Comment se protéger de l'espionnage industriel sans bourse délier ?

- Intelligence économique -

Date de mise en ligne : mardi 28 avril 2009

Spyworld Actu

Le contre-espionnage, très peu pour vous ? Dirigeant de PME ou de PMI, vous êtes surtout préoccupés à faire que les affaires fonctionnent et considérez que les histoires de renseignement industriel, cela concerne surtout les grandes sociétés.Détrompez-vous.

« En France les attaques concurrentielles sont négligées. Or ce sont souvent les PME et PMI qui sont la cible d'espionnage économique, parce qu'elles sont innovantes, et que les grands groupes du CAC 40 sont mieux sécurisés en interne face à ces attaques », explique Bernard Lage* de la société Geos.

Avec l'aide d'experts de l'intelligence économique, UsineNouvelle.com vous livre une fiche pratique pour vous y retrouver, et protéger votre entreprise.

I) SE POSER LES BONNES QUESTIONS

Du bon sens, encore du bon sens. « On oublie les éléments basiques, il suffit pourtant souvent de mettre en place des procédures simples pour limiter les risques », souligne l'expert Frank Puget* de la société Kermeur. Et puisqu'il s'agit de ne pas perdre de vue les règles de base, mieux vaut cibler par quelques questions clés les zones rouges.

1) Quel type d'information est détenu par qui ?

Nouveaux projets du pôle de R et D, tarifs pratiqués par les commerciaux, planning des livraisons du pôle logistique... qui sait quoi dans l'entreprise ? Un organigramme de l'information vous permet de faire un premier tour d'horizon des zones à « sécuriser ».

2) En quoi ces informations sont-elles intéressantes pour des acteurs extérieurs ?

A chacun des rendez-vous qui rythment la vie de l'entreprise, des informations utiles peuvent être collectées par un interlocuteur avisé.

Visites d'entreprises. Lorsque vous accueillez un potentiel partenaire sur un site de production, gardez bien à l'esprit que cela attise les curiosités : on a déjà vu des visiteurs porter des semelles autocollantes, pour recueillir des résidus de matières composites au sol, afin de les faire analyser ensuite.

Salons. Les salons professionnels sont un lieu de prédilection pour l'espionnage industriel. Au mondial de l'automobile par exemple, certains visiteurs arpentent les allées avec des chemises à carreaux calibrés pour se prendre en photo aux côtés des nouveaux véhicules, afin de mesurer l'écart d'ajustement entre les pièces de carrosserie. On croise toujours des individus à plat ventre ou dans un coffre, ou très occupés à filmer à 2 cm de distance des phares d'une voiture dernier modèle ! A plus petite échelle, dans n'importe quel salon, il est assez simple de se faire passer pour un chercheur d'emploi à un stand, dans l'objectif de recueillir des informations précieuses.

Administrations. Si votre société se porte candidate à un appel à projets, afin de recevoir des financements d'une collectivité locale (appel à projet biomasse de l'Ademe ou de la CRE, fonds de démonstrateur de recherche, prix aux entreprises innovantes de la Région par exemple), il est fort possible que tout le contenu de votre dossier se trouve

sur Internet. « Via des logiciels très spécialisés, il est aisé d'avoir accès au web caché : tandis que Google ne nous restitue que 5% des pages du web réel, « Lexis-nexis » permet d'en explorer 60 à 70% » explique Franck DeCloquement* de la société Kermeur. Un auditeur d'une société commercialisant les bombonnes plastiques d'eau s'étonnait ainsi de retrouver son bilan et son compte de résultats sur la toile, alors qu'il ne les avait communiqués qu'à un organe administratif. Cette mésaventure s'explique en partie par cette possibilité de retrouver tout cela sur le web caché grâce au moteur de recherche adéquat.

Parfois, une collectivité locale, en voulant faire la preuve de son activisme en matière de soutien à l'innovation, peut publier des données confidentielles sur les projets qu'elle finance : en indiquant qu'une société projette de bâtir certains types de locaux par exemple, des concurrents avisés peuvent parfois en déduire des informations sur son activité.

Logiciels de traduction. Autre détail qui nous est donné par Systran, leader mondial des logiciels de traduction automatique : des secrets industriels ont été divulgués lorsque des cadres d'entreprises stratégiques ont copié-collé des textes sensibles dans des traducteurs en ligne, qui ont été captés par des tiers que sont les salariés de Systran. En règle générale, tout ce qui passe sur Internet peut être lu !

Discrétion. C'est humain, nous avons tous tendance à parler en partie de notre travail à nos amis, à nos proches. Reste qu'il est aisé de capter l'information par ouïe-dire. Devant les entreprises à la pause cigarette, durant les « after work » ou dans les bars, quoi de plus facile que de laisser ses oreilles traîner ? Les grands bâtiments anonymes sont d'ailleurs souvent la cible d'intrusions. « Sur le parvis de la défense, nul ne se connaît : il suffit de dire à la personne qui entre « j'ai oublié mon badge », et l'on entre très facilement. Cela marche dix fois de suite ! » raconte un spécialiste. Autre technique employée par des concurrents pour s'informer : les faux entretiens d'embauche. « il suffit d'appâter les gens par un profil de poste sur mesure via une petite annonce, et de demander au candidat de parler des projets en cours », raconte un expert.

Face Book, Twitter et autres réseaux sociaux du web 2.0 sont également un terrain privilégié pour les fureteurs. Les services de renseignements britanniques ont d'ailleurs la réputation de recruter des jeunes sur face book selon la capacité qu'ils montrent à s'auto promouvoir.

3) Comment l'information circule-t-elle entre ces différents pôles ?

Quels sont les modes de correspondance pratiqués dans votre entreprise : téléphone, courrier, livraisons par coursiers ou par la Poste ? Dans une entreprise familiale en particulier, il est facile de s'installer dans une routine de confiance et de ne plus faire attention : « tu prends le doc demain sur mon bureau », « je prends ton courrier » : l'organisation et la protection des données est souvent floue et informelle.

Téléphone. Espion potentiel de choix, le téléphone mérite une attention particulière. Les remous médiatiques autour du Blackberry de Barack Obama et du système échelon sont en ce sens symptomatiques. « Quand un entrepreneur fait réparer son téléphone portable, il est facile de le substituer par un spy-phone (un espion informatique, NDLR) », raconte un expert. Les téléphones fixes ne sont pas plus sécurisés. « N'importe quelle prise téléphonique peut se révéler être un dispositif électronique de captation » explique-t-il. Des micros de basse impédance peuvent être installés.

Photo. Attention également aux documents que vous transportez sous le bras : outre le fait d'être oubliés dans un taxi ou un métro, ces documents peuvent être photographiés sans que vous ne le sachiez. Des dirigeants de Scotland yard et des ministres britanniques (ou français) se sont déjà fait épingler par des appareils de paparazzis au zoom très efficace, sur des dossiers sensibles.

A titre d'exemple, voici une photo de « l'inauguration » de Barak Obama du 20 janvier dernier, dans laquelle il est possible de distinguer nettement chaque personne dans la foule (cela peut prendre un peu de temps pour charger le fichier, mais cela vaut la peine de patienter ! Pointez quelque part. Utilisez la petite main pour agrandir la photo. Attendez quelques secondes et vous serez en focus). Cette photo a été prise avec une caméra-robot de 1.474 megapixel, soit avec 295 fois plus de puissance que les photos à 5 megapixels de nos caméras familiales. Une seule photo permet de « ficher » un million de personnes.

4) Comment et où stockez-vous les informations ?

Qui gère le parc informatique ? Quelle est la nature des sous-traitants ? Encore une fois, lorsqu'une routine s'installe, on oublie de faire le minimum. Une borne wi-fi mal calibrée, et ce sont des débats internes, des documents qui peuvent fuiter. Des escroqueries de la part d'un membre de la famille d'un salarié ou d'intérimaires sont toujours possibles. Des sociétés de ménage extérieures qui ont recours à l'intérim peuvent prélever de la documentation dans les poubelles ou faire des photocopies, voire prélever des informations sur clé USB. Les solutions sont assez simples : détruire les documents avant de les jeter, protéger l'accès aux ordinateurs par des codes secrets... « Il est possible d'ôter des droits, empêcher que les ordinateurs puissent utiliser des clés USB », explique un informaticien

Des sociétés de conseil en intelligence économique pourront réaliser pour vous des tests d'intrusion, vérifier les fragilités du système informatique, faire des essais sur les disques durs pour voir si des programmes malins ont été intégrés. Les Key logers par exemple, permettent de voir à distance tout ce qu'un individu tape sur son clavier. C'est ce qui a, entre autres, été employé pour espionner Yannick Jadot de Greenpeace.

« Pour conserver une traçabilité des échanges, l'entreprise peut aussi vérifier les e-mails, mais il faut que les salariés soient informés » ajoute un expert.

Circuits fermés. Votre société doit aussi prendre garde à ne pas voir détournés ses propres réseaux de surveillance : « même fermés, des circuits internes peuvent être piratés » rapporte un spécialiste. Mais avant de s'atteler à ces subtilités, des éléments très simples qui ne demandent pas d'investissement lourd peuvent être utilisés. « On est pratiquement dans l'exploitation du bon sens », rappelle Franck DeCloquement de la société Kermeur. Un autre spécialiste évoque même une « gestion des risques intrusifs en bon père de famille ».

A titre d'exemple, quatre ordinateurs contenant les plans de la prison de Nancy, qui devrait ouvrir entre le 22 et le 26 juin 2009, ont ainsi été volés en février dans les locaux de la société de BTP Eiffage, chargée de la construction. Les disques durs des ordinateurs contenaient également les codes de fabrication des clefs de ce nouvel établissement pénitentiaire de 690 places. Les cambrioleurs n'avaient eu qu'à forcer une porte et une fenêtre pour pénétrer dans les lieux. Heureusement les machines ont été retrouvées le 21 mars dans un immeuble en construction. Mais le « happy end » n'est pas toujours au rendez-vous.

5) Comment préparez-vous un voyage ?

Un élément basique que vous gagnerez à ne pas négliger : faites un point avant chaque déplacement, en toute circonstance. Utiliserez-vous un ordinateur portable dans l'avion, ou tout autre mode de transport ? « Il est très facile de photographier un écran à distance », rappelle un expert. Utilisez en toute innocence une borne wi-fi dans un aéroport, et c'est tout le contenu stocké dans votre ordinateur qui peut être capté. Si votre ordinateur est saisi durant un passage à la douane d'un pays, puis vous est rendu dans les 5 minutes, il peut avoir été copié de fond en comble. En Chine, les taxis sont sonorisés...

Le lieu d'hébergement lors d'un séminaire auquel vous pouvez vous rendre à l'étranger mérite aussi que l'on s'y

arrête. Que laisserez-vous sur place en journée ? Que prendrez-vous avec vous ? Il est possible que la chambre d'hôtel, coffre fort compris, soit « visitée » en l'absence du propriétaire des bagages, cela s'est déjà vu. Lors des salons professionnels, des conférences d'experts auxquelles vous participerez, ou lors du pot en fin de journée, il peut vous arriver de laisser filer des informations stratégiques, d'indiquer que vous cherchez des ingénieurs d'un profil particulier, ce qui donne une idée des projets futurs ou des innovations que vous menez à bien.

Cette liste vous effraie ? Rassurez-vous : une fois conscient des points faibles, acheter une déchiqueteuse de papier, suivre les consignes de sécurité, opérer des piqures de rappel nécessaires n'est pas des plus coûteux. Et puis, pour démystifier, toutes les entreprises ne sont pas prises pour cible. Voici néanmoins quelques conseils pour celles qui pourraient l'être, et qui vous seront des plus utiles mêmes si vous ne faites pas partie du lot des « espionnées ».

II) PASSER A L'ACTION SANS DEVENIR PARANOÏAQUE

« Tout le monde n'est pas systématiquement victime de pillages malveillants », rassure Frank Puget. Il s'agit avant tout, concernant les PME-PMI, d'entreprises travaillant sur des segments à haute valeur ajoutée, sur des marchés de niche. Car, comme partout ailleurs, espionner a un coût, et l'attaquant ne prendra d'initiative que si le jeu en vaut la chandelle : il doit être sûr des gains qu'il pourra par la suite en tirer.

1) Remettre le curseur sur les yeux et les coeurs de l'entreprise : ses employés

« A 80% les erreurs sont humaines » explique un spécialiste. Le premier pas consiste donc pour vous à permettre aux salariés de prendre conscience des enjeux. Le paragraphe « sensibiliser et former les salariés à la protection des informations sensibles de l'entreprise », du guide SCIE des bonnes pratiques en matière d'intelligence économique, est assez renseigné et très utile .

Premier rempart dont vous ne pourrez pas faire l'économie, selon le directeur de la société Kermeur : bien connaître votre secteur d'activité, vos clients, vos fournisseurs, vos concurrents, vos salariés. Mieux vaut cloisonner certains informations stratégiques en interne : tout le monde n'a pas besoin d'avoir accès à tout. Les procédures de sécurité que vous mettrez en place doivent être simples : de bon sens, et applicables sans contraintes majeures. Et rien de tel que montrer l'exemple : si le chef d'entreprise applique lui-même les consignes qu'il a édictées en direction de ses salariés, il a d'autant plus de chances de réussir. Encore et toujours, soyez attentif à vos troupes : même sans le vouloir, un employé déçu est un terreau fertile pour des attaques non-conventionnelles, des acquisitions d'informations par le truchement de l'humain. D'autant que la France a longtemps négligé de prendre la mesure de ce phénomène.

Car au-delà de la formation, les salariés sont la pierre angulaire de votre stratégie de protection. Ils sont les yeux et le coeur de votre entreprise, et peuvent se révéler être un atout majeur comme une vulnérabilité d'ailleurs, selon le sort que vous leur réservez. « Tout le monde connaît les risques d'intrusion liés aux systèmes informatiques. Mais la faille est bien souvent humaine » précise Frank Puget. Des salariés déçus ou en passe d'être licenciés, un encadrement qui reprend en main une société ayant subi un plan social de 400 départs, et qui doit gérer à la suite ceux qui restent, tout cela fragilise de toute évidence une entreprise. Un attaquant utilisera toutes ces faiblesses.

Votre entreprise peut être victime d'une atteinte à son image : dénigrement des produits et services, appel au boycott, mise en cause des dirigeants, diffusion d'informations erronées, utilisation malveillante du nom de l'entreprise, de ses marques, détournement de sa communication (slogans - défiguration du site Internet, mise en ligne d'un faux site...). A titre d'exemple, la mouvance antinucléaire a lors de l'affaire d'espionnage de Greenpeace et de Sortir du Nucléaire par EDF inventé un compte twitter au PDG d'EDF et lui avait prêté les commentaires suivants : « 6 ans qu'on essaye de retrouver le salaud de chez nous qui envoie des docs à Sortir du nucléaire. Si on

avait trouvé, on n'en serait pas là (...) » Ces attaques qui ternissent la réputation de l'entreprise peuvent aller jusqu'à la mise en péril de la santé économique d'un groupe.

2) Se faire conseiller

Pour mieux protéger votre entreprise, vous pouvez aussi vous appuyer sur des sociétés de conseil spécialisées : cela n'est pas forcément très coûteux. « Les PME viennent nous voir quand quelque chose les a alertées » rapporte Bernard Lage de la société Geos. « Ou lorsqu'un nouveau directeur général, qui vient d'un grand groupe, s'aperçoit que ce n'est pas sécurisé ».

En général, le cabinet auquel vous ferez appel vous présentera un devis au préalable. Si cela vous convient, il pratiquera un audit de sécurité de l'information, et analysera les menaces et les risques : logiciels, aspects humains, configuration des locaux... Ensuite, il vous fera des recommandations. La société Geos par exemple s'est occupée de 7 ou 8 entreprises l'année dernière. Des petites structures dont le chiffre d'affaires est compris entre 3 et 10 millions d'euros. Voire moins de 1 million d'euros pour l'une d'entre elles. « Il peut s'agir d'affaires de famille : des entreprises gérées par l'arrière grand-père, puis le grand-père, le père, le fils, dans lesquelles on décèle beaucoup de négligences » confie-t-il.

Equipement informatique. En termes de matériel, une lettre de mission pourra vous faire des recommandations et des estimations de coût : quel type de machine acheter, traiter directement ou pas avec le fournisseur... « Le chiffrement ne coûte pas très cher. Parfois il n'est pas nécessaire de mettre en oeuvre de gros investissements, quelques milliers d'euros suffisent », explique un expert. Une protection contre le risque d'intrusion sur trois postes informatiques coûte par exemple 1500 euros. L'achat d'un serveur unique, premier pas afin d'assurer la sécurité informatique d'une entreprise, coûte 20 000 à 30 000 euros suivant la taille de l'entreprise. « Tout dépend du nombre de sites, de l'importance de la recherche et développement, des unités de production, de l'ampleur », poursuit l'expert. Pour une structure moyenne, comptez entre 10.000 et 15.000 euros pour une mission de conseil en protection de l'information.

De quoi parle-t-on ?

- **Espionnage industriel.** Vol caractérisé de secrets industriels ou d'informations : la définition est ici pénale. « Tous les bons services secrets du monde font ça » rapporte un expert.

- **Intelligence économique.** Actions dont le but est d'asseoir un avantage concurrentiel. « L'intelligence s'entend ici comme une compréhension du monde qui nous entoure » explique Frank Puget de Kermeur.

3) Ne pas franchir la ligne rouge

Lorsque l'on étend les enjeux de l'espionnage industriel à ceux plus larges de l'intelligence, beaucoup de « petits conflits de basse intensité » se font jour : des attaques subversives, des campagnes de dénigrement foisonnent, sur le terrain. « Il n'y a souvent plus de moyen de savoir qui est votre adversaire, ni s'il vous attaque vraiment. Parfois c'est tout simplement imbitable », confie un expert.

Et c'est là que le bât blesse. Dans ce cadre le jeu du plus malin, se donner les moyens de riposter ou de se protéger peut mener à flirter dangereusement avec la loi. « On connaît les limites, on a des droits et des devoirs » explique un cabinet de conseil : « lorsque le droit ne nous permet pas de protéger de façon efficace une entreprise, nous

préconisons de déposer une plainte. L'instruction judiciaire permet d'aller sur des comptes bancaires, de faire des saisies : un arsenal juridique dont nous ne disposons pas à notre niveau ».

Ce que vous risquez. Le secret des correspondances privées, le traitement des données nominatives précisées par la Cnil engagent la responsabilité du chef d'entreprise, qui être mise en cause en cas de non respect des procédures dans la mise en place d'un processus de cybersurveillance des salariés par exemple.

Le non respect des dispositions de la loi Informatique et Liberté est passible d'une amende de 300.000 euros et de 5 ans d'emprisonnement pour le responsable du traitement des données à caractère personnel (art. 226-16 à 24 du code pénal). En cas de reconnaissance de la responsabilité pénale de l'entreprise en tant que personne morale, les amendes sont quintuplées et les peines peuvent aller jusqu'à la dissolution (art 131-38 et 39 du code pénal).

Illégal. Le guide SCIE des bonnes pratiques en matière d'intelligence économique fait la liste des actes et comportements répréhensibles : l'enregistrement des paroles audio ou images vidéo à l'insu de l'intéressé, l'intrusion volontaire ou involontaire dans un système informatique et l'utilisation de l'information à des fins de dénigrement, le vol d'information dans l'entreprise (y compris dans les poubelles situées dans les locaux de l'entreprise), la corruption active et/ou passive en France et à l'étranger , l'usurpation ou l'usage de fausses identités, la simulation de rachat d'une entreprise ou la mise en oeuvre de fausses procédures juridiques pour obtenir des informations sensibles...

Légal. Il liste à l'inverse les bonnes pratiques à utiliser dans le cadre de la collecte d'informations : rappeler (par exemple, par la signature d'une charte) aux collaborateurs impliqués dans la collecte d'informations, le respect des règles déontologiques et notamment en matière de droit d'auteur, d'utilisation des fichiers papier ou électroniques contenant des données à caractère personnel, de recours à des pratiques légales excluant l'obtention d'informations par toute pression morale ou financière ou par l'emploi de fausses identités. Faire signer des engagements de « bonnes pratiques » aux prestataires en intelligence économique auxquels l'entreprise recourt (cf. à titre d'exemple la charte éthique sur le site de la Fepie, Fédération des Professionnels de l'Intelligence Economique).

Un garde-fou légaliste dont Bernard Lage s'est fait le chantre. « Quand on fait de l'investigation, on a vite fait de déborder. L'envie de satisfaire le client, souvent le fait d'auditeurs jeunes, ambitieux, peut pousser à dépasser la ligne rouge », confie-t-il. « C'est la classique histoire du feu rouge qu'il est toujours possible de griller », renchérit Frank Puget, « Tout le monde sait qu'il est interdit de le franchir, mais aucun obstacle physique ne l'empêche. Alors certains jettent un coup d'oeil, et passent outre... malheureusement ».

Des techniqques où vous risquerez gros, et au gain peu évident. « Les techniques illégales sont idiotes » confie Bernard Lage. S'introduire sur le fichier central de police peut par exemple donner aux enquêteurs privés l'impression de se valoriser, mais l'information n'y est pas forcément fiable ni exploitable : une personne entendue pour infraction n'est pas toujours condamnée, des erreurs de police sont également possibles. « Je préfère passer par des méthodes fines légales, on arrive presque au même résultat » explique le dirigeant de Geos. Pour enquêter sur une personne suspectée de fraude, tout citoyen a par exemple accès au cadastre, par le biais duquel le patrimoine de cette personne peut être évalué.

La loi de Nicolas Sarkozy de 2003, dont les décrets d'application ne sont pas encore parus, a d'ailleurs introduit un label qui oblige les sociétés d'intelligence économique à obtenir un agrément sur certains aspects de l'investigation qu'elles mènent. Pour obtenir l'agrément, les personnels des agences de recherche privée doivent être diplômés de la licence « Sécurité des biens et des personnes » de l'université Panthéon Assas II par exemple, où les étudiants bachotent droit civil, droit pénal... Un agent bénéficiant de 5 ans d'ancienneté dans l'investigation peut également faire valider ses acquis. Outre la garantie de ne pas violer le cadre de la légalité, faire appel à une société d'intelligence agréée permet par exemple de détenir des rapports qui peuvent être produits en justice avec beaucoup

plus de poids.

Cette fiche pratique en main, nous espérons que vous pourrez prendre au mieux les décisions qui faciliteront la vie de votre entreprise, sur le terrain de la protection de l'information, et plus globalement de la bonne santé de l'activité. Et si d'autres conseils ou difficultés valent la peine d'être partagés, faites-nous en part à redaction@usinenouvelle.com

Ana Lutzky

**Bernard Delage est gérant de Géos business intelligence. Ancien fonctionnaire de police, il a pris en charge des enquêtes sur le financement et le blanchiment du terrorisme. Frank Puget et Franck DeCloquement sont respectivement Directeur Général et Directeur du développement de la société Kermeur, spécialisée dans la protection, la contre-ingérence et la gestion des crises des personnes et des entreprises. Merci à eux et aux autres experts qui nous ont conseillés pour cette fiche pratique.*

Post-scriptum :

http://www.usinenouvelle.com/articl...