Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFECTURE DE LA RÉGION FRANCHE -COMTÉ
PRÉFECTURE DU DOUBS

GUIDE DES BONNES PRATIQUES EN MATIERE

D'INTELLIGENCE ECONOMIQUE

Novembre 2008

SOMMAIRE

GUIDE DES BONNES PRATIQUES
EN MATIERE
D'INTELLIGENCE ECONOMIQUE

Le mot du Préfet de Région :

Constituée de quatre départements, le Doubs, le Jura, la Haute-Saône et le Territoire de Belfort, la Franche-Comté bénéficie d'une situation géographique stratégique, car elle se situe au cœur de l'Europe, à proximité de grandes villes telles que Lyon et Strasbourg, mais aussi de régions très industrialisées, comme la région Rhône-Alpes ou le Land du Bade-Würtemberg en Allemagne. Elle développe en outre des liens privilégiés avec la Suisse, pays limitrophe avec lequel elle possède 230 kilomètres de frontières communes. Cette prise en compte de la réalité de la géographie économique incite certaines collectivités locales de cette zone à s'unir comme l'illustre la métropole Rhin-Rhône, association des villes et agglomérations franco-suisses.

L'industrie y occupe une place importante. Hormis quelques grands groupes nationaux et internationaux tels que Peugeot, Alstom, Smooby, General Electric, Solvay, Faurecia, le tissu industriel régional est composé de très nombreuses PME, dont certaines sont leaders dans leur domaine. Toutefois, c'est le secteur de la sous-traitance qui domine car il représente quelques 1.100 entreprises. Les secteurs industriels principaux sont l'automobile et le travail des métaux, avec un savoir-faire particulier en microtechniques et traitement des surfaces, héritage historique de l'industrie horlogère.

Toutefois la lunetterie, la plasturgie, la filière bois, les industries agroalimentaires et toutes les activités qui leurs sont liées constituent aussi une source importante d'emplois pour la région.

Le potentiel innovant de la région a également donné naissance aux pôles de compétitivité des Microtechniques et Véhicule du Futur. En raison de l'activité industrielle franc-comtoise, des partenariats sont naturellement engagés avec les pôles voisins Vitagora et Plastipolis.

Cette vitalité de l'industrie franc-comtoise ne manquera pas de susciter des convoitises. Afin de maintenir nos compétences régionales, de pérenniser nos activités industrielles et de préserver l'emploi, il convient de connaître les risques qu'encourent les entreprises face à la concurrence exacerbée née de la mondialisation et de la proximité de voisins étrangers dynamiques économiquement (Suisse, Allemagne).

L'objet des politiques nationale et régionale d'Intelligence Economique vise à apporter un soutien aux décideurs.

Il convient donc maintenant de résumer ces dispositifs avant de présenter les mesures qui peuvent être mises en œuvre au sein de chaque entreprise ou laboratoire.

A la suite de la publication en juin 2003 d'un rapport parlementaire intitulé « rapport Carayon », l'Etat a décidé d'engager une nouvelle politique publique pour faire face aux défis auxquels est confrontée l'économie française. Cette politique publique, dont la finalité est d'assurer la compétitivité du tissu industriel, la sécurité de l'économie et des entreprises, ainsi que le renforcement de l'influence de la France, fait appel au potentiel offert par l'intelligence économique, définie par l'actuel Haut Responsable pour l'Intelligence Economique comme « la maîtrise et la protection de l'information stratégique pour tout acteur économique ». Il s'agit, très concrètement, en mutualisant l'ensemble des ressources utiles de l'Etat, d'aider les différents acteurs économiques à développer la maîtrise et la protection des informations stratégiques, action qui pérennisera leurs activités économiques dans un monde ultra concurrentiel.

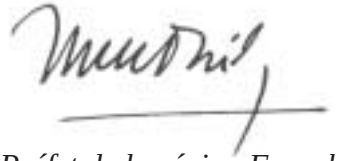
Cette politique publique d'intelligence économique se décline à deux niveaux :

Au plan national par des mesures de protection accrues à destination des pôles de compétitivité, ainsi qu'une attention soutenue envers des établissements considérés comme stratégiques et des mesures de soutien privilégié à l'investissement national pour ces entités.

Au plan régional, en Franche-Comté, par la mise en œuvre d'un schéma stratégique territorial d'intelligence économique qui comporte notamment, pour son volet défensif, un plan régional de sécurité économique au sein duquel trouve naturellement sa place un « guide des bonnes pratiques en matière d'intelligence économique ».

Ce « Guide des bonnes pratiques en matière d'Intelligence Economique », que vous avez actuellement entre les mains, a pour objectif de vous éclairer sur l'intérêt de la mise en œuvre et du suivi d'une véritable politique de sécurité économique au sein de votre établissement.

Jacques BARTHELEMY



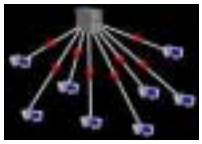
Préfet de la région Franche-Comté
Préfet du Doubs

GUIDE DES BONNES PRATIQUES
EN MATIERE
D'INTELLIGENCE ECONOMIQUE

Préambule

Si de nombreux chefs d'entreprise mesurent désormais l'intérêt de promouvoir l'intelligence économique sous son angle offensif, ils négligent souvent de consacrer du temps, un budget et donc des moyens à son aspect défensif. Pourtant, il est impératif d'avoir conscience que chaque société, *quelle que soit la taille,* peut devenir un jour une « cible » potentielle d'un concurrent averti et que dès lors, elle se trouvera vulnérable face à certaines pratiques, parfois déloyales, utilisées par la concurrence pour s'approprier ses innovations, son savoir-faire, ou pour la déstabiliser et l'affaiblir.

Exemple de vulnérabilité relevée



Printemps 2008
3 individus ont pénétré nuitamment dans les locaux d'une entreprise travaillant pour le domaine du nucléaire, avant de pirater le serveur de messagerie de la société. Le modus operandi utilisé (lignes téléphoniques coupées, hurleurs des alarmes brisés, pas d'effraction ni de vol, garage du responsable bloqué par une voiture) et l'attaque informatique réalisée sur le serveur pour permettre de le commander à distance montrent une grande technicité et illustrent le recours à des techniques illégales de recueil d'informations

Afin de pouvoir contrer ces menaces, il faut préalablement identifier ce qu'il est impératif de protéger sous forme d'un noyau dur d'informations stratégiques, puis connaître les moyens de protection disponibles afin de pouvoir mettre en œuvre ceux qui apparaissent les plus appropriés.

GUIDE DES BONNES PRATIQUES
EN MATIERE
D'INTELLIGENCE ECONOMIQUE

Que faut-il protéger ?

Il est impératif de protéger toute information dont la divulgation est susceptible d'apporter à une entreprise concurrente une plus-value, notamment en terme de compétitivité. Il convient de prendre conscience que la nature des informations à protéger ***est spécifique à chaque entreprise*** et peut même varier dans le temps. Il appartient donc au chef d'entreprise, avec l'assistance de ses cadres, d'identifier très précisément ce périmètre vital et de mettre en œuvre les moyens utiles de protection.

Bien que le « périmètre vital » susmentionné soit spécifique à chaque entité industrielle ou scientifique, certains renseignements sont toujours convoités par la concurrence. Ils concernent en particulier :

- La politique de recherche et développement
- La production
- La stratégie commerciale et le marketing de l'entreprise
- Le fonctionnement de l'entreprise

Comment se protéger ?

A l'analyse des préjudices subis par les entreprises en raison d'une atteinte, cinq grandes catégories de vulnérabilités ont été recensées :

- 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

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, et à interdire ainsi 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.

Exemple de vulnérabilité relevée

Février 2006 :

Dans le cadre d'un contact avec la direction d'un laboratoire de recherche, 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 permet qu'un contrôle vocal.***
- ***une fois dans les lieux, aucune vérification n'est effectuée et une personne étrangère peut aisément y circuler.***
- ***existence d'une simple porte en bois sans protection particulière permettant l'accès aux locaux.***
- ***absence d'une armoire forte pour la conservation des produits sensibles.***

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 et la prise de mesures spécifiques pour contrôler les accès ;
- 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, différencié par catégories de personnes (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).

Ces mesures méritent d'autant plus d'être prises qu'elles n'imposent pas nécessairement de lourds investissements et qu'elles constituent un premier et nécessaire filtre protégeant le patrimoine de l'entreprise.

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.

Exemple de vulnérabilité relevée :

Automne 2007 :
Un serveur informatique destiné à un organisme de recherche dédié à la sauvegarde et à la conservation des données importantes dans le cadre de la recherche fondamentale a fait l'objet d'une intrusion informatique, au cours de laquelle a eu lieu une tentative de téléchargement d'informations.

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 pare-feu, 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 connections sans fil par rapport à l'environnement de l'entreprise (Wi-fi notamment).

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).

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.

Exemple de vulnérabilité relevée

Très régulièrement, les entreprises et laboratoires subissent des vols d'ordinateurs portables, que des mesures de sécurité élémentaires auraient pu éviter. Le préjudice subi est très souvent lourd de conséquences, surtout s'il s'agit d'un vol ciblé, mais également lorsqu'il s'agit « seulement » d'un acte crapuleux.
Juin 2008 :
Un ordinateur portable appartenant au responsable d'une PME travaillant pour la Défense a été volé par effraction au sein de la société. Cet ordinateur dont le contenu n'était pas chiffré, contenait des développements logiciels spécifiques ainsi qu'un grand nombre d'e-mails et le carnet d'adresses Internet. La probabilité d'un vol ciblé est très forte.
Eté 2008 :
Une valise « égarée » dans un aéroport étranger a été restituée le lendemain à son légitime propriétaire. Après inventaire du contenu du bagage, il était constaté l'absence d'une clé USB contenant des informations stratégiques en rapport avec l'activité d'une entreprise française travaillant pour les domaines aéronautique et spatial. A l'analyse, il ne fait aucun doute qu'il s'agit d'une opération ciblée de recueil de renseignements économiques, ayant probablement bénéficié du soutien des services spéciaux du pays où se trouve implantée la société étrangère concurrente.

Quelques recommandations

Au sein de l'entreprise :

- ranger systématiquement l'ordinateur portable en lieu sûr (armoires fortes) ou à défaut utiliser des antivols 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. Prendre systèmatiquement en considération le risque de vol (cf. exemple supra).

2.3) Autres équipements de TIC

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

Une copie des documents traités sur des photocopieurs munis d'un disque dur peut être récupérée, notamment lors d'opérations de maintenance.

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 (envois extérieurs, journal des appels, « entrée en tiers etc…) ;
  - sensibiliser les personnels 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, à la télécopie ou au téléphone, sauf en utilisant des lignes sécurisées, ou en procédant au cryptage des données.

3) INTÉGRER LE RISQUE LIÉ AU FACTEUR HUMAIN

Le personnel 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 indélicats.

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.

Exemple de vulnérabilité relevée

Hiver 2007 :

Un ingénieur d'une grande entreprise française a transmis de façon quelque peu hâtive et inconsidérée des informations sollicitées téléphoniquement par un ingénieur étranger, employé dans une entreprise partenaire. Ce n'est qu'ultérieurement qu'il a appris que cet étranger n'était pas fiable et qu'il a alors pris conscience qu'il était allé « trop loin » dans la communication d'informations sensibles.

Il est de l'intérêt de l'entreprise de mettre en place une politique de sécurité économique qui lui est 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 la pérennité de l'activité, 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…).

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.

Exemple de vulnérabilité relevée

Printemps 2008 :

Après avoir parfaitement ciblé les personnels français susceptibles de détenir les connaissances technologiques manquantes, des cadres de l'entreprise étrangère cliente au sein de laquelle les expatriés français intervenaient, ont exercé des pressions sur nos compatriotes afin d'obtenir de précieux renseignements d'ordre technologique. Deux d'entre eux se sont vus proposer la remise d'une importante somme d'argent et un troisième se serait fait « piéger » en acceptant les faveurs d'une prostituée.

- 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, sans 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 » et refuser les propositions « alléchantes »

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…)

Exemple de vulnérabilité relevée

Printemps 2008 :

Après avoir été exclu d'un organisme de recherche français, un doctorant tiers a pu continuer ses travaux concernant des applications sensibles car il avait, préalablement à son renvoi, « cloné » l'unité centrale du laboratoire dans lequel il exerçait et disposait des logiciels d'imagerie 3D nécessaires pour poursuivre ses travaux.

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.

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 le stagiaire 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 clefs à l'issue du stage et changement des éventuels codes d'accès.

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.

Exemple de vulnérabilité relevée

Avril 2006

Le responsable d'une unité de recherche médicale a soumis ses travaux pour avis avant publication, à un confrère étranger de réputation internationale et travaillant sur les mêmes sujets. Celui-ci a pourtant profité de ces échanges pour s'attribuer la paternité des travaux, les publiant sous son nom dans les revues scientifiques ad hoc. Il a également déposé un brevet sur l'une des découvertes et en vend désormais les licences d'exploitation au plus grand bénéfice de son laboratoire. N'ayant pas pris les mesures adéquates, le chercheur français a renoncé à lancer la moindre procédure contre son confrère indélicat.

Année 2008 :

A l'occasion d'un grand salon professionnel international, une société étrangère a refusé le stand de 2000 m2 qui lui était initialement proposé pour s'installer sur un plateau de 150 m2 dont le seul intérêt résidait précisément dans sa localisation géographique, à proximité immédiate des emplacements des sociétés. Au cours de la période d'ouverture du Salon aux seuls professionnels, ont pu être observés, par une porte arrière restée ouverte, de nombreux appareils électroniques, pouvant être assimilés à des dispositifs d'interception des communications radio-électriques et/ou téléphoniques (par voie hertzienne). Etaient notamment présents des équipements d'analyse et de traitement des signaux acoustiques.

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 à celles relatives aux publications écrites pour les informations mises à disposition sur le site de l'entreprise, 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.

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.

Exemple de vulnérabilité relevée

Printemps 2008 :

Un consultant spécialisé dans les nouvelles technologies de l'information et de la communication, ayant effectué une mission de quelques mois au sein d'un groupe industriel français, a créé une société concurrente dans un pays européen, en dépit des accords de confidentialité et de non concurrence stipulés dans son contrat et serait même sur le point de livrer la technologie de son ancien employeur à des clients chinois.

Printemps 2008 :

Un homme d'affaires étranger s'est rapproché d'une jeune société française particulièrement innovante dans le domaine de la transmission de communications. Sous couvert d'un audit préalable à de juteux contrats, il a obtenu des informations, tant techniques que commerciales, auprès de la direction bien naïve de l'entreprise et n'a bien sûr donné aucune suite aux « propositions » commerciales initiales.

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 son 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'actionnariat 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 connaissance des clients (leur solvabilité, les menaces de rachat qui pèsent sur eux) ;
- 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.

Questionnaire d'autodiagnostic

Il ne s'agit pas de recenser toutes les vulnérabilités de l'entreprise mais d'identifier ce qui paraît être les points faibles majeurs de sa sécurité.

	OUI	NON
1 – PARTICULARITES DU RISQUE AU SEIN DE NOTRE ENTREPRISE :		
1. Votre entreprise possède-t-elle un savoir faire unique ou hautement technologique ?	☐	☐
2. Votre entreprise travaille-t-elle pour des secteurs d'activités sensibles tels que l'armement, l'aviation civile ou militaire, l'espace, l'énergie, les nouvelles technologies ou autres	☐	☐
3. Estimez-vous être une cible potentielle pour des pirates informatiques ?	☐	☐
2 – SECURITE GENERALE DE L'ENTREPRISE :		
1. Estimez-vous que votre entreprise est bien protégée contre tous types d'intrusions ou de piratages ?	☐	☐
2. La sécurité de votre entreprise justifie-t-elle une ligne budgétaire à part entière ?	☐	☐
3. Existe-t-il une démarche de sécurité (objectifs, organisation, moyens, procédures, systèmes d'alerte …) ?	☐	☐
4. Avez-vous désigné ou recruté un personnel chargé de la sécurité ? Est-il connu du personnel ?	☐	☐
5. Avez-vous procédé ou fait procéder à un diagnostic de sécurité de votre entreprise ?		
3 – SECURITE DES LOCAUX :		
1. Avez-vous réglementé l'accès et la circulation des personnes au sein de votre entreprise ? Ces règles sont-elles connues et appliquées ?	☐	☐
2. Les locaux contenant des informations sensibles (bureau d'étude – local serveur – comptabilité …) sont-ils réellement sécurisés (fermés à clef, clefs dans le coffre-fort, permissions à employés compétents, contrôle d'accès,alarme …) ?	☐	☐
3. Vos déchets de papier sont-ils systématiquement passés à la déchiqueteuse ou incinérés ?	☐	☐
4. Les déchets de votre société sont-ils gérés par un employé de confiance ?	☐	☐
5. Les services d'entretien de votre entreprise travaillent-ils pendant les heures ouvrables ?	☐	☐
6. Existe-t-il une classification d'accès selon les secteurs de sensibilité ?	☐	☐
7. Existe-t-il des moyens techniques de surveillance (détection d'intrusion, éclairage sectorisé, vidéo ou télésurveillance …) ?	☐	☐
8. En cas d'intrusion détectée, l'intervention est-elle organisée et encadrée ?	☐	☐
9. Les visiteurs sont-ils accueillis selon un processus déterminé ? Le personnel en charge de l'accueil est-il sensibilisé aux risques de captation d'informations par manipulation psychologique ?	☐	☐
10. Si l'entreprise fait appel à une société de gardiennage et/ou de nettoyage, celle-ci est-elle bien identifiée (dirigeants, nationalité …) ? Son accès aux locaux est-il limité ? Ses conditions d'intervention dans l'entreprise sont-elles précisées ?	☐	☐

Questionnaire d'autodiagnostic

	OUI	NON
4 – SECURITE DE L'INFORMATION :		
1. La sécurité de l'information est-elle prise en compte ?	☐	☐
2. Avez-vous identifié et inventorié les informations sensibles de votre entreprise ?	☐	☐
3. Des règles d'archivage, de sauvegarde des données, de secours, et de destruction des supports sont-elles instaurées ?	☐	☐
4. Avez-vous instauré une politique de classification et d'accès à l'information physique et informatique ?	☐	☐
5. Vous êtes assuré. Une clause de confidentialité existe-t-elle dans le contrat ? La compagnie d'assurance de votre entreprise est-elle bien identifiée (dirigeants, nationalité …) ?	☐	☐
5 – SECURITE INFORMATIQUE :		
1. Une charte de sécurité pour l'usage d'Internet et des ordinateurs portables est-elle en place ?	☐	☐
2. Le personnel est-il sensibilisé aux risques liés à l'informatique, aux réseaux, aux portables ? Applique-t-il des règles précises de sécurité (relatives aux mots de passe, à l'orientation des écrans, à l'extinction des ordinateurs en fin de service, à l'envoi de courriels …) ?	☐	☐
3. Les connaissances du personnel sont-elles actualisées en matière de sécurité informatique ?	☐	☐
4. Avez-vous entendu parler d' « ingénierie sociale » (social engineering) ?	☐	☐
5. La conception de vos réseaux internes et externalisés a-t-elle été réalisée par un professionnel ?	☐	☐
6. Contrôlez-vous régulièrement l'utilisation des postes de votre entreprise avec votre administrateur réseau en la présence de vos employés ?	☐	☐
7. La maintenance et la sécurité informatique de vos réseaux sont-elles prises en charge par un professionnel ? La société et les personnes qui en sont chargées sont-elles clairement identifiées ?	☐	☐
8. Vos réseaux internes et externalisés sont-ils dissociés ?	☐	☐
9. Les postes informatiques connectés au réseau (intranet ou internet) sont-ils éteints les soirs et week-ends voire durant les pauses repas ?	☐	☐
10. Interdisez-vous : ⇨ l'usage de matériels informatiques personnels dans l'entreprise ? ⇨ à vos collaborateurs de travailler en dehors de l'entreprise sur des données sensibles ?	☐ ☐	☐ ☐
11. Changez-vous régulièrement les mots de passe des postes informatiques, des serveurs ?	☐	☐
12. Vos mots de passe comportent-ils plus de 7 caractères ?	☐	☐
13. Vos mots de passe comportent-ils des caractères alphanumériques, des accentuations, et/ou des caractères spéciaux ?	☐	☐

Questionnaire d'autodiagnostic

	OUI	NON
6 – SECURITE DES TRANSPORTS SENSIBLES :		
1. Le transport de fret et de courrier sensible est-il organisé et fait-il l'objet d'un outil spécifique ?	☐	☐
2. Les incidents survenus à l'occasion du transport sont-ils signalés, répertoriés puis analysés ?	☐	☐
3. Si l'entreprise fait appel à une société de transport de fret ou de courrier sensible, celle-ci est-elle bien identifiée (dirigeants, nationalité …) ? Ses conditions d'intervention sont-elles précisées ?	☐	☐
7 – SENSIBILISATION DES PERSONNELS ET PARTENAIRES :		
1. Vos employés et/ou vous-même avez suivi une formation : ⇨ sur la sécurité informatique ? ⇨ sur la sécurité des entreprises ?	☐ ☐	☐ ☐
2. Le règlement intérieur, l'affichage, les contrats de travail particuliers mentionnent-ils une obligation de confidentialité ?	☐	☐
3. Avez-vous défini des règles relatives à la communication interne et externe ?	☐	☐
4. Si l'entreprise fait appel à un cabinet d'audit, de conseil, de lobbying, etc… celui-ci est-il bien identifié (dirigeants, nationalité …) ?	☐	☐
5. Les partenaires et sous-traitants sont-ils liés par une obligation de confidentialité ?	☐	☐
6. Vos partenaires sont-ils associés à la sécurité de l'information ?	☐	☐
7. Souhaiteriez-vous participer à des conférences thématiques relatives à la sécurité des entreprises ?	☐	☐
8 – SECURITE JURIDIQUE :		
1. L'entreprise protège-t-elle ses informations stratégiques et ses process (brevets, enveloppe Soleau, dépôts de marques et modèles, contrats …) ?	☐	☐
2. Les mesures de protection qu'elle prend sont-elles conformes au droit ?	☐	☐

Sans tenir compte des trois premières questions, 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, qui doit néanmoins vous inviter à prendre les mesures utiles à assurer une meilleure sécurité au sein de votre établissement.

Direction Régionale du Renseignement Intérieur
Capitaine Patrick THOMAS
intel.eco-besancon@interieur.gouv.fr
Tél : 03-81-21-11-91

Gendarmerie Nationale
Capitaine Bruno MIGEOT
bruno.migeot@gendarmerie.interieur.gouv.fr
Tél : 03-81-40-50-53
Adjudant Christophe ROUBEY
christophe.roubey@gendarmerie.interieur.gouv.fr
Tél : 03-81-40-50-43

Trésorerie Générale - Service de Coordination
à l'Intelligence Economique
Monsieur Ouahid BEN AMAR
Chargé de Mission régional à L'Intelligence Economique
ouahid.ben-amar@finances.gouv.fr
Tél : 03-81-25-20-23

Vos interlocuteurs en Région Franche-Comté