

espionnage économique

fuite des informations

sécurité économique

GUIDE DES BONNES PRATIQUES

protection de la propriété industrielle

vulnérabilité informatique

GUIDE DES BONNES PRATIQUES EN MATIERE DE SECURITE ECONOMIQUE

«L'intelligence économique peut être définie comme la maîtrise et la protection de l'information stratégique pour tout acteur économique» (Alain Juillet, Haut responsable chargé de l'Intelligence Economique au Secrétariat Général de la Défense Nationale – conférence des Préfets du 09/12/2004).

Une politique publique d'intelligence économique au service des entreprises

■ ■ ■ ■ ■ Le contexte actuel de mondialisation, s'il est générateur de croissance pour les acteurs économiques, augmente en même temps l'âpreté de la concurrence technologique, industrielle et commerciale à laquelle les entreprises sont confrontées. Cette situation est désormais perçue par chacun de nous à travers des phénomènes tels que la désindustrialisation, les délocalisations, le recul de nos exportations et la persistance à un niveau élevé du chômage, ainsi que l'observation de l'intérêt croissant de fonds d'investissements étrangers pour certaines de nos entreprises innovantes.

■ ■ ■ ■ ■ Dans ce cadre, la plupart des Etats ou des grands groupes industriels s'efforcent de recueillir du renseignement sur l'activité de leurs concurrents, l'état de leur Recherche et Développement (R&D), mais aussi leurs faiblesses et leurs vulnérabilités. Les nouvelles technologies de l'information et de la communication ont rendu ce type d'informations de plus en plus facilement accessibles et difficiles à protéger.

Conscients de ces nouveaux enjeux, les pouvoirs publics ont initié des actions pour promouvoir l'intelligence économique, à la fois sous l'angle offensif (savoir capter les informations stratégiques et influencer son environnement en fonction de ses propres besoins) et sous l'angle défensif (savoir protéger ses propres informations stratégiques). Ces actions sont déclinées à tous les niveaux :

■ ■ ■ ■ ■ au plan national, le gouvernement a déployé dès 2004 un plan d'action pour le développement dans notre pays d'une véritable politique publique d'Intelligence Economique au service des entreprises. Il comporte notamment des mesures de protection à l'intention des pôles de compétitivité, une attention accrue aux établissements stratégiques et des mesures de soutien privilégiées à l'investissement national dans ces établissements.

■ ■ ■ ■ ■ au plan local, l'Etat et la Région Alsace mènent depuis 1998 des actions de sensibilisation des entreprises à ces nouveaux risques, et des actions de diffusion des méthodes de protection et de recherche d'information stratégique (programme IEA² puis COGITO, en partenariat avec les CCI d'Alsace). Le Forum annuel de la Veille à Sélestat, le Centre Régional de Veille Stratégique à Colmar, les appels à projets collectifs de la DRIRE et de la Région sont issus de ces programmes.

L'enjeu est de maintenir nos parts de marché, notre croissance, nos emplois et, par voie de conséquence, notre rang mondial (1% de la population mondiale, 6^{ème} puissance économique).

Entreprendre et innover ne suffit pas : il faut également se protéger !

L'approche offensive et l'approche défensive sont indissociables pour les entreprises, car à quoi bon élaborer des outils de veille, faire de la recherche et être à la pointe de la technologie si vos propres informations sensibles et vos savoir-faire sont laissés à la disposition de la concurrence ?

C'est pourquoi il est indispensable de mettre en place au niveau de l'entreprise une démarche en réduction de risque, visant à protéger à la fois sa recherche, ses savoir-faire, sa politique commerciale, mais aussi son personnel, de la convoitise de ses concurrents.

Négliger la sécurité économique active ou retarder les décisions à ce sujet crée par conséquent un risque majeur pour la pérennité de l'entreprise.

Cependant, il ne s'agit pas de protéger tout et n'importe quoi, mais bien d'identifier l'information jugée stratégique pour l'entreprise. Pour mener à bien cette démarche, le chef d'entreprise doit, dans un premier temps, recenser ses catégories de savoir-faire jugés stratégiques, cette opération devant être entourée de la plus grande confidentialité.

Il doit ensuite chercher l'équilibre entre les risques encourus et le coût de la protection à mettre en œuvre, afin de déterminer les mesures de sécurité économique adaptées à sa société.

Ce guide, illustré d'exemples concrets, a été conçu pour diffuser les principes de base de la sécurité économique en entreprise. Il est issu d'une collaboration entre la Brigade de Surveillance du territoire de Strasbourg, la Direction Régionale des Renseignements Généraux d'Alsace, la DRIRE Alsace, le détachement de la Direction de Protection et de la Sécurité de la Défense de Strasbourg, la Trésorerie Générale, la Gendarmerie Nationale et la Région Alsace. Ces différents acteurs se tiennent à la disposition des chefs d'entreprises pour les aider à évaluer et à détecter les risques auxquels sont exposées leurs structures et à se protéger contre ceux-ci. Une liste d'interlocuteurs en Alsace figure au dos de ce guide, n'hésitez pas à les contacter !

SOMMAIRE

Que faut-il protéger ?

La politique de recherche et de développement de la société	2
La stratégie commerciale et le marketing de l'entreprise	2
Le fonctionnement de l'entreprise	2

Comment se protéger ?

1) Assurer la sécurité physique de l'entreprise	3
2) Assurer la sécurité informatique de l'entreprise	4
■■■■■■■ le système informatique de l'entreprise	4
■■■■■■■ les risques particuliers liés à l'ordinateur portable	5
■■■■■■■ autres équipements de Technologies de l'Information et de la Communication (TIC)	5
3) Intégrer le risque lié au facteur humain	6
■■■■■■■ le personnel de l'entreprise	6
■■■■■■■ les voyages professionnels	6
■■■■■■■ les visiteurs et stagiaires	7
4) Maîtriser la communication de l'entreprise	8
5) Maîtriser les risques liés à l'environnement économique et aux partenaires de l'entreprise	8

Questionnaire d'autodiagnostic	9
--------------------------------------	---

QUE FAUT-IL PROTÉGER ?

Chaque entreprise fonde sa compétitivité et son attractivité sur des informations que certains concurrents sont tentés de recueillir par des moyens légaux, mais aussi par des méthodes déloyales, voire illégales.

Ces renseignements ont principalement trait à :

La politique de recherche et développement de la société

Cela couvre à la fois la recherche fondamentale pour certains laboratoires, mais également, pour la plupart des entreprises, l'étude et le développement de produits nouveaux ou de nouveaux process.

Ce type d'informations constitue bien souvent le socle de l'entreprise. Leur captation par la concurrence est susceptible de mettre en péril la société. Elle résulte généralement de la perte ou du vol de supports informatiques insuffisamment protégés (notamment les ordinateurs portables), mais est parfois le fruit d'indiscrétions, d'imprudences ou de négligences de la part de membres du personnel de l'entreprise.

■ ■ ■ ■ ■ Juin 2006

Un chercheur d'un laboratoire français, qui avait participé à une conférence s'étant déroulée au sein des locaux de son principal concurrent européen, a oublié sur place d'importants échantillons emmenés à cette occasion. Ces échantillons n'ont finalement pas été perdus, puisqu'ils ont permis au laboratoire étranger de devancer son homologue français dans le dépôt d'un brevet.



La stratégie commerciale et le marketing de l'entreprise

Cela concerne les fichiers clients, les marchés en cours, les politiques tarifaires envisagées, les campagnes promotionnelles, les projets de rachat de concurrents, les perspectives de développement à l'international, etc.

Ces données stratégiques doivent également être entourées d'une certaine confidentialité. Gérer au mieux les droits d'accès à ces informations est une priorité.

■ ■ ■ ■ ■ Octobre 2005

Une entreprise textile française, ayant mis au point un tissu particulièrement innovant s'est adressée à un partenaire étranger habituel, afin d'assurer la campagne marketing dudit produit. Cependant, peu de temps après, la société sollicitée diffusait une plaquette publicitaire reprenant les caractéristiques et s'attribuant la paternité de l'innovation française.

Le fonctionnement de l'entreprise

Cela touche les données personnalisées sur les employés, les organigrammes, les plans et système de sécurité des locaux, etc.

Des entreprises peuvent ainsi trouver un intérêt à connaître l'organisation de leurs principaux concurrents, notamment en vue «d'approcher», voire de débaucher les personnels clefs de l'entreprise.

■ ■ ■ ■ ■ Avril 2007

Un grand groupe industriel, ainsi que plusieurs de ses filiales ont fait l'objet de manœuvres de recherche de renseignement par la méthode dite de «l'ingénierie sociale», qui consiste à obtenir des informations en exploitant la confiance, l'ignorance et la crédulité de son interlocuteur, notamment par le biais de questionnaires téléphoniques ou de mailing. Les secrétariats de direction de ces sociétés ont ainsi été la cible d'appels téléphoniques relatifs à leur personnel de direction, le but de cette démarche consistant vraisemblablement à reconstituer un organigramme complet de l'ensemble de ce groupe industriel.

Une fois recensés les types d'informations à protéger, encore faut-il mettre en oeuvre, au sein de l'entreprise, les dispositifs de sécurité adaptés.

COMMENT SE PROTÉGER ?

En assurant la sécurité physique de l'entreprise.

Les principales recommandations relèvent essentiellement de 5 domaines correspondant à des grandes catégories de vulnérabilités :

- la sécurité physique de l'entreprise (son site et ses locaux),
- la sécurité informatique,
- le facteur humain,
- la communication de l'entreprise,
- l'environnement et les partenaires (notamment pour les pôles de compétitivité).

Il appartient à chacun de trouver dans ce guide les recommandations les plus appropriées à sa situation particulière.

1) Assurer la sécurité physique de l'entreprise : protection de son site et de ses locaux.

La sécurité physique du site et des locaux constitue le premier niveau de protection de l'entreprise. Elle vise notamment à empêcher toute intrusion, à contrôler, voire à limiter les déplacements, à interdire tout recueil indu d'informations stratégiques.

Il s'agit des mesures à mettre en œuvre en priorité. Rien ne sert en effet de protéger le réseau informatique de la société, si les locaux n'ont pas été préalablement sécurisés.

Quelques recommandations :

■ ■ ■ ■ ■ Protection du site par :

- des barrières physiques adaptées (mur d'enceinte, grilles, codes d'accès) ;
- un éclairage «intelligent» ;
- la définition de zones réservées ou protégées à accès limité ;
- le recours au gardiennage ou à la vidéosurveillance (veiller toutefois à recourir dans ce domaine à des professionnels reconnus).

■ ■ ■ ■ ■ Protection des locaux par :

- des systèmes d'alarme (anti-incendie et anti-intrusion) ;
- l'utilisation de mobiliers de sécurité (armoires fortes, coffre-fort, etc.) ;
- la pose de volets, voire de barreaux sur certaines ouvertures, (notamment celles situées au rez-de-chaussée) ;
- la gestion des accès (équilibre entre les mesures de protection et les règles d'hygiène et de sécurité du travail), avec si possible un poste de garde ou de filtrage des entrées/sorties.



■ ■ ■ ■ ■ Une bonne gestion des déplacements à l'intérieur du site et des locaux par:

- le port obligatoire d'un badge, de préférence nominatif, mentionnant la qualité de son détenteur (employé, intérimaire, stagiaire, visiteur) ;
- la tenue d'un registre des visites, dans lequel figurent l'identité, les heures d'arrivée et de départ et l'objet de la visite ;
- l'établissement d'un plan de sécurité interne, avec accès restrictif aux zones les plus sensibles de l'entreprise, complété par un parcours de notoriété pour les visiteurs (circuit accompagné évitant les zones sensibles).

Malheureusement ces mesures, qui ont vocation à protéger le patrimoine de l'entreprise, et n'imposent pas nécessairement de lourds investissements, sont bien souvent insuffisamment observées.

■ ■ ■ ■ ■ Février 2006

Dans le cadre d'un contact avec la direction d'un laboratoire de recherches, et à l'occasion de la visite du site, il a été constaté des insuffisances liées à la sécurité des lieux :

- l'interphone installé à l'entrée de l'institut ne permettait qu'un contrôle vocal ;
- une fois dans les lieux, aucune vérification n'était effectuée, et une personne étrangère pouvait aisément y circuler ;
- l'existence d'une simple porte en bois sans protection particulière permettait l'accès aux locaux ;
- l'absence d'une armoire forte pour la conservation des produits sensibles.

COMMENT SE PROTÉGER ?

En maîtrisant les risques liés au système informatique.

2) Assurer la sécurité informatique de l'entreprise : les risques liés aux Technologies de l'Information et de la Communication (TIC)

2.1) Le système informatique de l'entreprise L'outil informatique est incontournable dans la vie de l'entreprise. Il l'expose cependant à des risques nouveaux susceptibles de lui porter de lourds préjudices.

A l'ère du tout numérique, l'essentiel des informations stratégiques figure sur supports informatiques. Protéger le système informatique des attaques ou tentatives d'intrusion sur le système, revient donc, bien souvent, à défendre le cœur de l'entreprise.

Quelques recommandations :

■ ■ ■ ■ ■ La station de travail individuelle

- utilisation d'un mot de passe personnel et secret d'au moins 8 caractères alphanumériques, changé régulièrement, et confié sous enveloppe cachetée au responsable de la sécurité des systèmes d'information (RSSI) qui le conserve dans un coffre ;
- usage d'un antivirus régulièrement mis à jour et réalisation de sauvegardes quotidiennes des fichiers sur un serveur dédié (ou à défaut sur un disque dur extractible mis en sécurité) ;
- désactivation totale ou partielle des périphériques sur les postes de travail (lecteurs disquettes, CD, port USB).

■ ■ ■ ■ ■ Le serveur réseau de l'entreprise

Il s'agit avant tout d'assurer l'imperméabilité du réseau interne de l'entreprise par :

- la désignation d'un administrateur réseau, responsable de la sécurité informatique ;
- la réalisation de l'ensemble des sauvegardes sur un seul et unique serveur placé dans une pièce sécurisée et à l'accès contrôlé ;
- la partition des données si possible sur plusieurs supports (disques durs amovibles/disques durs internes), de manière à rendre incompréhensible toute lecture indue et empêcher une vue d'ensemble ;
- une attitude vigilante par rapport aux opérations de télé-maintenance informatique ;

- la mise en place d'un accès individualisé et « traçable » pour la consultation des données sensibles.

■ ■ ■ ■ ■ Le réseau internet

- utilisation d'un anti-virus et d'un firewall, afin de préserver les échanges des attaques virales ou ciblées. Prévoir également une maintenance effective du réseau ;
- isoler les postes dédiés à l'internet du réseau intranet ;
- mesurer les risques liés aux connexions sans fil par rapport à l'environnement de l'entreprise (Wi-fi notamment).

■ ■ ■ ■ ■ Avril 2006

Une entreprise a développé un logiciel de conception assistée par ordinateur des plus innovants. Les échanges informatiques, via internet, entre le siège social de l'entreprise et ses différents bureaux situés à l'étranger ne bénéficiant d'aucune protection particulière (chiffrement, intégrité, sécurité), un des logiciels de la société a fait l'objet d'un craquage.

■ ■ ■ ■ ■ Comportement à adopter à l'égard de l'outil informatique :

- ne pas laisser son mot de passe accessible dans le bureau (bannir les post-it et autres aides mémoires) ;
- verrouiller sa session dès que l'on s'éloigne de l'ordinateur, doter son écran de veille d'un mot de passe et s'assurer que son écran d'ordinateur n'est pas visible de l'extérieur du bâtiment ;
- utiliser des supports dont la provenance est connue, ou, à défaut, veiller à recourir à des stations de décontamination ;
- ne conserver sur le réseau et sur les postes individuels (surtout les portables) que les données d'actualité, les plus anciennes étant sauvegardées et stockées en lieu sûr ;
- se méfier des courriers électroniques douteux même s'ils empruntent l'identité d'expéditeurs connus ;
- rendre compte de tout incident et faire appel à une personne ressource qualifiée (RSSI).

■ ■ ■ ■ ■ Avril 2006

Un responsable d'un pôle de compétitivité a laissé un ressortissant étranger télécharger des données sur son ordinateur portable avec une clé USB sans contrôler cette opération.

COMMENT SE PROTÉGER ?

En maîtrisant les risques liés à l'ordinateur portable et aux autres équipements de TIC.

2.2) Les risques particuliers liés à l'ordinateur portable

Parce que l'ordinateur portable expose à des vulnérabilités nouvelles, son utilisation doit répondre à des exigences de sécurité spécifiques.

Quelques recommandations :

■ ■ ■ ■ ■ Au sein de l'entreprise :

■ ranger systématiquement l'ordinateur portable en lieu sûr (armoires fortes), ou à défaut utiliser des antivol agréés.

■ ■ ■ ■ ■ En dehors de l'entreprise :

- assurer une surveillance permanente sur l'ordinateur portable, en ne le laissant pas dans le coffre d'une voiture, ni dans sa chambre d'hôtel, ni dans la salle de travail durant les pauses ;
- conserver les données sensibles sur un support amovible (clé USB, carte mémoire flash, etc.), tout particulièrement lors des déplacements à l'étranger.

■ ■ ■ ■ ■ Avril 2006

Une société française spécialisée dans le domaine de la recherche médicale a été victime d'un cambriolage au cours duquel l'ordinateur portable de son directeur général, laissé sur son bureau, a été volé. Ce vol était probablement ciblé car aucun autre objet n'a été dérobé, alors qu'un ordinateur du même type se trouvait dans la même pièce. Cela constitue un préjudice considérable pour la société, 90% de sa stratégie étant susceptible d'être ainsi dévoilée. De plus, les données figurant sur l'ordinateur ne bénéficiaient d'aucune mesure de protection.



2.3) Autres équipements de TIC

L'évolution technologique impose d'être vigilant non plus seulement dans l'utilisation du seul matériel informatique.

Quelques recommandations :

- les photocopieurs et les fax de dernière génération sont équipés de disques durs : il importe de bien veiller à l'effacement ou à la récupération des données en cas de maintenance ou de location du matériel ;
- les téléphones GSM ou satellitaires, les courriels, les PDA Communicants et les GPS ont un très faible niveau de sécurité, et une totale «traçabilité», qui doivent être pris en compte par les utilisateurs ;
- les installations téléphoniques imposent de :
 - sécuriser les autocommutateurs par le contrôle de certaines fonctions programmables (renvois extérieurs, journal des appels, «entrée en tiers», etc.) ;
 - sensibiliser le personnel assurant l'accueil téléphonique au respect des règles de sécurité et de confidentialité ;
- prévoir la mise à disposition de déchiqueteuses (coupe croisée indispensable), plutôt que de recourir à l'externalisation pour la destruction des documents ;
- définir les règles de sécurité et d'accès pour les archives de l'entreprise ;
- éviter d'avoir recours, pour les transmissions d'informations sensibles, à l'internet, au fax ou au téléphone, sauf à utiliser des lignes sécurisées ou de procéder au cryptage des données.

COMMENT SE PROTÉGER ?

En intégrant le risque lié au personnel de l'entreprise et aux voyages professionnels.

3) Intégrer le risque lié au facteur humain

Le personnel de l'entreprise est détenteur d'une partie de la richesse de l'entreprise. Il constitue par conséquent une cible privilégiée pour les services de renseignements étrangers ou les concurrents indésirables.

3.1) Le personnel de l'entreprise

La sécurité économique au sein de l'entreprise est l'affaire de tous. Chacun à son niveau de responsabilité ou d'exécution doit se sentir concerné et impliqué.

Ainsi, il est de l'intérêt de l'entreprise de mettre en place une politique de sécurité économique qui lui serait propre, notamment en rédigeant un document fixant les règles à mettre en œuvre, et en désignant un responsable de sécurité économique. Ces règles de sécurité s'appliqueront tant à l'intérieur qu'à l'extérieur de l'entreprise.

Le chef d'entreprise gagnera à présenter aux employés les risques encourus par l'entreprise à raison de négligences ou de malveillances en matière de sécurité, et leurs répercussions sur sa pérennité, et donc sur l'emploi.

■ ■ ■ ■ ■ A l'intérieur de l'entreprise, veiller à :

- ranger les documents de travail sensibles sous clé, lors de la pause déjeuner, le soir ou durant le nettoyage des bureaux ;
- détruire les documents sensibles devenus inutiles, y compris les brouillons (proscrire l'utilisation de la simple poubelle) ;
- respecter les consignes liées à la protection de l'information ou du système informatique ;
- nettoyer les bureaux et retirer les feuilles du paperboard après toute réunion ;
- être attentif et conserver une certaine réserve à l'égard des visiteurs, stagiaires, clients et fournisseurs ;
- ne pas laisser, sans surveillance, dans les locaux les prestataires de services extérieurs (nettoyage, maintenance, etc.).

■ ■ ■ ■ ■ Année 2000

Le dirigeant d'une entreprise a reconnu publiquement avoir engagé une agence de détectives privés douteuse afin de fouiller les poubelles d'un concurrent, et avoir offert 1200 dollars aux personnels chargés du ménage dans l'établissement visé, en échange de quelques sacs à ordures.

■ ■ ■ ■ ■ A l'extérieur de l'entreprise, veiller à :

- adopter une attitude discrète et réservée sur son entreprise, notamment lors des déplacements professionnels (colloques, foires, transports en commun, restaurants, etc.) ;
- n'emporter que les informations et matériels strictement nécessaires à la mission et exercer à leur égard une vigilance constante, en prenant toutes les mesures de précaution utiles ;
- rendre compte immédiatement et complètement de tout fait inhabituel, y compris des erreurs commises, mais aussi des informations collectées même fortuitement ;
- canaliser les élans de collaborateurs fiers d'exposer leurs travaux ou ceux de l'entreprise aux yeux du monde.

3.2) Les voyages professionnels

Les règles de sécurité économique ne s'arrêtent pas aux portes de l'entreprise, ni aux frontières. En voyage en France ou à l'étranger, le personnel en mission doit être particulièrement vigilant.

Quelques recommandations :

- définir un cadre précis à la mission, en prévoyant notamment les sujets qui peuvent être abordés et ceux qui doivent être évités ;
- ne pas être porteur d'informations stratégiques, sauf impérieuse nécessité ;
- observer les lois et règlements des pays visités ;
- éviter les conversations à caractère professionnel durant les transports et être prudent lors des comptes-rendus téléphoniques ;
- surveiller constamment ses outils de travail (mallette, ordinateurs et téléphones portables) ;
- éviter d'utiliser les moyens de communication mis à disposition dans les hôtels ;
- se méfier des rencontres «amicales spontanées».

■ ■ ■ ■ ■ Juin 2006

Lors d'un déplacement à l'étranger, un technicien appartenant à un groupe français a fait l'objet d'une opération de séduction de la part d'une interprète, qui lui a clairement demandé de fournir des données techniques confidentielles appartenant au groupe. Sa curiosité n'ayant pas été assouvie, elle a ultérieurement réitéré sa demande par courriel, en recommandant à son interlocuteur d'utiliser une adresse électronique plus personnelle et si possible externe à l'entreprise dans le cadre de leurs échanges.

COMMENT SE PROTÉGER ?

En intégrant le risque lié aux visiteurs et aux stagiaires.

3.3) Les visiteurs et stagiaires

Tout visiteur ou stagiaire peut recueillir des informations jugées stratégiques pour l'entreprise (travaux de recherches ou d'études - techniques de fabrication avancées - politique commerciale, etc.)

■ ■ ■ ■ ■ Mesures communes aux visiteurs et stagiaires :

- définir une zone protégée interdite à toute personne non autorisée ;
- ne pas permettre que le visiteur entre en relation avec des salariés non préalablement désignés ;
- créer un circuit de visite et instituer le port du badge ;
- ouvrir un registre des visites ;
- accompagner le(s) visiteur(s) durant l'ensemble de la visite et établir un programme de visite ;
- ouvrir une consigne pour les téléphones portables ou autres appareils permettant des enregistrements photos, vidéos ou sonores.

■ ■ ■ ■ ■ Mars 2006

Un technicien d'une société d'aménagement intérieur travaillant sur un site particulièrement sensible, lié à la recherche de pointe, a été surpris à prendre des photos avec son mobile à l'intérieur d'une zone protégée de l'établissement. L'objet de son intervention ne justifiait en rien sa présence dans ce laboratoire.



■ ■ ■ ■ ■ Mesures spécifiques aux stagiaires :

- avant le stage : examen du CV, définition du contenu du stage, signature d'une clause de confidentialité et désignation d'un tuteur ;
- pendant le stage : veiller au respect des horaires et des lieux autorisés, prendre des mesures de surveillance et de contrôle concernant l'accès au réseau informatique, à la téléphonie et à la photocopieuse ; se faire communiquer une adresse où il peut être joint en cas d'urgence ;
- à la fin du stage : rédaction d'un rapport de sécurité par le tuteur et examen approfondi des travaux du stagiaire visant à la non divulgation de données jugées sensibles ou stratégiques (communication du rapport de stage au responsable «sécurité»). Récupération des badges et clés à l'issue du stage et changement des éventuels codes d'accès.

■ ■ ■ ■ ■ Juin 2005

Un étudiant étranger, accueilli dans un centre de recherches fondamentales dans le cadre de sa thèse, a détourné à son profit des informations confidentielles sur le point d'être brevetées. En effet, usant des droits informatiques de son tuteur imprudemment confiés par ce dernier, l'étudiant a obtenu, grâce à ces données, un prix dans une prestigieuse école européenne. Il aurait pu, sans l'intervention du centre français, obtenir une aide pour la création d'une entreprise innovante.

COMMENT SE PROTÉGER ?

En maîtrisant la communication de l'entreprise et les risques liés à l'environnement économique.

4) Maîtriser la communication de l'entreprise

Dans une économie mondialisée, la communication de l'entreprise est devenue vitale. Toutefois, cet exercice doit être maîtrisé.

■ ■ ■ ■ ■ **La communication écrite** : effectuer une relecture attentive des publications de l'entreprise, qu'elles soient internes (bulletin) ou externes (brochures, plaquettes de présentation, documentations techniques) et veiller à ce qu'elles ne livrent pas d'informations sensibles.

■ ■ ■ ■ ■ **Le site web** : prendre des précautions semblables pour les informations mises à disposition sur le site de l'entreprise à celles relatives aux publications écrites, tout en établissant également un contrôle des consultations du site web.

■ ■ ■ ■ ■ **La participation aux foires, salons et colloques** : assurer la protection des prototypes et contrôler la sensibilité des publications, échantillons, etc., exposés ou mis à disposition.

■ ■ ■ ■ ■ Septembre 2006

Lors d'un salon international, une société spécialisée dans l'équipement de pointe (dans les domaines aéronautique, spatial et nucléaire) a constaté la disparition d'un exemplaire unique d'un prototype concernant l'avionique. Outre le préjudice financier qu'elle a causé, cette disparition a eu pour conséquence d'entraîner un retard conséquent pour la commercialisation de ce nouveau produit. Même s'il n'a fait l'objet d'aucun brevet et n'entre dans aucun contrat classifié, il s'agit néanmoins d'un produit très concurrentiel, sans équivalent sur le marché, qui devait permettre à la société d'élargir son champ de prospection commerciale.

5) Maîtriser les risques liés à l'environnement économique et aux partenaires de l'entreprise

La sécurité et la compétitivité de l'entreprise dépendent de sa capacité à protéger ses informations stratégiques. Elles sont également subordonnées à son aptitude à analyser, et à maîtriser les risques générés par sa dépendance envers ses partenaires, ses sous-traitants et ses clients.

Quelques recommandations :

■ ■ ■ ■ ■ Protéger ses savoir-faire et informations stratégiques :

- en utilisant à bon escient les procédures visant la protection de la propriété intellectuelle et industrielle (dépôt de brevets, marques, dessins), afin de pouvoir lutter plus efficacement contre les risques de contrefaçon ou d'espionnage industriel ;
- en obtenant des partenaires habituels (clients, sous-traitants et filiales) ou occasionnels (consultants, stagiaires) la souscription à des clauses de confidentialité ou de non-concurrence ;
- en anticipant le départ de tout cadre affecté à un poste stratégique de l'entreprise (cessation d'activité, débauchage, etc.), par la préservation de ce savoir-faire (formation d'un autre cadre), et par des mesures de précaution en vue d'en empêcher la divulgation (signature préalable d'une clause de non concurrence).

■ ■ ■ ■ ■ Analyser le positionnement et la dépendance de l'entreprise par rapport à son environnement en s'interrogeant :

- sur la part que prend l'actionariat dans la mise en place de la stratégie et les risques de conflit d'intérêt avec un actionnaire ;
- sur la structure de la clientèle de l'entreprise : le chiffre d'affaires dépend-il d'un nombre limité de clients et quel est le degré de votre connaissance de vos clients (solvabilité, menaces de rachat) ;
- sur le positionnement de l'entreprise par rapport aux fournisseurs ou sous-traitants : existence de dépendance stratégique à l'égard de fournisseurs et risque éventuel de rupture d'approvisionnement ;
- sur le positionnement de l'entreprise par rapport à ses partenaires financiers : niveau d'endettement susceptible de présenter un risque pour l'entreprise et niveau de dépendance à l'égard des subventions publiques.

■ ■ ■ ■ ■ Le cas des Pôles de compétitivité

Les pôles de compétitivité répondent à un besoin vital de coopération. Ils permettent d'accélérer les flux d'innovations et valorisent les entreprises stratégiques, qui disposent ainsi de soutien pour améliorer leur compétitivité. Leur mode de fonctionnement en réseau sur des activités très innovantes, ayant vocation à connaître un rayonnement international, pose toutefois la question délicate des informations asymétriques détenues et échangées par les adhérents. La sécurité de l'ensemble du pôle dépend de la prise en compte de cette problématique par son organe de gouvernance. La sécurisation de la chaîne de validation des projets, ainsi que du réseau informatique sont donc des priorités, de même que la mise en place par chacun des acteurs du pôle d'une politique individuelle de sécurité informatique.

QUESTIONNAIRE D'AUTODIAGNOSTIC

Il ne s'agit pas de recenser toutes les vulnérabilités de l'entreprise, mais plutôt pour vous d'identifier vos points faibles en matière de sécurité économique. Ce questionnaire pourra ensuite servir de base de travail pour un examen plus approfondi de la situation de votre entreprise avec les services publics chargés d'une mission de sécurité économique.

1. Particularités du risque au sein de votre entreprise :		oui	non
Avez-vous identifié le savoir-faire le plus stratégique pour votre entreprise ?	<input type="checkbox"/>		<input type="checkbox"/>
Votre entreprise travaille-t-elle pour des secteurs d'activité sensibles tels que l'armement, l'aviation civile ou militaire, l'énergie, les nouvelles technologies ou autres ?	<input type="checkbox"/>		<input type="checkbox"/>
Etes-vous en position de leader sur l'un de vos marchés ?	<input type="checkbox"/>		<input type="checkbox"/>
Etes-vous associés ou partenaires d'un pôle de compétitivité ?	<input type="checkbox"/>		<input type="checkbox"/>
2. Sécurité physique de l'entreprise :			
Avez-vous réglementé l'accès et la circulation des personnes au sein de votre entreprise ? Ces règles sont-elles connues et appliquées ?	<input type="checkbox"/>		<input type="checkbox"/>
Avez-vous désigné ou recruté un personnel chargé de la sécurité ? Est-il connu du personnel de l'entreprise ?	<input type="checkbox"/>		<input type="checkbox"/>
Avez-vous assuré la protection du site par des barrières physiques (grilles, clôtures) ou par des moyens techniques de surveillance (détection d'intrusion, vidéosurveillance, etc.) ?	<input type="checkbox"/>		<input type="checkbox"/>
Les locaux contenant des informations sensibles sont-ils réellement sécurisés (contrôle d'accès, fermeture, etc.) ?	<input type="checkbox"/>		<input type="checkbox"/>
Assurez-vous une gestion des déchets (usage de déchiqueteuses ou incinération) et cette gestion est-elle confiée à un employé de confiance ?	<input type="checkbox"/>		<input type="checkbox"/>
Si votre entreprise recourt à une société de gardiennage et/ou de nettoyage, celle-ci est-elle bien identifiée, son accès aux locaux est-il limité et ses conditions d'intervention prédéfinies ?	<input type="checkbox"/>		<input type="checkbox"/>
En cas d'intrusion détectée, l'intervention est-elle organisée ou encadrée ?	<input type="checkbox"/>		<input type="checkbox"/>
3. Sécurité informatique :			
Existe-t-il une charte de sécurité pour l'usage d'internet et du matériel informatique ?	<input type="checkbox"/>		<input type="checkbox"/>
Avez-vous désigné un responsable des systèmes de sécurité de l'information (RSSI) ?	<input type="checkbox"/>		<input type="checkbox"/>
Votre personnel est-il sensibilisé aux règles élémentaires en matière de sécurité informatique (usage de mots de passe, de sauvegarde et d'antivirus) ?	<input type="checkbox"/>		<input type="checkbox"/>
Les postes informatiques connectés au réseau (intranet ou internet) sont-ils éteints tous les soirs et week-ends, voire durant les pauses repas ?	<input type="checkbox"/>		<input type="checkbox"/>
Interdisez-vous l'usage de matériels informatiques personnels dans l'entreprise et à vos collaborateurs de travailler en dehors de l'entreprise sur des données sensibles ?	<input type="checkbox"/>		<input type="checkbox"/>
4. Risques liés au facteur humain :			
Avez-vous mis en place une véritable politique de sécurité ? Si oui, a-t-elle été exposée et commentée à l'ensemble du personnel de l'entreprise ?	<input type="checkbox"/>		<input type="checkbox"/>
Des recommandations particulières sont-elles données aux personnels en déplacement (usage «contrôlé» de l'ordinateur portable, nature des documents emportés, personnes rencontrées, etc.) ?	<input type="checkbox"/>		<input type="checkbox"/>
Des mesures de sécurité ont-elles été prises pour encadrer les visites au sein de l'entreprise (parcours dit de «notoriété», définition de zones réservées, obligation du port de badge et tenue d'un registre de visiteurs) ?	<input type="checkbox"/>		<input type="checkbox"/>
Avez-vous établi des mesures spécifiques de contrôle de l'activité des stagiaires (droits d'accès au réseau informatique et à la documentation sensible de l'entreprise, rédaction d'un rapport de stage, désignation d'un tuteur et signature d'une clause de confidentialité) ?	<input type="checkbox"/>		<input type="checkbox"/>
5. Risques liés à l'environnement et à la communication de l'entreprise			
La communication écrite de l'entreprise fait-elle l'objet d'un contrôle par vous-même ou par un service spécialement chargé de cette mission ?	<input type="checkbox"/>		<input type="checkbox"/>
Avez-vous pris toutes les dispositions pour sécuriser votre site Web (contrôle des publications et des consultations du site) ?	<input type="checkbox"/>		<input type="checkbox"/>
Assurez-vous la sécurité de vos prototypes ou échantillons exposés à l'occasion des foires, salons ou colloques ?	<input type="checkbox"/>		<input type="checkbox"/>
Votre entreprise protège-t-elle ses informations stratégiques et ses process (par le dépôt de brevets, enveloppes Soleau, contrats, etc.) ?	<input type="checkbox"/>		<input type="checkbox"/>
Les mesures de protection prises sont-elles conformes au droit ?	<input type="checkbox"/>		<input type="checkbox"/>

Les quatre premières questions mises à part, plus le nombre de réponses «oui» est élevé, plus le niveau de sécurité est grand. **Mais attention** : il ne s'agit que d'une évaluation. Elle doit donc vous inviter à approfondir ce questionnaire pour mieux l'adapter aux réalités de votre entreprise.

VOS INTERLOCUTEURS EN ALSACE EN MATIERE DE SECURITE ECONOMIQUE

Structures	Missions	Contacts
	<p>La Direction de la Surveillance du Territoire (DST) mène des actions de contre-espionnage pour défendre les intérêts fondamentaux de la nation, et de contre-terrorisme. Elle assure aussi une mission de protection de notre patrimoine économique, par une démarche de sensibilisation individuelle et collective auprès des établissements scientifiques et industriels. Spécialisée dans la lutte contre la prolifération des armes de destruction massive, elle exerce également un contrôle du respect de la réglementation s'appliquant à nos structures les plus sensibles. Elle a compétence sur l'ensemble du territoire national.</p>	<p>Capitaine Olivier CHAMPEAU intel.eco-strasbourg@interieur.gouv.fr Tél : 03.90.23.13.20</p>
	<p>Force de sécurité, la gendarmerie participe à l'attractivité des territoires par la prévention des atteintes aux entreprises et par la sécurisation des axes d'échange. En effet, plus de 90% des TPE/PMI/PME sont implantées dans des régions où la gendarmerie exerce seule la responsabilité de sécurité publique. Fort de son maillage dense au travers des 4000 unités territoriales, elle partage quotidiennement l'information avec les entreprises et les concitoyens.</p>	<p>Lieutenant-colonel GAMET Chef du Bureau Emploi-Renseignement Région de Gendarmerie Alsace ber.strasbourg@wanadoo.fr Tél : 03.88.37.53.72</p>
	<p>Les Renseignements Généraux sont chargés de la recherche et de la centralisation des renseignements destinés à informer le gouvernement. Ils participent à la défense des intérêts fondamentaux de l'Etat et concourent à la mission générale de sécurité intérieure. Grâce à leur maillage territorial, et à leur connaissance intime des entreprises, les RG assurent également une mission d'Intelligence économique.</p>	<p>Commandant Dominique FUCHS Correspondant Intelligence Economique dominique.fuchs@interieur.gouv.fr Tél : 03.90.23.10.41</p>
	<p>La Direction de la Protection et de la Sécurité de la Défense (DPSD) est le service dont dispose le Ministre de la défense pour assumer ses responsabilités en matière de sécurité du personnel, des informations, des matériels et des installations sensibles du ministère, ainsi que les entreprises réalisant des travaux protégés, au titre de contrats classés ou à clause de sécurité. Sa mission fondamentale est la contre-ingérence, qui consiste à déceler et à déjouer les menaces relatives au terrorisme, à l'espionnage, à la subversion ou sabotage, et au crime organisé qui s'appliquent à la défense.</p>	<p>Lieutenant Thierry MEYNIEL Tél : 03.90.23.32.11</p>
	<p>Le chargé de mission régional à l'intelligence économique (CRIE) dépend du service de coordination à l'intelligence économique (SCIE) rattaché au secrétariat général du ministère de l'économie, des finances et de l'emploi, ainsi que du ministère du budget, des comptes publics et de la fonction publique. Il est placé auprès du Trésorier-payeur général de région, conseiller du Préfet de région pour les affaires économiques et met en œuvre la politique publique d'intelligence économique dans sa dimension territoriale, telle qu'elle est définie par le Préfet. Il est également à la disposition du Haut fonctionnaire de défense et de sécurité (HFDS) pour les missions de défense économique.</p>	<p>Laurent MACÉ Chargé de mission Intelligence Economique laurent.mace@finances.gouv.fr Tél : 03.88.56.54.95.</p>
	<p>La Division Développement Industriel de la Direction Régionale de l'Industrie, de la Recherche et de l'Environnement (DRIRE) Alsace accompagne financièrement les actions collectives incitant à la mise en réseau d'entreprises autour de projets structurants. Parmi ses priorités, elle soutient les initiatives collectives dans le domaine de l'intelligence économique.</p>	<p>Ferdinand TOMARCHIO Chef de la Division Développement Industriel ferdinand.tomarchio@industrie.gouv.fr Tél : 03.88.25.92.20</p>
	<p>Dans le cadre de son Schéma Régional de Développement Economique (SRDE), la Région Alsace, au travers de la Direction du développement économique, s'est fixée parmi ses objectifs de dynamiser l'attractivité et la compétitivité du site «Alsace». Ceci implique notamment le soutien à l'innovation sous toutes ses formes, l'accompagnement au développement du tissu économique dans toutes ses composantes et l'impulsion de stratégies et d'actions collectives dans le cadre de pôles et filières. C'est pourquoi, la Région Alsace compte poursuivre la dynamique engendrée par le lancement du programme COGITO et mener des actions en partenariat, afin d'élargir et de professionnaliser la pratique de l'intelligence économique.</p>	<p>Christophe SAGNIER Chargé d'études à la Direction du développement Economique christophe.sagnier@region-alsace.eu Tél : 03.88.15.66.82.</p>

SITES UTILES

www.inpi.fr > Institut National de la Propriété Industrielle |
 www.ladocfrancaise.gouv.fr > La Documentation Française
www.legifrance.gouv.fr > Site du Droit Français |
 www.adae.pm.gouv.fr > Agence pour le Développement de l'Administration Electronique |
 www.intelligence-economique.gouv.fr > le site du Haut Responsable pour l'Intelligence Economique
www.ssi.gouv.fr > Direction Centrale de la Sécurité des Systèmes d'Information (SGDN)