processus bien définis et bien compris de tous ;
- Les moyens réglementaires d'assurer le respect de ces processus ;
- Une culture de défense réellement pluridisciplinaire ;
- La sensibilisation régulière des collaborateurs aux techniques d'arnaques courantes ;
- Un bon recrutement à la tête de ce dispositif ;
- Et puis des tests, des tests, des tests !

Le jeu et les tests « grandeur nature » favorisent l'apprentissage des bons réflexes

GS Mag : De quelle manière communiquer et sensibiliser au mieux les collaborateurs à ces problématiques ?

Jérôme Saiz : Ai-je déjà mentionné l'importance des tests ?
Plus sérieusement, les options de sensibilisation sont nombreuses. Je suis pour ma part convaincu de l'intérêt de la « ludification » pour faire passer des messages et acquérir de bons réflexes, à travers notamment l'usage de Serious Games. En « vivant » des situations problématiques à travers un jeu, les collaborateurs sont beaucoup plus susceptibles d'intégrer durablement les bonnes pratiques de sécurité que s'ils avaient été soumis à une présentation plus traditionnelle. L'aspect ludique provoque en outre une adhésion largement supérieure au message qui est délivré.
Viennent ensuite les tests. Les exercices de crise permettent de mettre sous tension, de manière sélective, les processus et l'organisation quotidienne. Ils créent ainsi la « mémoire musculaire » de l'entreprise face à des événements déstabilisants et, par définition, hors-normes. Il n'y a pas de secret : tout le monde est mauvais lorsqu'il est confronté pour la première fois à une crise. C'est pourquoi il est vital que cette première fois soit un exercice, réalisé dans un cadre maîtrisé.

Encadrez les allées et venues dans vos locaux

GS Mag : Comment gérer et encadrer au mieux l'accueil de nouveaux employés, stagiaires, prestataires, visiteurs… au sein de l'entreprise ?

Jérôme Saiz : Vaste sujet ! De manière très générale, il est indispensable de pouvoir s'appuyer sur des processus bien définis, connus de tous, et de donner aux collaborateurs les moyens de les respecter. Sans ces conditions de base, il ne se passera rien. Et évidemment, décrire en détails ces processus dépasse le cadre de ces lignes !

Mais à titre d'exemple, parmi les mesures de tout premier niveau, presque des évidences, il est important de disposer d'un solide circuit d'intégration et de départ pour les salariés, qui couvre, outre les moyens d'accès physiques aux locaux, également le système d'information (provisionnement et destruction automatique des accès basés sur la présence du salarié dans les outils de paie ou dans la base téléphonique, par exemple). Certes, un projet de gestion des identités et des accès (IAM) est lourd et structurant, mais il apporte à terme un vrai bénéfice.

Concernant les stagiaires, il va sans dire qu'ils doivent a minima être accompagnés tout au long de leur stage par un collaborateur et mentor de confiance (ne serait-ce parce que sinon ce n'est pas un stage, et c'est illégal), qu'ils doivent si possible bénéficier d'un accès au réseau informatique limité aux besoins de leur stage et que leur rapport doit être relu et validé avant d'être rendu public.

Pour les prestataires qui auront accès aux locaux ou à des informations sensibles, il est important de collecter un minimum de renseignements sur la société avant de contractualiser. Des choses telles que sa structure capitalistique, ses principaux clients, ses antécédents (et ceux de ses dirigeants)…, ont toutes leur importance, et peuvent bien souvent être collectées publiquement et légalement. Il faut ensuite se poser la question d'en encadrer correctement les interventions : signature d'un registre d'interventions avec le détail des actes attendus et réalisés, ouverture et fermeture des accès distants de manière ad hoc par un collaborateur, escorte du prestataire selon la sensibilité des locaux accédés, etc. Bien entendu, cela n'est pas toujours possible, mais les exceptions doivent être identifiées, justifiées et documentées.

Enfin, pour ce qui est des visiteurs, un zonage efficace des locaux est une mesure de sûreté fondamentale, avec tous ses corollaires en matière de contrôle d'accès, de port apparent du badge et

d'accompagnement des visiteurs… à l'arrivée comme au départ ! Et lorsque c'est envisageable, une politique dite « bureaux propres », avec l'installation d'armoires fortes (à ne pas confondre avec un coffre-fort) est une très bonne pratique, qui évitera notamment les tentations des visiteurs « égarés » et autres stagiaires ou prestataires un peu trop curieux.

Il s'agit là de mesures très élémentaires, qui devraient déjà avoir fait l'objet, au moins, de réflexions au sein de l'entreprise. À moins de partir de zéro, ce qui n'arrive que rarement en dehors des plus petites structures, le travail du consultant sécurité/sûreté est le plus souvent d'aller au-delà de ces évidences, et notamment d'adapter le dispositif aux menaces spécifiques à l'entreprise.

Ne sous-estimez pas vos adversaires !

GS Mag : Quid du travail à distance ou du déplacement de collaborateurs à l'étranger ?

Jérôme Saiz : L'adaptation du matériel informatique utilisé en déplacement est essentielle. Les collaborateurs dont les déplacements sont occasionnels ne devraient jamais se déplacer avec leur ordinateur de travail quotidien. Cela nécessite bien entendu de mettre en œuvre des outils et des processus d'accès et de sauvegarde à distance adaptés, mais c'est à mon sens une mesure incontournable. De même que le chiffrement intégral du disque dur par une solution de confiance (bénéficiant par exemple d'un Visa de Sécurité délivré par l'ANSSI), la protection du BIOS par un mot de passe et une protection à deux facteurs pour l'ouverture des sessions.
Il convient ensuite de sensibiliser les collaborateurs aux risques encourus lors du passage de frontières (un grand classique), mais également lors de leurs séjours à l'hôtel et même chez leurs partenaires commerciaux sur place.
Des comportements adaptés, une certaine retenue et une connaissance des « affaires » passées peuvent vraiment aider les collaborateurs à ne pas tomber dans les pièges les plus grossiers. J'ai ainsi observé lors de nombreuses séances de sensibilisation que pour bon nombre de collaborateurs, ce qui les rend vulnérables c'est avant tout une méconnaissance totale de jusqu'où un adversaire est capable d'aller. Ils n'imaginent par exemple pas une seconde qu'un concurrent va pouvoir sonoriser tous les taxis de la ville lors d'une convention majeure à l'étranger (véridique), soudoyer le personnel de l'hôtel où ils descendent (aussi), ou bien encore qu'un gouvernement étranger va pouvoir piéger les prises de rechargement USB dans les chambres d'un hôtel (idem). Pourtant, ils sont non seulement friands de ces anecdotes, mais une fois qu'ils ont vraiment compris que tout cela n'existe pas qu'au cinéma, ils deviennent beaucoup plus prudents.
En matière d'Intelligence Économique et de sûreté, si la paranoïa à l'excès n'est pas une bonne chose, une trop grande naïveté ne l'est pas non plus !

Ne mettez pas tous vos œufs dans le même panier !

GS Mag : Quels sont vos conseils pour éviter la fuite de savoir-faire ou d'acteurs clés d'une entreprise ?

Jérôme Saiz : Avant tout de ne pas concentrer tout le savoir-faire dans une seule personne, souvent de manière totalement empirique. Il est important de pouvoir tirer profit de tous les savoirs de manière structurée et accessible (de façon contrôlée, évidemment).
Pour cela, il est nécessaire de faire l'inventaire des connaissances stratégiques (les savoirs et savoir-faire), de modéliser leur circulation et de repérer les « goulets d'étranglement ». En accompagnant des entreprises dans une telle démarche, l'on découvre souvent des « nœuds » de rétention de l'information insoupçonnés, très loin de la vision théorique de l'organigramme. Et le risque, c'est que ceux-ci, puisqu'ils sont invisibles, ne bénéficient pas forcément de la protection à laquelle ils devraient avoir accès.
Il y a également le cas très courant de l'entreprise dont le « sachant », celui à qui tout le monde faisait appel, est parti à la retraite. Elle comprend alors rapidement que c'était une erreur… mais trop tard ! Et cela vaut également pour ce classeur Excel devenu absolument monstrueux au fil des années, qui tient debout par miracle et surtout avec l'attention quotidienne de son créateur. Et qui ne sera d'ailleurs peut-être plus compatible avec les versions majeures d'Excel qui suivront le départ de son concepteur (exemple vécu).
Bref… il n'est pas inutile de s'intéresser sérieusement au domaine de la modélisation des processus métiers !
Ensuite, évidemment, il sera vital d'étudier de près toute demande de partenariat, d'assistance financière ou de rachat quand les choses vont mal, et de ne pas hésiter à solliciter l'avis des services de l'État.

Aucun répit pour la lutte économique…

GS Mag : Enfin, à quoi devons-nous, selon vous, nous attendre dans les années à venir, et quels axes pourraient être développés pour renforcer la sécurité économique en France ?

Jérôme Saiz : Malheureusement, en matière de lutte économique, il n'y a pas de « détente », ou de périodes de paix. Les pratiques d'espionnage économique ne vont pas se tarir. Et les adversaires peuvent être de tous bords. Le général Carter Clarke, qui a dirigé au début des années 50 la NSA, l'agence de renseignement américaine, est connu pour avoir dit au *sujet des alliés des États-Unis : « Ils sont nos amis aujourd'hui et seront nos ennemis demain. Alors, apprenons-en autant que nous le pouvons à leur sujet tant qu'ils sont nos amis, car ce ne sera plus possible lorsqu'ils seront nos ennemis* ».
C'était vrai à l'époque et ça l'est d'autant plus aujourd'hui dans le domaine économique. Et pourtant, nous vivons dans une ère de « coopétition », où les entreprises sont régulièrement amenées à collaborer avec des concurrents potentiels, à utiliser leurs services, à avoir recours aux mêmes fournisseurs en ligne ou à se disputer les mêmes collaborateurs. Cette « schizophrénie » des intérêts économiques va aller en augmentant, notamment si l'on considère les mutations profondes qu'implique la transformation numérique des entreprises. Celles qui ne prennent pas encore en compte cette vision se placent à mon sens dans une position difficilement tenable pour l'avenir. ■■■

* Jérôme Saiz est consultant au sein de la société OPFOR Intelligence. Il est auditeur de l'Institut national des hautes études de la sécurité et de la justice (INHSJ), titulaire du titre d'« Expert en Protection des Entreprises & Intelligence Économique » (RNCP 1) et certifié CT CERIC en sûreté/malveillance par le Centre National de Prévention et de Protection (CNPP).