MAÎTRISE ET PROTECTION DE L'INFORMATION

Juin 2006

Rédigé par le CLUSIF, le document **"MAÎTRISE et PROTECTION de l'INFORMATION"** vise à sensibiliser **les responsables d'entreprise, principalement de PME,** aux risques inhérents à l'utilisation des technologies de l'information et de la communication et à **les aider à s'engager dans une politique réfléchie, globale et structurée de protection de leurs informations.**

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

30, rue Pierre Sémard, 75009 PARIS
Tél. : +33 153 25 08 80 – Fax : +33 1 53 25 08 88
e-mail : clusif@clusif.asso.fr - Web : http://www.clusif.asso.fr

TABLE DES MATIÈRES

REMERCIEMENTS

Le CLUSIF tient ici à mettre à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Eric	**BALANÇA**	*Venice Security*
Bruno	**KEROUANTON**	*Clear Channel*
Jean	**LACROIX**	*ERCOM*
Eric	**PETIT**	*Ministère de l'économie des finances et de l'industrie*
Erick	**SABATIER**	*Ecureuil Vie – Groupe Caisse d'Epargne*

Ainsi que les membres du CLUSIF et les personnes compétentes ayant participé au comité de relecture.

« *Ne pas prévoir, c'est déjà gémir !* » (Léonard de Vinci)

« *Mieux vaut penser le changement que changer de pansement*. » (Francis Blanche)

1 Histoires vraies

Aujourd'hui, qu'elle soit grande ou petite, **l'entreprise est soumise à une concurrence de plus en plus intense et complexe.** La mondialisation des échanges et la globalisation de l'offre de produits et services modifient les habitudes et les attitudes des clients. Leurs attentes en matière de prix, de qualité, de réactivité, d'innovation, de design, de packaging, de services associés, sont autant d'informations qu'une entreprise doit savoir déchiffrer et maîtriser pour conserver ou accéder à de nouveaux marchés.
L'entreprise est aussi confrontée à de brusques changements de son environnement, comme par exemple, l'apparition d'un concurrent agressif, l'introduction de contraintes normatives ou de nouveaux comportements commerciaux. Pour anticiper ces évolutions, les décideurs ont besoin **des bonnes informations**, **au bon moment, dans un format exploitable**.

Dans le cadre de son activité, l'entreprise est également dans **l'obligation de diffuser des informations**. Lorsqu'elle recherche des clients, travaille avec des partenaires, informe ses actionnaires, ses employés, la société transmet un grand nombre d'éléments sur son activité, son organisation, sa stratégie ou ses projets.

Enfin, dans une compétition où l'image est devenue prééminente, l'entreprise doit savoir **communiquer pour protéger ses intérêts**, tout en observant les espaces où circulent les informations, les avis, les appréciations, les rumeurs, les bruits la concernant.

Pour gérer ces flux d'informations, la quasi-totalité des entreprises utilise **les technologies numériques de l'information et de la communication, en particulier le réseau Internet, facteurs de compétitivité mais aussi sources de vulnérabilités**. C'est pourquoi, l'entreprise doit sécuriser l'information pour, à la fois :

- Prévenir **les diffusions intempestives** d'informations devant rester confidentielles.
- Agir contre **les manipulations** d'informations la concernant.
- Ne pas faciliter **la captation illégale** de ses données.

"Echec à l'exportation" et "**Pression concurrentielle"** sont deux mésaventures arrivées à des entreprises trop confiantes alors qu'un peu d'organisation et quelques moyens leur auraient permis de sécuriser l'information et d'éviter bien des déboires.

Echec à l'exportation

Une PME française de 200 personnes, leader sur le marché hexagonal des pièces détachées de machines-outils pour l'industrie automobile, souhaitait développer son portefeuille de clients étrangers afin de s'adapter aux opérations de délocalisation de ses clients.

Elle répondit à l'appel d'offres d'un important constructeur automobile chinois qui cherchait à moderniser l'ensemble de ses lignes de production. Pour la première fois, la PME française était en compétition avec trois entreprises étrangères, une allemande, une coréenne et une américaine, loin de son environnement d'affaires habituel. Elle envoya les éléments techniques demandés par Internet et, quelques jours avant l'annonce du résultat de la consultation, ses responsables se rendirent en Chine pour communiquer l'offre finale en matière de prix.

Ayant analysé les produits concurrents, les industriels français sont persuadés que le marché ne saurait leur échapper. Et pourtant, c'est l'entreprise américaine qui l'emportera.
Les responsables chinois ont exposé les facteurs qui ont guidé leur choix.

Le premier était la maîtrise des éléments techniques du cahier des charges. Les sociétés française et américaine avaient un niveau équivalent.
Le second était le prix. La proposition américaine se situait 5 % en dessous de celle de la société française.

Les dirigeants de l'entreprise française l'apprendront plus tard : le concurrent américain avait eu connaissance de l'ensemble de leur dossier technique et accès à leur proposition de prix avant l'annonce de la décision de l'acheteur chinois.

Les raisons d'un échec

Compte tenu de la qualité et de la valeur technique de son offre, l'entreprise française aurait dû remporter le marché. Toutefois, elle s'est affaiblie elle-même, en commettant trois erreurs :

- La transmission des éléments techniques s'est effectuée par Internet sans protection particulière. Elle a probablement été interceptée.
- Lors du déplacement en Chine, durant un dîner organisé pour l'ensemble des soumissionnaires, les ordinateurs portables des dirigeants français sont restés dans leurs chambres d'hôtel. Celles-ci ont été visitées et les éléments constitutifs de la tarification, stockés sur un ordinateur portable, ont été copiés.
- L'entreprise française a limité ses recherches d'informations sur ses concurrents à leurs compétences techniques. Une approche plus générale lui aurait permis de savoir que le groupe américain avait déjà connu des démêlés judiciaires, au Brésil et au Moyen-Orient, à la suite de marchés remportés "de justesse".

Ce qu'il aurait fallu faire

Pour mettre toutes les chances de son côté, l'entreprise française aurait dû prendre une série de mesures associant des éléments stratégiques, comportementaux et techniques.

Les éléments stratégiques
L'analyse des informations ouvertes (marketing, produits, recrutement, organisation, image…) sur les concurrents aurait fourni des indications précieuses, en particulier sur leurs stratégies commerciales.
Cela supposait une démarche cohérente d'intelligence économique – identification de la nature des informations utiles, plan de recherche, validation, tri, analyse des résultats, mise à disposition des décideurs concernés - impulsée par la direction générale et accompagnée d'investissements en moyens humains et techniques.

Les éléments comportementaux
Pour un appel d'offres stratégiques, d'un montant élevé sur un marché en pleine croissance dans un pays aux pratiques commerciales incertaines, les dirigeants auraient dû manifester plus de vigilance.
Ils auraient pu présumer de la possibilité de pratiques déloyales de la part de leurs concurrents et adopter des comportements adaptés. Par exemple, l'association aux ordinateurs portables de supports amovibles – Cédérom, Clé USB - conservés par les responsables tout au long de leur séjour, aurait réduit les risques de vol d'informations confidentielles.

Les éléments techniques
Des outils de sécurisation pour le stockage et la transmission de documents sensibles, en particulier de chiffrement fort, auraient, soit empêché l'exploitation des documents transmis sur Internet, soit réduit son temps d'exploitation de la durée nécessaire pour "casser" les clés.
De même, si l'ordinateur "visité" à l'hôtel avait été protégé par des mots de passe solides ou d'autres dispositifs physiques, l'intrusion aurait été plus compliquée et aurait, peut-être, échoué. A défaut de mesures de protection pour empêcher le vol d'informations, un système de détection de copie du disque dur, aurait incité les responsables à adapter leur proposition.

Pression concurrentielle

Un éditeur de logiciels dispose d'une centaine de clients fidèles. Spécialisé sur le marché des applications verticales pour les entreprises du secteur alimentaire, il n'a pas de réels concurrents sur le marché français.
Un jour, des acheteurs le sondent sur d'éventuels bogues dans la dernière version de son logiciel. Ces derniers lui indiquent qu'ils ont reçu des appels de journalistes sollicitant des témoignages d'utilisateurs rencontrant des difficultés avec un module du logiciel. Aucun défaut sérieux n'ayant été documenté sur cet élément, l'entreprise ne réagit pas à cette alerte.
Pourtant, un communiqué diffusé par une agence de relations publiques britannique, s'appuyant sur "l'étude d'un cabinet indépendant", mentionne des

problèmes lors de mise à jour du logiciel. Plusieurs journaux de la presse informatique reprendront ces allégations, en les complétant par des analyses sur les conséquences pour le devenir de l'éditeur.
Parallèlement à cette rumeur sur la qualité du logiciel et sur ses répercussions financières, l'éditeur français s'aperçoit que ses commerciaux sont démarchés par un cabinet de recrutement et que les noms de domaines Internet le concernant sont systématiquement réservés par une société inconnue.
Il prend enfin conscience qu'une campagne de déstabilisation est orchestrée contre lui. Cependant, malgré une mise au point officielle sur la fiabilité de ses produits et sur sa situation économique, la méfiance s'est instaurée et plusieurs contrats en cours de négociation seront annulés.

Les raisons d'une vulnérabilité

La chaîne de vulnérabilités ne concerne pas directement le système d'information de l'entreprise mais le manque d'intérêt porté à l'environnement et au capital informationnel - image, savoir de ses commerciaux, protection de sa marque -.

Exploitant tranquillement depuis plusieurs années une activité de niche, l'éditeur n'était pas préparé à faire face à une situation exceptionnelle. L'opération de déstabilisation menée par un cabinet étranger spécialisé n'aurait peut être pas aussi bien réussi si l'éditeur français avait :

- été attentif aux signaux faibles. Les questions de ses clients auraient dû l'alerter, d'autant que les interrogations sur la fiabilité de son logiciel étaient relayées, dans des forums Internet, par des échanges entre informaticiens d'entreprises du secteur alimentaire ;
- communiqué pour ne pas permettre à la rumeur de prendre corps et de se propager ;
- pris rapidement des dispositions spécifiques aux situations de crise.

Ce qu'il aurait fallu faire

Compte tenu qu'aucune entreprise n'est à l'abri d'une crise majeure, une telle éventualité aurait dû être envisagée et les conditions pour y faire face, définies à l'avance.

Cela supposait :

- d'identifier les vulnérabilités de l'entreprise et les risques potentiels ;
- de sensibiliser et former les dirigeants à accepter "l'imprévu" et à adopter les bonnes réactions ;
- d'élaborer des dispositions spécifiques et des scénarios d'actions possibles, afin d'avoir une "boîte à outils" permettant de réagir vite.

Le plus en amont possible, l'entreprise aurait pu disposer des capteurs identifiant les signaux faibles annonciateurs de difficultés à venir : rumeurs, obligation de rappeler un produit, crise sociale, contestation d'une "association", introduction d'une nouvelle réglementation, etc.
Cela passait par l'utilisation d'outils spécifiques d'analyse des forums Internet, par l'écoute des différents partenaires de l'entreprise, par l'étude des changements dans le comportement des fournisseurs ou des clients, etc.

Une fois la crise déclenchée, l'entreprise aurait dû accepter de :

- s'engager - une crise ne se résout pas sans une intervention volontariste des dirigeants des entreprises concernées - ;
- ne pas chercher à la minimiser - ou à la déporter sur un tiers - ;
- lui consacrer des moyens - humains, techniques et organisationnels - suffisants pour sa gestion et sa résolution.

La constitution d'une cellule de crise, la mobilisation de différents vecteurs de communication - sites Web de crise et interventions dans les forums, contrôle des interviews des employés, communiqués de presse, etc -, éventuellement le recours à des professionnels habitués aux traitements des situations exceptionnelles, sont souvent indispensables pour sortir rapidement de la crise et pour en limiter ses conséquences.

2 L’intelligence économique

Le Haut responsable pour l'intelligence économique auprès du Premier ministre, Alain Juillet, définit **l’intelligence économique** comme **"la maîtrise et la protection de l’information stratégique pertinente par tout acteur économique"**.

Pendant longtemps, en particulier lorsqu'il s'agissait d'une PME, le chef d'entreprise avait la possibilité de gérer seul l'ensemble des informations nécessaires à la conduite de sa structure. Désormais, pour **assurer la compétitivité de son entreprise,** le dirigeant a besoin d'**intégrer un nombre croissant de paramètres** - économiques, financiers, normatifs, technologiques, juridiques, politiques, sociétaux, etc. – qui doivent être validés, valorisés et pour certains sécurisés.

Si dans les dispositifs de maîtrise de l'information mis en place, **la dimension humaine reste prépondérante,** les technologies de l'information et de la communication offrent de nombreux outils efficaces pour :

- **Rechercher, exploiter et conserver** les informations.
- **Diffuser** rapidement et massivement **des informations** tout en **en protégeant d'autres** qui ne doivent être accessibles qu'à certaines personnes bien identifiées.
- **Défendre** l'entreprise et **garantir sa réputation**, en intervenant dans une multitude d'espaces d'information et de décision.

En utilisant le réseau Internet, l'entreprise accède rapidement et facilement à une masse considérable d'informations. Les moteurs de recherche, la consultation du Web invisible, l'interrogation de bases de données, le recours à des logiciels spécialisés – aspiration ou surveillance de sites, analyse sémantique de textes, création automatique de résumés, cartographie des résultats, traductions à la volée de sites en langue étrangère, etc.- démultiplient ses capacités de recherche.

Pour réaliser une veille étendue, l'entreprise complète ses informations obtenues à partir de sources électroniques par la lecture de la presse généraliste et spécialisée, l'étude des rapports d'activité et des documents publicitaires de ses concurrents et partenaires. Elle interroge les organisations et fédérations professionnelles, les chambres consulaires, les dispositifs publics d'information des entreprises, les réseaux d'experts. Elle participe à des salons, des colloques. Elle exploite les savoirs déjà capitalisés dans l'entreprise ainsi que des échanges informels avec ses partenaires – clients, fournisseurs, concurrents, etc. –.

Dans sa démarche d'intelligence économique, l'entreprise respectera quelques règles.

- **La majeure partie des informations utiles à l'entreprise est disponible sur des "sources ouvertes".** Cela ne signifie pas que ces informations sont gratuites mais qu'elles sont accessibles sans l'utilisation de moyens illégaux – vol, extorsion, chantage, atteinte au secret des correspondances, usurpation d'identité qui engagent la responsabilité civile ou pénale de l'entreprise.
- **Le droit de la propriété intellectuelle est connu.** Toute reproduction ou copie pour un usage professionnel d'un écrit, d'une image, d'un enregistrement sonore sans l'accord de son auteur est une contrefaçon. A condition de citer les noms des auteurs et ses sources, il est néanmoins possible de reprendre de courtes citations, faire des commentaires de textes ou réaliser des revues de titres de presse – à ne

pas confondre avec un "panorama de presse" correspondant à l'assemblage d'articles ou d'extraits d'articles -.

- **Les dispositions sur les libertés individuelles sont assimilées.** Par exemple, si les traitements d'informations conduisent à l'élaboration de bases de données contenant des données sur des personnes physiques ; ces traitements seront déclarés. En cas de doute, l'entreprise peut consulter la Commission Nationale Informatique et Liberté (CNIL).

Pour être efficace, avant de se lancer dans la collecte d'informations, l'entreprise a intérêt à **identifier ses besoins** et **élaborer un plan de recherche** en fonction de sa stratégie et des objectifs poursuivis. Elle définira des moyens financiers et humains ainsi que le temps d'investigation disponible. Elle fixera la précision et l'originalité des informations à trouver.

La veille correspond à la première étape du dispositif d'intelligence économique. Pour être pleinement exploitées, les données rassemblées nécessitent généralement d'être **triées, validées, analysées et reformatées**. Afin de s'aider dans cette démarche, l'entreprise peut utiliser de nombreux outils numériques.
Des outils de gestion documentaire permettent le classement par thèmes, l'indexation des documents par mots clés, la sélection de personnes habilitées à certains documents protégés.
Des logiciels d'analyse dégagent les grandes tendances, les corrélations, les signaux faibles des informations reçues et stockées.
D'autres programmes informatiques réalisent automatiquement des résumés de documents, organisent et cartographient les connaissances.
Des dispositifs permettent d'être alertés lors de l'arrivée de nouvelles informations, de gérer l'expertise disponible et d'assurer une exploitation en commun de l'information stratégique.

Si pour disposer d'informations et brasser des idées, l'entreprise peut s'appuyer sur l'ensemble de ses collaborateurs et partenaires, la structuration et la valorisation des données nécessitent un peu de savoir-faire. Elles seront confiées, de préférence, à une personne – ou une équipe – curieuse mais aussi discrète, parlant anglais et intéressée par les technologies de l'information.
L'entreprise a aussi la possibilité de faire appel à des compétences externes : consultants privés, services de l'administration ou chambres consulaires.
Quel que soit l'organisation et les outils mis en place, **l'intelligence économique** doit être considérée comme **un moyen pour éclairer et accompagner des décisions.** Sa finalité n'est pas de se substituer aux choix et aux responsabilités des dirigeants.

Un dispositif d'intelligence économique sert également à **promouvoir la notoriété de l'entreprise** et **défendre ses intérêts par des actions d'influence** sur son environnement.
Comme pour la recherche d'informations, ces actions de communication s'inscriront dans le cadre de la légalité. Elles ne dénigreront pas ou ne désorganiseront pas les concurrents, ne chercheront pas à tromper les partenaires ou les décideurs publics.

Une démarche maîtrisée de veille, de gestion et de partage de l'information implique que l'entreprise détermine les informations dont la confidentialité doit être assurée, non seulement en raison des inconvénients que leur divulgation entraînerait, mais aussi des exigences légales ou réglementaires existantes. **La politique de sécurité relative à son capital et son environnement informationnels portera en priorité sur son organisation interne et son système d'information, élément central de la gestion de l'information, mobilisera son personnel et ses partenaires, couvrira sa communication et la diffusion d'informations la concernant**.

En résumé, l'intelligence économique c'est :

1. **S'appuyer sur une démarche et une organisation structurées émanant de la volonté du plus haut niveau de l'entreprise.** L'intelligence économique ne consiste pas "à faire de la prose comme Monsieur Jourdain".

2. **Répondre à des besoins précis préalablement identifiés.** L'intelligence économique ne vise pas à tout savoir, tout contrôler, tout protéger.

3. **Encourager la circulation et le partage des informations,** en élaborant et en entretenant des réseaux, en distinguant ce qu'il faut diffuser de ce qui doit être préservé.

4. **Valoriser les informations en les sélectionnant,** en les validant et en les agençant afin d'optimiser leur exploitation.

5. **Placer les hommes au cœur du dispositif.** Les outils informatiques, les systèmes de surveillance automatisés ne remplaceront jamais (totalement) le génie humain. L'intelligence économique est d'abord un état d'esprit.

6. **Avoir une déontologie.** Respecter une éthique et se conformer au droit permettent de travailler sereinement et de durer dans son métier.

7. **Adopter un comportement ni naïf, ni paranoïaque.** Savoir que toute entreprise à des informations qui doivent être protégées et des partenaires auxquels elle peut faire confiance.

8. **S'adapter et cultiver les soutiens.** Les connaissances, outils, réseaux utilisés pour maîtriser l'information, la communication, l'influence, évoluent rapidement. Si nécessaire, faire appel à des compétences extérieures de confiance pour pouvoir y répondre ou pour accroître son efficacité.

9. **Etre attentif** pour contrer les menaces, saisir les opportunités, évaluer les rapports de force, accompagner les changements et nourrir sa créativité.

10. **Refuser l'inévitable et envisager l'inattendu.**

3 La sécurité de l'information

Parce que toutes les entreprises ont des informations intéressantes, un concurrent peu scrupuleux n'hésitera pas à :

- ***voler des supports informatiques,***

A la suite de son intervention dans une conférence, le dirigeant d'une grande société de télécommunications étrangère s'est fait dérober son ordinateur portable dernier cri utilisé pour son exposé.
D'après la presse, ce vol serait particulièrement embarrassant, non pour la valeur du matériel subtilisé, mais parce qu'il contenait plusieurs mégabytes de données confidentielles, notamment des informations privées sur l'histoire de la société, une base de données financières ou une messagerie remplie de contacts d'intérêt primordial.

- ***pénétrer le réseau informatique interne,***

Le salarié d'une entreprise utilise un modem qu'il laisse branché en permanence afin de tester épisodiquement la disponibilité d'un service Minitel *(encore)* offert par l'entreprise.
Un jour, il reçoit un message électronique d'un pirate informatique qui le remercie de lui avoir donné le moyen de pénétrer le réseau de l'entreprise en contournant le pare-feu installé qui représentait un obstacle particulièrement gênant.

- ***intercepter les communications,***

Une société française envoie par courriel sa réponse à l'appel d'offres d'une entreprise australienne. Elle reçoit quelques minutes après et avant la clôture du marché, l'accusé de réception demandé dans son message. Le lendemain, elle apprend que sa proposition est arrivée hors délais et que le marché a été remporté par un concurrent américain.

Après enquête, elle se rendra compte que son courriel a été détourné et que l'accusé de réception reçu était un faux. L'offre française a été séquestrée le temps nécessaire pour qu'elle n'arrive pas dans les délais impartis afin d'être prise en compte par l'acheteur australien.

- ***abuser vos employés, vos partenaires.***

Une nouvelle escroquerie connaît un succès grandissant sur internet : le "phishing" ou "hameçonnage".

Des internautes reçoivent un message électronique qu'ils croient provenir de leur banque. Celui-ci les invite à cliquer sur un lien afin de mettre à jour leurs données personnelles. Ainsi, ils sont redirigés vers un site web d'apparence identique à celui de leur établissement bancaire où un questionnaire leur demande de saisir leur identifiant, leur mot de passe, leur numéro de compte, de carte bancaire, etc.

S'assurer de l'identité de son interlocuteur, avant de communiquer des données sensibles par messagerie, est un réflexe à acquérir lorsque l'on échange des informations par l'intermédiaire de l'Internet.

Pour protéger leurs informations, de nombreuses entreprises appliquent des mesures de sécurité au fur et à mesure qu'apparaissent les problèmes. Pourtant, **une politique de sécurité de l'information est une démarche qui nécessite de la réflexion et de la cohérence.** Il s'agit d'assurer à la fois :

- **la disponibilité** des ressources et des informations ;
- **l'intégrité** des données ;
- **la confidentialité** des données ;

- **la preuve / traçabilité** des accès aux informations.

Le dispositif de l'entreprise doit être **global et itératif.** Il prend en compte **toutes les composantes** impliquées - personnes, supports, moyens, organisation - et il est compatible avec les autres volets de la sécurité – sécurité des personnes, des bâtiments, de la production, etc. -.
Pour obtenir cette cohérence, il faut :

⇨ **Connaître les menaces –** intrusions, sinistres, erreurs humaines, etc.- pesant sur les différentes composantes impliquées dans l'élaboration, l'utilisation, la diffusion, le traitement, la conservation et la destruction des informations utiles à l'entreprise.

⇨ **Identifier les vulnérabilités de l'entreprise,** celles relatives aux technologies mais aussi celles relatives aux différents facteurs humains, organisationnels ou physiques utilisés par l'entreprise.

⇨ **Définir des niveaux de risques acceptables,** en tenant compte, d'une part, de leurs conséquences, d'autre part, des coûts ou des contraintes nécessaires à leur réduction.

⇨ **Proportionner les solutions à la valeur des informations à protéger** - elles ont un coût acceptable pour l'entreprise, ne gênent pas ses capacités de communication, n'occasionnent pas de contraintes disproportionnées pour les utilisateurs, etc **-.**

⇨ **Arrêter les règles de classification de l'information** ainsi que les modalités de sa circulation, de son exploitation, de son stockage et de sa destruction.

⇨ **Responsabiliser les personnes** maniant des informations sensibles pour qu'elles assurent leur sécurité.

⇨ **Former toutes les parties prenantes –** personnel, partenaires, prestataires – afin qu'elles aient la capacité et la volonté de préserver les informations sensibles qui leur sont confiées.

⇨ **Gérer la sécurité,** notamment en analysant les incidents, en traitant rapidement les risques émergents, en s'adaptant aux évolutions des menaces, etc.

L'entreprise doit garder à l'esprit que :

- **Une protection absolue n'existe pas ;** néanmoins une sécurité ajustée permet de réparer beaucoup de maladresses, de décourager un nombre important d'attaques et de minimiser les conséquences d'erreurs ou d'agressions.
- Si des moyens techniques sont bien souvent nécessaires, **les solutions sont principalement organisationnelles et fonctionnelles,** elles nécessitent **du réalisme et du bon sens.**

4 Le système d'information

Sauf exception, à un moment de son cycle de vie - création, utilisation, diffusion, archivage - **l'information est dématérialisée** pour être transmise ou conservée à l'aide d'un support numérique.
C'est pourquoi, les entreprises ne peuvent pas aborder la sécurité de l'information sans se concentrer sur **leur environnement numérique composé :**

- **des postes de travail informatique et serveurs** (données, PABX, etc.) ;
- **des applications** (systèmes d'exploitation, suites bureautiques, logiciels métiers, etc.) ;
- **des infrastructures de communication et de télécommunication** (réseaux locaux, liaisons inter-sites, réseau téléphonique, accès Internet, liaison radio, etc.).

Aujourd'hui, les "formats de communication" se sont normalisés - notamment le protocole IP (*Internet Protocol*) support de transmission unique pour la voix, les données, les images -, les technologies sont arrivées à maturité, les prestataires maîtrisent les processus d'intégration.

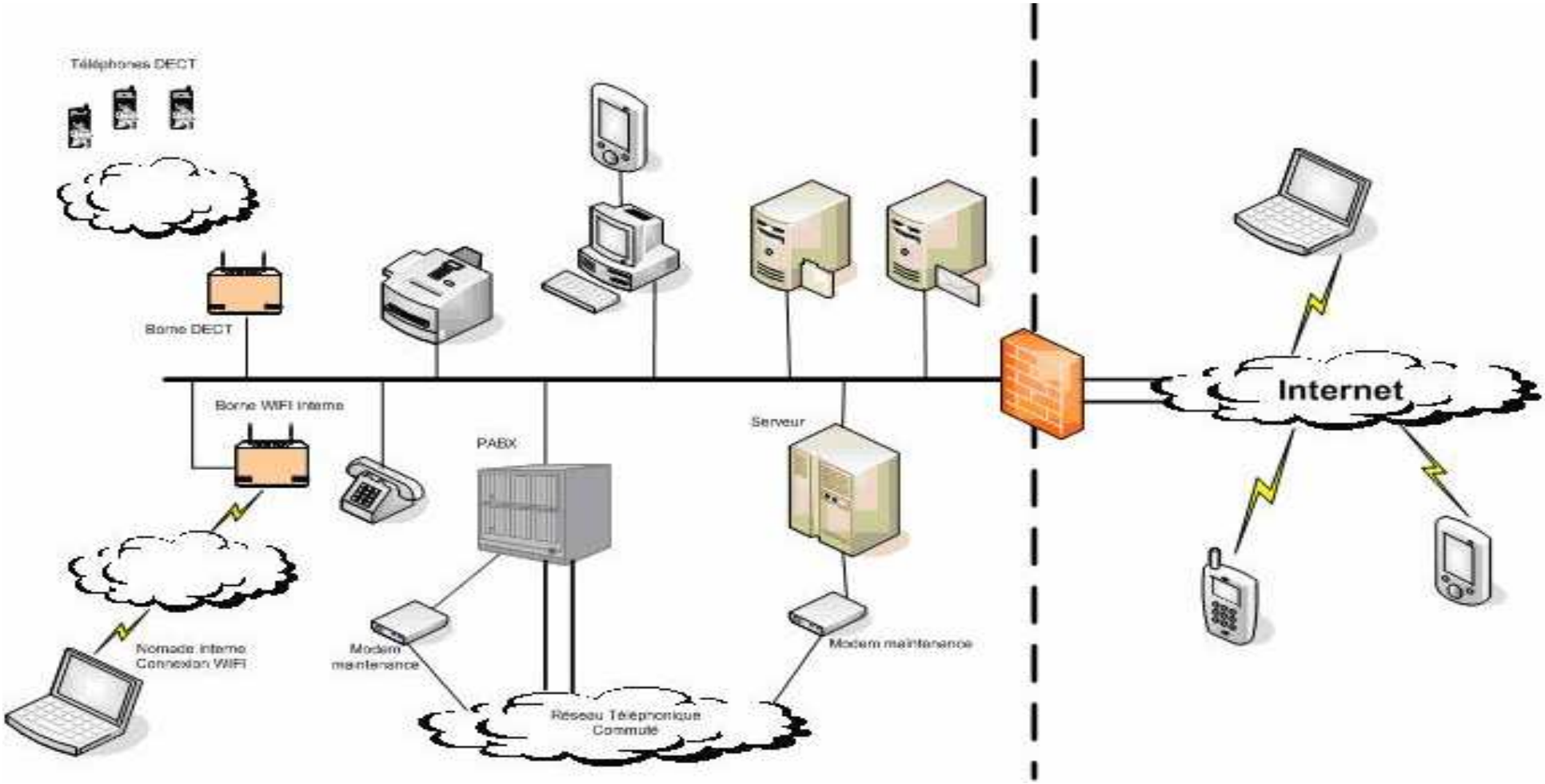
Pour accroître leur réactivité et leur efficacité, les entreprises ont :

- développé leur réseau d'information et de communication aussi bien en interne qu'en externe ;
- multiplié les possibilités de connexions vers d'autres réseaux ;
- déployé des solutions nomades.

Ainsi, assurer la protection de l'environnement numérique nécessite de :

- **Connaître l'ensemble des matériels installés ;**
- **Identifier tous les points d'accès au système d'information et de communication ;**
- **Couvrir un périmètre plus vaste que celui délimité par les locaux de l'entreprise.**

Schéma du système d'information dans une entreprise communicante



5 La sécurité du système d'information

Comme pour la protection de l'information, la sécurité du système d'information repose d'abord sur des éléments **organisationnels et fonctionnels,** les éléments **techniques venant en complément**. Pour que la sécurité du système d'information soit assurée au mieux, il faut :

- ⇨ **Nommer** une personne et son suppléant qui auront **en charge la responsabilité de la sécurité du système d'information (SSI)**.
- ⇨ Avoir des **politiques de gestion des ressources humaines et de fournisseurs et partenaires de confiance**, **cohérentes** avec le niveau de sécurité désiré pour le système d'information.
- ⇨ **Agir pour réduire les comportements à risques** – téléchargement de programme à partir d'Internet, ouverture sans discernement des messages électroniques, réponse à une sollicitation par messagerie concernant des informations confidentielles, etc.- par la formation, l'élaboration de documents précisant les règles d'utilisation des matériels ou engageant la responsabilité des utilisateurs, etc .
- ⇨ **Construire le réseau** et **paramétrer les matériels et logiciels (aussi)** en fonction des impératifs de sécurité pour que les mesures arrêtées n'offrent pas de possibilité de contournements.
- ⇨ **Ne retenir que des solutions maîtrisables** par les personnes en charge de la SSI qui doivent comprendre ce qu'elles font.
- ⇨ Réaliser un **inventaire des matériels et des logiciels** et tenir à jour des tableaux de correspondance avec les utilisateurs.
- ⇨ **Administrer le réseau** de l'entreprise en formalisant les procédures d'habilitation des utilisateurs – enregistrement, retrait – et en documentant les actions réalisées sur le système d'information – installation, restauration, traitement des incidents, test de validité-.
- ⇨ Disposer d'une **passerelle unique** vers l'Internet avec un **pare-feu** et une **sonde** de détection et de blocage des échanges de données suspects.
- ⇨ Installer des **logiciels de sécurité - antivirus, anti-spyware, anti-spam et anti-troyens** - sur tous les postes informatiques ainsi que sur les serveurs connectés au réseau.
- ⇨ Appliquer très régulièrement les **correctifs de sécurité** diffusés par les concepteurs de logiciels et **mettre à jour les bases de signatures** antivirus, anti-troyens des postes informatiques et des serveurs.
- ⇨ **Faire appel, si nécessaire, à un prestataire extérieur** qui saura apprécier la sécurité de votre système d'information, le configurer, l'administrer, le faire évoluer. *Les offres gratuites d'audit de sécurité à distance doivent être utilisées avec prudence.*
- ⇨ **Ne pas oublier la protection du dispositif de sauvegarde** des données.

6 Les informations confidentielles et le système d'information

Pour ses informations les plus sensibles, l'entreprise **durcira la protection appliquée au système d'information**. Elle assignera des mesures plus strictes à une partie de son environnement numérique et multipliera les lignes de défense afin de disposer d'**un système sécurisé en profondeur.** Par exemple :

- ⇨ Les données confidentielles seront t**raitées uniquement sur des postes de travail non connectés au réseau**.
- ⇨ Les données confidentielles **ne pourront pas être embarquées sur un ordinateur portable.**
- ⇨ Les données confidentielles seront **stockées sur des disques durs amovibles** mis dans une armoire forte ou un coffre entre deux utilisations.
- ⇨ En plus de l'identifiant et du mot de passe du terminal, les dossiers auront des **mots de passe différents, solides et renouvelés** régulièrement.
- ⇨ Les ordinateurs auront les **connecteurs USB désactivés et un dispositif d'identification à la mise en route** - carte à puce, biométrie, reconnaissance vocale, etc. -.
- ⇨ Les ordinateurs disposeront de logiciels de **détection d'erreurs ou d'intrusions.**
- ⇨ Les ordinateurs pourront, si nécessaire, être munis d'un **dispositif de contre-mesures aux interceptions par rayonnement, conduction ou captation des signaux** et installés dans des locaux à la sécurité renforcée.
- ⇨ **L'utilisation de la messagerie est déconseillée.** Si aucune autre solution n'existe, les échanges électroniques seront chiffrés avec des produits qualifiés.

*Pour plus d'informations, nous vous incitons **à consulter le recueil de fiches pratiques, établies par le CLUSIF sur le site :***

http://www.clusif.asso.fr/fr/production/ouvrages/fiches-micro/

Les fiches contiennent notamment des recommandations qui permettent de gérer la sécurité des postes utilisateurs.

*Le réseau des **Chambres de Commerce et d'Industrie** propose également aux dirigeants et décideurs de PME, **des présentations des impacts économiques, juridiques et techniques des cyber-risques.** Ces actions sont, suivant les régions, accompagnées de propositions de diagnostics et audits pouvant être pris en charge par des dispositifs publics de soutiens financiers aux entreprises.*

7 La situation des réseaux sans fils

Dans ce paragraphe, nous aborderons les réseaux Wi-Fi, sachant que la démarche adoptée par les attaquants et les recommandations pour la protection des données sont transposables aux technologies similaires de communication par ondes radio : satellite, GPRS, EDGE, UMTS.

De nombreuses entreprises sont équipées de réseaux sans fils - les réseaux Wi-Fi - permettant des transmissions radio à la norme 802.11.
Par rapport au câblage informatique d'un bâtiment, cette **technologie** est **peu onéreuse.** Permettant des déplacements libres dans le bâtiment sans avoir à brancher un câble, elle est particulièrement **pratique** pour accélérer les échanges.
Il serait dommage qu'elle soit pénalisante pour l'entreprise en raison d'une sécurité mal maîtrisée ou insuffisante.

Les systèmes sans fils font circuler « dans les airs » des informations et permettent à toute personne munie d'un ordinateur et d'une carte Wi-Fi de se raccrocher à un réseau situé dans leur environnement proche. Il est donc **facile de se connecter à un réseau Wi-FI** - et cela sans même le vouloir ou le savoir - et **d'intercepter des données** sans être physiquement présent dans les murs de l'entreprise.

La vulnérabilité des entreprises est renforcée par la diffusion sur des sites Internet, d'une cartographie précise des sociétés équipées de bornes d'accès Wi-Fi et leur niveau de protection.

De même, un ordinateur portable appartenant à une entreprise peut, après avoir été dérobé, donner accès à son réseau Wi-FI. Un vol d'ordinateur portable peut être commis uniquement dans ce but. **Quelques conseils** pour installer et utiliser un réseau sans fil :

- ⇨ **Positionner les points d'accès** et **régler leur puissance** suivant la zone à couvrir.
- ⇨ **Modifier les configurations et mots de passe** du constructeur, installés par défaut.
- ⇨ **Activer toutes les mesures de protection disponibles** (WPA au minimum) éventuellement en se référant aux notices et documents constructeurs.
- ⇨ **Mettre à jour les logiciels contenus dans les points d'accès et les cartes Wi-Fi** (firmwares ou microcodes) en les téléchargeant sur les sites web des constructeurs.
- ⇨ **Interdire le Wi-Fi pour l'accès aux informations sensibles** ou préalablement faire appel à un expert en sécurité des réseaux sans fils qui procédera à un audit et produira ses conseils.
- ⇨ **Déployer des outils de sécurité du type pare-feu** entre le réseau Wi-fi et le réseau local et gérer les comptes des utilisateurs et les droits d'accès associés.

8 Le plan de continuité des activités

Une **mauvaise manipulation**, volontaire ou involontaire, mettra à mal ponctuellement ou durablement le fonctionnement du système d'information.
Un **incendie, un dégât des eaux, une panne, un vol** portant sur le matériel informatique immobilisera tout ou partie de l'activité de l'entreprise.
Une **intrusion** dans le réseau permettra à une personne ou à un programme malveillant de modifier ou de supprimer des données ou des fonctions.
Compte tenu de **la diversité des menaces et de la multiplication des outils de communication connectés à son système d'information, aucune entreprise n'est à l'abri d'un sinistre informatique**. La faible sensibilité de son activité ou l'absence d'une forte pression concurrentielle ne sont pas des garanties contre des attaques extérieures, de nombreux "pirates" sont uniquement motivés par la réalisation d'exploits à partir des failles informatiques.

L'entreprise aura donc intérêt à prévoir un dispositif de sauvegarde et une stratégie de reprise pour pallier tout dysfonctionnement de son système d'information.
La **détermination** et la **mise en œuvre du plan de continuité des activités** se déroulent traditionnellement de façon séquentielle, suivant quatre étapes :

1 ► **L'analyse des besoins et des risques** - identification des enjeux, évaluation des impacts, étude de l'existant sur les plans techniques, fonctionnels et organisationnels -.

2 ► La définition de **la stratégie de continuité** des activités.

3 ► Le déploiement des **solutions retenues**.

4 ► La mise en place de **tests** et d'une **maintenance.**

Pour garantir une reprise rapide de l'activité en cas de sinistre, le **plan de continuité des activités** de l'entreprise abordera :

- ⇨ La fréquence de **sauvegarde** des données informatiques, les **modalités de transferts** et la **qualité des informations enregistrées**.
- ⇨ Les **conditions de stockage** des données sauvegardées – volume disponible, éloignement du système d'information de base, **facilité et rapidité d'accès** -.
- ⇨ Les **moyens de télécommunication** (voix et données) offerts par le **site d'accueil**.
- ⇨ Les **ressources humaines** mobilisables en support des équipes internes ou en substitution.
- ⇨ Le **matériel de remplacement** et son délai de disponibilité.
- ⇨ La définition d'une **cellule de gestion de crise**.

*Vous pouvez télécharger le dossier « **Plan de Continuité d'Activité – Stratégie et solution de secours du SI** » de la commission technique de sécurité logique du **CLUSIF**, à l'adresse :*
http://www.clusif.asso.fr/fr/production/ouvrages/pdf/PlanContinuiteActivite.pdf

9 Protéger l'environnement du système d'information

Les menaces et vulnérabilités issues des connexions aux réseaux ne représentent qu'une partie des risques pesant sur le système d'information.
Une personne malveillante ayant accès à un ordinateur peut aisément brancher une clé mémoire USB, voire un baladeur MP3, ou introduire une disquette pour récupérer, en un temps très court, des fichiers informatiques. Elle peut installer un logiciel (chevaux de Troie, logiciel espion) ou un matériel discret (de type *keylogger*) permettant de connaître sur la durée, l'activité d'un poste informatique.

Pour se protéger, le plus simple reste encore de limiter l'accès physique aux ordinateurs. En conséquence :

- ⇨ **Identifier les zones nécessitant une sécurité renforcée et mettre en place des systèmes de surveillance** – caméras, détecteurs d'intrusion – et de contrôle d'accès – badges, sas, personnel d'accueil – ainsi que des plans d'intervention et de gestion des incidents spécifiques à ces "lieux sensibles".

- ⇨ **Verrouiller les postes de travail à l'aide d'un mot de passe complexe –** combinaison de lettres, chiffres et autres caractères -, changé régulièrement, mémorisé par des utilisateurs sensibilisés aux techniques des personnes mal intentionnées – ingénierie sociale, phishing -.

- ⇨ **Configurer les ordinateurs afin qu'ils ne démarrent pas à partir d'une disquette d'un cédérom ou d'une clé USB** et qu'ils se mettent **en veille** avec un redémarrage par mot de passe.

- ⇨ **Fermer à clé la porte d'un bureau** lorsque personne ne s'y trouve.

- ⇨ **Conserver les doubles des clés des bureaux, des clés de chiffrement et des mots de passe dans des lieux fiables et protégés.**

- ⇨ **Etablir des règles pour les visiteurs –** stagiaires, clients, fournisseurs, presse, etc – par exemple, port d'un badge, interdiction d'introduire un téléphone portable, un lecteur MP3, une clé USB, un ordinateur portable dans les zones "sensibles" ou lors de réunion "confidentielles", accompagnement systématique du visiteur à partir de l'entrée, etc.

- ⇨ **Prendre en compte la dimension "sécurité" dans le choix des prestataires de services** intervenant dans les locaux - nettoyage, gardiennage, maintenance informatique et téléphonique, des photocopieurs, etc. **- et définir des clauses de confidentialité dans l'élaboration des contrats** passés avec ces derniers.

- ⇨ **Responsabiliser et éduquer le personnel** pour qu'il connaisse, suive et fasse respecter l'ensemble des mesures de sécurité physique de l'entreprise.

10 Encadrer la mobilité du travail

Disposer d'informations et d'outils de traitements lors de déplacements est souvent indispensable. Mais lorsqu'un collaborateur quitte l'entreprise avec un ordinateur portable, il faut qu'il soit particulièrement vigilant. Outre sa valeur, les informations qu'il contient peuvent en faire un objet particulièrement attractif pour des voleurs.
Il est également facile de copier le contenu du disque dur si l'on se sépare, même quelques minutes, de son ordinateur portable ou d'en surveiller l'utilisation dans un lieu public.

- Pour diminuer les risques de vol ou de copie :

⇨ **Garder votre ordinateur portable près de vous** – éviter la soute lors de déplacements aériens, les vestiaires des restaurants, etc-.

⇨ **Equiper votre ordinateur d'un cadenas et/ou d'une alarme.**

⇨ **Choisir une sacoche "informatique" qui n'attire pas l'attention.**

- Pour réduire les conséquences d'un vol :

⇨ **Nettoyer, entre "deux sorties", votre machine des données non-indispensables,** en utilisant un logiciel spécialisé dans la destruction complète des données numériques.

⇨ **Bloquer son démarrage à l'aide d'un mot de passe solide.**

⇨ **Chiffrer le disque dur**.

⇨ **Détruire tous les fichiers temporaires** avant d'éteindre l'ordinateur, éventuellement automatiser cette fonction avec un logiciel spécialisé.

⇨ **Transporter vos données sur des supports amovibles –** cédérom, clé USB – qui ne seront pas conservés avec l'ordinateur.

- Lors de son utilisation :

⇨ **Interdire le téléchargement de programmes.**

⇨ **Respecter la plus grande prudence vis-à-vis des utilisations en mode Wi-fi ou WiMax.**

⇨ **Mettre à jour les correctifs de sécurité avant de le reconnecter sur le réseau de l'entreprise.**

- Lors d'une utilisation dans un lieu public (train, salle d'attente, café, etc.) :

⇨ **Travailler uniquement sur des documents non confidentiels**.

⇨ **Utiliser des filtres** rendant l'écran opaque pour vos voisins.

⇨ **Désactiver tous les moyens de communication offerts par votre ordinateur portable** – ports infrarouges, Wi-fi, Bluetooth, etc-.

- Lors d'une connexion avec le réseau de l'entreprise :

⇨ Créer un « **sas de sécurité** » pour **décontaminer et transférer les données** du portable qui revient de déplacement.

⇨ Disposer d'une **authentification forte de l'utilisateur** au moment de sa connexion à distance.

⇨ Opter pour **une sécurisation de la transmission des données.**

La plupart des préconisations mentionnées peuvent s'appliquer à l'ensemble des terminaux mobiles (PDA, SmartPhone, etc.).

11 Maîtriser la diffusion de ses informations

La communication de l'entreprise n'est pas exclusivement électronique et de nombreuses personnes - les dirigeants, les commerciaux, le personnel en relation avec des prestataires de service, avec l'administration – diffusent, de façon formelle ou informelle, des informations.
Des échanges dans des lieux publics ou privés, des interventions lors de colloques, des sollicitations à titre personnelles - **« idéologie, sexe, argent, orgueil »** - , des réponses à des questionnaires, à des appels d'offres, à des interviews, sont autant d'occasions d'exposer des connaissances n'ayant pas vocation à être rendues publiques ou de donner une mauvaise image de l'entreprise en raison de prestations inadéquates.
Les technologies numériques de l'information et de la communication ont l'inconvénient d'augmenter ces menaces et d'introduire de nouvelles vulnérabilités. Par exemple, l'entreprise doit savoir que :

- ***l'utilisation de ces technologies laisse des traces,***

Un site Internet propose un accès gratuit aux bases mondiales de brevets.
Le travail de recherche d'antériorité s'en trouve simplifié pour les entreprises souhaitant protéger leurs inventions. Cela permet aussi à l'entreprise informatique à l'origine de ce site, de repérer les grandes tendances technologiques se dégageant des requêtes et d'observer directement le comportement de ses concurrents.

- ***les fonctionnalités des outils associés à ces technologies ne sont pas toujours connues par l'ensemble des utilisateurs,***

L'association des diplômés d'une école de commerce envoie un courrier électronique à toute une promotion, sans utiliser la fonction "copies cachées" permettant de dissimuler les adresses électroniques des autres destinataires lors d'un envoi multiple. Quelques jours après, une société de recrutement, employeur de l'un des ex-élèves, utilisera la liste de diffusion de l'association pour contacter l'ensemble de la promotion.
Plusieurs diplômés apprécieront modérément cette récupération de données personnelles et une proposition de débauchage arrivant directement dans leur boîte aux lettres électronique professionnelle.

- ***ces technologies amplifient la vitesse et le périmètre de diffusion des informations,***

Suite à une erreur de saisie, un magasin à l'enseigne d'un corsaire, afficha sur son site de vente en ligne un agenda électronique (PDA) à 269 € au lieu de 699 €, prix normalement conseillé. En quelques heures, plusieurs centaines d'internautes seront séduits par cette offre particulièrement avantageuse.
Rapidement, le site rectifiera son erreur, néanmoins il aura aussi dû livrer 150 PDA au premier prix annoncé. *(Ce nombre correspond au stock disponible au moment de la mise en ligne initiale de l'annonce).*

- ***la démultiplication des canaux de diffusion de l'information accroît les risques de brouillage ou d'erreur.***

Un producteur de boisson à bulles d'Atlanta souhaite reprendre un concurrent français, créateur d'une célèbre petite bouteille ronde. Il remet aux autorités françaises de régulation de la concurrence un dossier montrant que cette acquisition ne lui donnera pas une position dominante sur le marché des sodas.
Malheureusement pour lui, certaines données mentionnées dans le dossier ne correspondent pas à celles figurant sur le site Web américain de l'industriel d'Atlanta.
Les informations inopportunes seront promptement retirées du site Web, mais trop tard, les autorités françaises en ont pris connaissance. L'offre de reprise n'est plus crédible, elle sera rejetée.

Naviguer sur Internet, envoyer des messages électroniques, intervenir sur des forums, informer grâce à son site Web, sont des activités indispensables pour l'entreprise souhaitant se développer, identifier les menaces et les opportunités, anticiper les changements.

Afin que l'utilisation des outils de communication numériques ne se retourne pas contre elle, l'entreprise devra réduire les comportements à risques de son personnel et de ses principaux partenaires. Pour cela, il lui faudra :

- ⇨ **Apprécier leur capacité et leur volonté de préserver les informations** qu'elle leur confie.
- ⇨ **Elaborer des règles (*)** – inscription dans les contrats de travail d'engagements de confidentialité absolue par rapport à certaines informations, modalités de réponses aux diverses sollicitations extérieures, charte informatique interdisant les téléchargements, les interventions dans les forums, formulant des restrictions concernant l'envoi de pièces jointes aux messages électroniques, etc-.
- ⇨ **Sensibiliser** pour que tous comprennent que la communication et la sécurité des informations sont étroitement imbriquées et qu'ils acceptent les mesures imposées par la nécessité de protéger certaines d'entre elles.
- ⇨ **Déployer des moyens de sécurité**, matériels et logiciels, adaptés aux échanges entre le système d'information et les réseaux extérieurs – serveur mandataire, pare-feu, antivirus, dispositif de chiffrement, réseau privé virtuel, etc – et les **mettre régulièrement à jour**.
- ⇨ **Former** à la maîtrise des outils de communication et des dispositifs de sécurité associés.

(*) Actuellement, la loi n'apporte pas de réponse explicite aux litiges liés au secret des correspondances électroniques. Les décisions des tribunaux cherchent à définir un équilibre entre le respect de la vie privée et les obligations professionnelles.
***Un employeur ne peut lire que les messages professionnels**. C'est-à-dire qu'il doit respecter la confidentialité des messages personnels même si :*

- *le salarié utilise le matériel de son entreprise,*
- *le message transite par une adresse électronique générique de l'entreprise,*
- *l'entreprise interdit les utilisations à des fins purement personnelles.*

*L'entreprise doit adopter une attitude prudente dans le **contrôle des messages électroniques** transmis ou reçus par ses employés. Elle aura intérêt à mettre en place une **charte informatique définissant des règles** comme l'usage modéré des messages non professionnels, la création de dossiers "privés" et "professionnels" ou l'introduction de signes permettant d'identifier le caractère des messages sans avoir besoin de les ouvrir.*

12 Surveiller la circulation des informations

Si maîtriser l'information c'est protéger ses informations contre le vol ou les diffusions inopportunes, c'est aussi connaître et essayer de contrôler celles que d'autres propagent sur vous et cela sans vous en avertir. Qu'ils s'agissent :

- ***de manœuvres volontaires de déstabilisation initiées par un concurrent,***

  Un distributeur américain de bouteilles de vodka a créé un site Web uniquement pour discréditer son fournisseur français. Les fausses informations du site seront reprises dans la presse écrite et, en quelques mois, le cours de l'action de la société française passera de 220 à 9 euros.
  Après une longue procédure judiciaire et plus de trois millions d'euros de frais d'avocat pour l'entreprise française, le distributeur américain sera condamné. Cette décision n'empêchera pas l'agresseur de racheter sa victime, moralement touchée et financièrement exsangue.

- ***de parasitismes liés au fonctionnement des technologies de l'information,***

  Pour faire référencer et classer leur site Internet par les moteurs de recherche, les webmestres utilisent des mots clés (métatags) invisibles pour les internautes. En introduisant sur son site des métatags au nom d'un concurrent, une entreprise apparaîtra lors de requêtes réalisées sur le nom de ce concurrent.

  Ce parasitisme est condamnable en France, mais combien d'entreprises en connaissent l'existence ?

- ***de canulars aux conséquences destructrices,***

  Pour s'amuser, un internaute a mis en ligne sur le Web un petit film amateur montrant comment ouvrir un cadenas avec un stylobille. Sur la vidéo apparaissait distinctement la marque du cadenas. Sans se poser la question d'un éventuel montage, la presse fit état de ce film, évoquant un défaut de conception du cadenas.
  Cette mauvaise publicité fut suffisante pour obliger le fabriquant à arrêter la production du modèle incriminé.

- ***d'erreurs matérielles, par exemple lors de la retranscription d'information.***

  Une PME française, spécialisée dans les systèmes d'analyse et de conversion de protocoles télécoms, publie, en 2000, des comptes excellents. Pourtant certains fournisseurs demandent à être payés avant livraison et des affaires sont perdues de façon inexplicable. Tout s'éclairera lorsqu'un client indiquera au PDG de la PME que sa société est considérée comme étant en quasi-dépôt de bilan dans la base de données d'une des principales sociétés d'informations financières. Malgré un préjudice estimé à plusieurs millions d'euros, la PME devra menacer le fournisseur d'informations de poursuites judiciaires pour qu'il daigne corriger les informations erronées de sa base de données.

Des informations, vraies ou fausses, circulent dans les forums, dans les blogs. Des sites parodiques, des messages électroniques ternissent la réputation d'entreprises ou de dirigeants. Simples canulars ou manifestations de personnes ou structures malveillantes, ces propos sont parfois repris par les médias traditionnels sans vérifications sérieuses. C'est pourquoi, les entreprises doivent surveiller l'apparition et la diffusion des informations qui la concernent afin d'agir dans les meilleurs délais.

Le détournement de noms de domaine peut aussi avoir des conséquences préjudiciables pour une entreprise - altération de l'image, détournement d'audience au profit d'un concurrent, restriction à la pénétration de marchés étrangers, impossibilité de développer un projet en utilisant le réseau Internet.

Si la désinformation – rumeurs, faux communiqués, manipulation de journalistes – ou le parasitisme ne sont pas une pratique nouvelle, le **réseau Internet et les messageries électroniques décuplent leur capacité et leur vitesse de propagation.**
En se matérialisant par des écrits ou des images, ces actes de malveillance ou simples "Hoax" acquièrent plus de crédibilité que la rumeur orale.
En étant numérisés, ils restent "en mémoire" et peuvent ressurgir plusieurs années après leur élaboration.

Pour réduire les manipulations d'informations qui sapent le moral du personnel et la confiance des partenaires, il est important de :

- ⇨ **Recouper les sources.** Dans sa recherche d'informations sur le réseau Internet, le veilleur est confronté en permanence à des rumeurs. Il lui appartient d'être prudent et systématiquement de chercher à **apprécier la fiabilité des informations.**

- ⇨ **Soigner sa réputation.** La rumeur aura plus de difficulté à s'établir et se développer face à une entreprise habituée à communiquer de façon claire et franche. Les relais d'opinion, la presse, les salariés reprendront moins les fausses nouvelles et seront plus enclins de la soutenir lors d'une campagne destinée à corriger une fausse information.

- ⇨ **Déposer les noms liés à sa dénomination sociale et à ses marques** dans les différentes extensions (.fr, .com, .biz, .eu).

- ⇨ **Surveiller les sites ayant des déclinaisons proches de ses noms de domaine -** similitudes phonétiques, noms mal orthographiés.

En résumé, la sécurité de l'information c'est :

1. **Admettre que l'on est virtuellement menacé et potentiellement vulnérable ;** cela n'arrive pas qu'aux autres.

2. **Identifier les informations qui doivent être protégées ;** toutes les entreprises en ont.

3. **Evaluer les risques afin d'établir un juste équilibre entre contraintes** – financières, organisationnelles, juridiques, etc. – **et protection** ; tout ne peut pas être protégé, tout ne mérite pas d'être protégé.

4. **Opter pour une démarche globale et cohérente ;** plutôt que pour un empilement de mesures particulières sans réflexion ni structuration de l'ensemble du dispositif.

5. **Accepter que certains risques se réalisent ;** les assurances et la justice sont des solutions à envisager.

6. **Avoir un système de sauvegarde et un plan de continuité ;** et les tester avant la catastrophe.

7. **Ne pas se limiter à protéger les informations dans l'entreprise ;** celles qui entrent, sortent, circulent autour de l'entreprise sont aussi des sources de vulnérabilité.

8. **Etre attentif et réactif ;** les mises à jour, l'inventivité des malveillants sont sans fin.

9. **Créer du consensus au sein du personnel, des partenaires ;** la protection est l'affaire de tous, la sécurité bénéficie à tous.

10. **Ne pas se contenter d'une posture défensive** ; plus on est curieux, plus on sera vigilant.

Annexe A - Les limites de l'intelligence économique

Pour décrypter les évolutions de ses concurrents, comprendre les changements ou peser sur son environnement, l'entreprise qui dispose d'un réseau de capteurs performants, qui a mis en place un système d'analyse des informations, qui sait partager les informations, n'aura pas besoin de recourir à des expédients n'ayant pas leur place dans une démarche d'intelligence économique.

Toutefois, avoir un comportement éthique, n'empêchera pas certains concurrents, certaines personnes mal intentionnées - salariés licenciés, fournisseurs éconduits, escrocs, etc. - d'utiliser des méthodes illicites. Les entreprises victimes de "délinquances économiques" ne doivent pas hésiter à contacter les services de police ou de gendarmerie compétents et à porter plainte.

- **L'accès aux secrets de ses concurrents.** Vouloir à tout prix disposer d'informations protégées peut conduire à recourir à des procédés illégaux, particulièrement risquées pour ceux qui si livrent et pour leurs commanditaires. De plus, les résultats obtenus sont souvent impossibles à mentionner - et donc à utiliser - et les sources invérifiables.

Le vol est la soustraction frauduleuse de la chose d'autrui - article 311-1 du code pénal.

Il est puni de **trois ans d'emprisonnement et de 45 000 € d'amende** - article 311-3 du Code pénal –*.Le vol d'information par reproduction, photocopie, exploitation de fichier informatique repose sur la combinaison du délit de "vol d'usage du support d'information" même temporaire et du délit de " détournement de confiance".*

Actuellement, une réflexion est en cours au niveau de l'Etat, afin de renforcer la législation sur le secret des affaires et mieux protéger les informations économiques sensibles des entreprises.

L'extorsion est le fait d'obtenir par violence, menace ou contrainte, notamment la révélation d'un secret ou la remise d'un bien quelconque. L'extorsion est punie de **sept ans d'emprisonnement et de 100 000 € d'amende** - article 312-1 du Code pénal -.

Le chantage est le fait d'obtenir, en menaçant de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération, notamment la révélation d'un secret ou la remise d'un bien quelconque. Le chantage est puni **de cinq ans d'emprisonnement et de 75 000 € d'amende** - article 312-10 du Code pénal -.

Les atteintes au secret des correspondances sont le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance. Ces actions sont punies d'**un an d'emprisonnement et de 45 000 € d'amende**.

Est puni de peines identiques, le fait commis de mauvaise foi d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions - article 226-15 du Code pénal -.

L'usurpation d'identité pour obtenir une information est assimilable à une escroquerie. Le fait, par l'usage d'un faux nom ou d'une fausse qualité, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge constitue **un délit puni de cinq ans d'emprisonnement et de 375 000 € d'amende** - article 313-1 du Code pénal –

Les peines sont portées à sept ans d'emprisonnement et à 750 000 € d'amende lorsque l'escroquerie est réalisée par une personne qui prend indûment la qualité d'une personne dépositaire de l'autorité publique ou chargée d'une mission de service public- article 313-2 du Code pénal -.

- **La désorganisation de ses concurrents.** Les manœuvres de désorganisation d'une entreprise peuvent également donner lieu à des poursuites en justice.

Les atteintes aux systèmes de traitement automatisé de données :

- Le fait **d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 000 € d'amende**. Lorsqu'il en est résulté, soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30 000 € d'amende - article 323-1 du Code pénal .
- Le fait **d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45 000 € d'amende** - article 323-2 du Code pénal -.
- Le fait **d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 € d'amende** - article 323-3 du Code pénal -.

La contrefaçon ne concerne pas uniquement les produits de luxe ou la copie illicite d'œuvres musicales ou cinématographiques. Toutes les entreprises ayant déposé une marque, un modèle ou un brevet peuvent en être victimes.
Les sanctions pénales prévues par le Code de la propriété intellectuelle (CPI) sont **une amende pouvant atteindre 150 000 € et une peine de prison de deux ans.** En cas de récidive, les peines encourues sont doublées - article L. 716-9 du CPI -.
Pour les contrefaçons de marque, le code des douanes prévoit la **confiscation des marchandises litigieuses, celle des moyens de transport et objets ayant servi à masquer la fraude, ainsi qu'une amende comprise entre une à deux fois la valeur de la marchandise de contrefaçon et un emprisonnement maximum de trois ans.**

La loi autorise également la fermeture, totale ou partielle de l'établissement ayant servi à commettre l'infraction et permet d'obtenir des dommages et intérêts en engageant une action civile.

Le dénigrement consiste à jeter le discrédit sur une personne ou une entreprise. L'utilisation de la liberté d'expression à dessein de nuire représente un usage préjudiciable pouvant constituer une attitude fautive au sens de l'article 1382 du Code civil..

La concurrence déloyale. Désorganiser un marché, tirer profit des efforts réalisés par une autre entreprise, tromper le public pour accroître sa clientèle, sont des actes de concurrence déloyale susceptibles d'engager la responsabilité civile (et parfois pénale) de leur auteur. Ils peuvent conduire aux versements de dommages et intérêts selon les articles 1382, 1383 et 1384 du Code civil.

Les actions en concurrence déloyale permettent à l'entreprise de se protéger, en dehors de toutes relations contractuelles, lorsqu'elle s'estime victime d'actes contraires aux usages et habitudes professionnels. Néanmoins, l'entreprise aura intérêt à renforcer la protection de ses informations par un aménagement approprié de ses contrats : clause de confidentialité dans ses contrats de travail, de partenariat, de sous-traitance, etc…

Ces différents exemples d'infractions montrent que l'entreprise n'est pas démunie pour combattre et faire réprimer les méthodes illégales mises en œuvre pour s'approprier son savoir ou perturber son fonctionnement.
De manière préventive, pour faciliter les actions en justice, l'entreprise aura intérêt à utiliser les différentes dispositions de protection offertes par le droit de la propriété intellectuelle et industrielle. Elle pourra également mettre en place des moyens contractuels vis-à-vis de ses employés, ses partenaires et ses visiteurs.

Annexe B - *Comment mettre en place une politique de sécurité de l'information ?*

Pour disposer d'une réelle protection de ses informations, il faut mettre en place une politique de sécurité de l'information couvrant un large périmètre. Les mesures prises concerneront tout le matériel et toutes les technologies contribuant à la circulation et au stockage de l'information, ainsi que les moyens de télécommunication.

La mise en place d'une politique de sécurité doit être instaurée sous l'impulsion de la Direction Générale de l'entreprise. Elle consiste à :

1 ► Etablir des règles, procédures et bonnes pratiques à mettre en œuvre.

2 ► Désigner les personnes en charge et les actions à entreprendre en cas de risques avérés.

3 ► Sensibiliser les utilisateurs aux menaces qui pèsent sur le système d'information.

4 ► Prendre les mesures nécessaires pour réduire ou assumer les risques.

La définition, l'application et le suivi des règles de sécurité doivent être conduits comme un véritable projet associant la direction de l'entreprise, les personnes en charges de la gestion des moyens informatiques et téléphoniques et les représentants des utilisateurs.
Les règles élaborées seront regroupées dans un document unique de référence. Certains de ces articles ou renvois pourront faire l'objet d'une insertion dans les contrats de travail et dans le règlement intérieur de l'entreprise, afin de lui donner un maximum d'impact.

Principales méthodes pour la mise en pratique

Pour mettre en place une politique de protection de l'information, il est possible de s'inspirer des modèles développés pour la protection des systèmes d'information.

A titre d'exemple et de façon non exhaustive, les principales méthodes sont :

- **MEHARI** (*MEthode Harmonisée d'Analyse de RIsques*), développée par le CLUSIF (*Club de la Sécurité de l'Information Français*) ;
  - http://www.clusif.asso.fr/fr/production/mehari/

- **EBIOS** (*Expression des Besoins et Identification des Objectifs de Sécurité*), développée par la DCSSI (*Direction Centrale de la Sécurité des Systèmes d'Information*) ;
  - http://www.ssi.gouv.fr/fr/confiance/ebios.html

- **CobiT** (*Control Objectives for Business & Related Technology*) de maîtrise et d'audit des systèmes d'information éditée par l'Information System Audit & Control Association (ISACA) ;
  - http://www.isaca.org

Les sujets à traiter

- **L'analyse des enjeux**
  - ⇨ **Identifier les informations sensibles**. Cela peut consister dans un premier temps à évaluer les répercussions financières dans les cas où une information est erronée, indisponible ou si elle passe à la concurrence.
  - ⇨ **Classer ses informations** en fonction de leur sensibilité.
  - ⇨ **Nommer une personne en charge** de la définition, de la mise en application et du suivi des règles et procédures en matière de sécurité. *Cette personne pourra se faire assistée par un conseil si nécessaire.*

- **Le recensement de l'existant.** Véritable « état des lieux », au cours de cette phase tous les éléments constitutifs du système d'information ou en interaction avec celui-ci sont recensés.

  A titre d'exemple, et de manière non exhaustive, figureront les éléments suivants :
  - ⇨ **L'infrastructure de communication,** locale et avec l'environnement extérieur, notamment le type de connexion (filaire ou sans fil),
  - ⇨ **Le matériel** : serveurs, postes de travail, ordinateurs portables, centrale de téléphonie, assistant personnel, téléphones mobiles avec un système d'exploitation embarqué, éléments actifs (switch, routeurs, …), éléments de sécurité (pare-feu), etc
  - ⇨ **L'ensemble des applications.**
  - ⇨ **La cartographie physique et logique du réseau :** architecture physique, diagramme des flux de données entre les différents matériels, etc.
  - ⇨ **La liste des utilisateurs** qui accèdent aux données et leur profil.

- **L'analyse des menaces, des vulnérabilités et des risques.** L'objectif de cette troisième étape est d'anticiper les risques pesant sur votre système d'information et de communication. Pour cela, il est préférable de procéder en trois temps :
  - ⇨ **Identifier les menaces potentielles.**
  - ⇨ **Répertorier les vulnérabilités** et leur potentialité ou probabilité d'apparition.
  - ⇨ **Estimer les impacts** si le risque était avéré et notamment les conséquences financières, directes ou indirectes, sur l'organisation.

- **La réduction des risques.** Cette étape s'articule autour de deux axes principaux :
  - ⇨ **Prendre les mesures nécessaires pour réduire ou assumer les risques préalablement identifiés.** Cela nécessite d'avoir une approche organisationnelle et technique. Ainsi les cadres dirigeants et les personnes en charge de domaines clé seront directement impliqués dans la définition des mesures de protection à mettre en place.
  - ⇨ **Communiquer auprès des collaborateurs** afin qu'ils adhèrent à la politique de sécurité et acceptent les éventuelles contraintes associées.

Annexe C - Fiches de réactivité

Que faut-il faire lorsqu'un ordinateur est infecté par un virus ?

Il y a de fortes chances pour qu'un ordinateur soit infecté par (au moins) un programme malveillant - virus ou cheval de Troie – si :

- Il est lent, il se bloque ou refuse de démarrer.
- Des fenêtres intempestives s'ouvrent au démarrage.
- Des messages d'erreurs, d'annonces de fermeture du système apparaissent sans raison.
- Des programmes sont apparus, sans avoir été installés par l'utilisateur.
- La page d'accueil de la connexion Internet a été modifiée ou ne peut plus être changée.
- La connexion Internet ne fonctionne plus ou s'établit de façon anormale.
- Des fichiers disparaissent, sont modifiés ou sont corrompus.

Les bons réflexes

L'utilisateur

⇨ Déconnecter la machine du réseau sans la mettre hors tension ni la redémarrer afin de ne pas provoquer de nouveaux dégâts et conserver un maximum d'éléments sur l'agression.

⇨ Prévenir rapidement la personne responsable de la sécurité informatique pour qu'elle s'assure qu'aucun autre poste du réseau n'est infecté.

Le responsable informatique - *Ces manipulations sont relativement délicates, une personne formée sera chargée de les réaliser ou elles seront confiées à un professionnel extérieur* -.

⇨ Faire une copie physique du disque dur infecté.

⇨ Rechercher l'origine de l'agression - analyse du trafic, des journaux d'événements -.

⇨ Localiser d'éventuelles autres compromissions sur le réseau de l'entreprise.

⇨ Evaluer les dommages.

⇨ Mettre en place la solution définie par le plan d'urgence, si elle existe.

Réparer :

réinstaller le système d'exploitation à partir d'une version saine,
appliquer les derniers correctifs de sécurité,
restaurer les données à partir d'une sauvegarde non compromise.

⇨ Changer l'ensemble des mots de passe.

Après

⇨ Porter plainte pour retrouver le responsable et couvrir votre responsabilité en cas de dégâts causés à partir de votre poste de travail.

Documenter l'attaque :

- vulnérabilité exploitée,
- matériels et logiciels concernés,
- conséquences pour l'entreprise,
- solutions mises en place.

⇨ Analyser la façon dont le problème a été géré.

⇨ Ajuster les protections techniques et organisationnelles.

Que faut-il faire pour utiliser sereinement le réseau Internet ?

Parce qu'il donne accès à une masse considérable de données, le réseau Internet est un formidable outil d'information et de communication. Il permet de vérifier des "bruits", de poser des questions dans des forums, de rafraîchir ou de conforter ses connaissances, de se faire connaître et de s'afficher.
Mais il ne faut pas oublier qu'Internet est aussi un moyen d'intoxication de vos appréciations, de surveillance de votre activité ou de pénétration de votre réseau informatique. Lorsque vous vous connectez à Internet vous devez adopter une attitude se situant entre la curiosité et la méfiance afin de profiter au mieux de cette source d'informations ou de communication sans vous exposer plus que nécessaire à des désagréments.

Internet est aussi le moyen de diffuser rapidement et massivement de l'information ciblée en utilisant l'envoi de courriers électroniques.
Sur Internet, un message utilise toujours le même itinéraire entre deux serveurs. Il ne changera de chemin qu'en cas de problème - panne d'un routeur, partie de réseau engorgée, etc.-. Avec quelques moyens techniques, vos communications électroniques peuvent donc être repérées, interceptées et/ou modifiées.

Les bons réflexes

- **Lors de vos recherches d'informations :**
  - ⇨ Garder votre jugement critique. La validité d'une information ne dépend ni de l'aspect du site qui la diffuse, ni de son positionnement dans les résultats d'un moteur de recherche.
  - ⇨ Utiliser pour vos interventions sur les forums de discussion ou les sites Internet, une adresse neutre dédiée à cet usage, plutôt que votre adresse professionnelle habituelle.
  - ⇨ N'oublier pas qu'il existe des "faux sites" destinés à la parodie, à la diffusion d'idéologie ou à l'escroquerie.
  - ⇨ Paramétrer votre navigateur pour bloquer les cookies, pour limiter l'historique et le volume des fichiers temporaires. Eventuellement, passer par un proxy anonyme qui servira d'intermédiaire afin de masquer votre identité.
  - ⇨ Supprimer régulièrement les cookies et les informations enregistrées dans l'historique et les fichiers temporaires et lancer régulièrement un logiciel de recherche et d'éradication des logiciels espions.
- **Lorsque vous utilisez votre messagerie électronique :**
  - ⇨ Bannir le réseau Internet pour transmettre des informations devant rester confidentielles.
  - ⇨ Préférer, pour vos pièces jointes, des logiciels dédiés à l'échange et à la visualisation des documents électroniques – type PDF -.
  - ⇨ Chiffrer et signer électroniquement vos messages sensibles.
  - ⇨ Faire confirmer par téléphone, avant de les prendre en compte, des informations ou des demandes qui vous semblent inhabituelles ou importantes.

Que faut-il faire contre une agression sur le réseau Internet ?

Un message repris par un forum de discussion, une information sur un site Internet, sur un blog équivaut à une publication par voie de presse. Si vous êtes victimes de fausses informations, de messages diffamatoires, le Tribunal de grande instance est compétent en matière d'action civile.

Pendant longtemps le principe du "premier arrivé, premier servi" s'est appliqué pour l'attribution des noms de domaine sur Internet. Cette règle a conduit à de nombreuses dérives et généré l'apparition de cybersquatteurs motivés par le chantage au rachat, le détournement de clientèles vers des concurrents ou la parodie de site. Le titulaire d'un nom de domaine n'étant pas propriétaire de celui-ci mais uniquement détenteur d'un droit d'usage, avoir obtenu l'enregistrement d'un site ne protège pas de poursuites pour contrefaçon, concurrence déloyale ou parasitisme.

Les bons réflexes

- **Face à une fausse information :**
  - ⇨ Enregistrer le texte en cause et, si possible, faire réaliser un constat d'huissier.
  - ⇨ Chercher à identifier, l'origine de cette action de déstabilisation – concurrent déloyal ou acte isolé de particulier, tentative d'escroquerie ou mauvaise plaisanterie - .
  - ⇨ Suivre la diffusion et les commentaires suscités pour apprécier si vous devez réagir.
  - ⇨ Contacter le webmestre du site ou le responsable du forum pour l'informer de la situation et bénéficier d'un droit de réponse.
  - ⇨ Occuper le terrain pour étouffer la désinformation en utilisant des moyens similaires à sa diffusion : réponses argumentées dans les forums, rubrique démontrant la contre-vérité sur votre site web, messages aux partenaires de l'entreprise.
  - ⇨ Eventuellement, déposer plainte afin qu'une enquête identifie l'auteur de la manipulation. *Les hébergeurs de sites et les fournisseurs d'accès à Internet ont l'obligation de conserver les informations permettant l'identification de personnes commettant des infractions.*
  - ⇨ Utiliser tous les moyens offerts par la justice pour faire interrompre la diffusion. *Une assignation en référé et une action civile permettent de faire cesser le trouble en urgence et de demander des dommages et intérêts dissuasifs.*
- **Face à un cybersquatteur :**
  - ⇨ Essayer d'obtenir la rétrocession du nom de domaine usurpé par la négociation.
  - ⇨ Solliciter le Centre d'arbitrage et de médiation de l'Organisation Mondiale de la Propriété Intellectuelle, pour trancher les litiges des noms de domaine en .com, .org. Cette possibilité ne s'applique pas encore aux noms de domaine géographiques (.fr, .be). *La procédure d'arbitrage n'est pas exclusive d'une action judiciaire classique.*
  - ⇨ Faire respecter ses droits avec le dépôt d'une plainte auprès du Tribunal de Grande Instance en cas d'échec de la négociation ou de préjudice important.
    - o Si le nom de domaine retenu est une marque, vous pouvez agir en contrefaçon.
    - o Si vous ne disposez pas d'un droit de propriété intellectuelle, vous pouvez invoquer la concurrence déloyale, le parasitisme commercial ou l'atteinte à l'image.
      Pour rendre sa décision, le tribunal regardera si :
      - ▪ *Le nom de domaine est identique ou suffisamment proche pour prêter à confusion avec une marque sur laquelle le requérant à des droits.*
      - ▪ *Le détenteur du nom de domaine a des droits ou des intérêts légitimes sur celui-ci.*
      - ▪ *Le nom de domaine enregistré est utilisé de mauvaise foi.*

Que faut-il faire en cas de crise ?

Certaines menaces sont imprévisibles ou difficiles à appréhender, d'autres trop onéreuses ou trop complexes pour être totalement enrayées. Ainsi, parallèlement à la mise en place d'une politique de sécurité cohérente et efficiente, l'entreprise aura intérêt à prévoir des plans de secours, à élaborer des dispositifs de reprise d'activité et à se préparer à affronter les situations de fragilité que sont les crises.

Les bons réflexes

- **Anticiper :**
  - ⇨ Connaître les points critiques de son activité, ceux dont le fonctionnement devra être prioritairement assuré.
  - ⇨ Compiler les informations indispensables pour résoudre rapidement une crise (annuaires de responsables, plans des lieux, moyens mobilisables, etc).
  - ⇨ Prévoir l'organisation pour la gestion de crises.
  - ⇨ Définir une boîte à outils pour être en mesure de prendre les premières "bonnes" décisions.
  - ⇨ Entretenir une image positive pour bénéficier d'un capital de sympathie.
  - ⇨ Simuler une crise pour connaître l'efficacité et la réactivité du dispositif.
- **Gérer :**
  - ⇨ S'appuyer sur une implication personnelle du chef d'entreprise pour :
    - inspirer un niveau de confiance élevé,
    - s'assurer que les solutions sont conformes à la culture et à la stratégie de l'entreprise,
    - conforter la légitimité de décisions inhabituelles ou innovantes.
  - ⇨ Créer une cellule de crise pour :
    - regrouper les informations et les compétences nécessaires à la prise des décisions, les outils et les indicateurs de suivi de la crise, les moyens de communications,
    - recueillir et traiter de façon coordonnée un maximum d'informations et adapter l'engagement de l'entreprise aux évolutions de la crise,
    - piloter efficacement les opérations : choix des actions concrètes et symboliques, synchronisation des moyens, maîtrise de la communication.
- **Communiquer :**
  - ⇨ Officialiser la parole de l'entreprise en reconnaissant la situation de crise.
  - ⇨ Répondre aux attentes en fournissant des éléments factuels exacts qui réduiront les risques d'interprétations, déformations et désinformations.
  - ⇨ S'assurer que les informations transmises sont comprises en établissant des contacts directs, en écoutant les réactions aux informations transmises.
  - ⇨ Adapter son discours au développement de la crise et de ses répercussions.
  - ⇨ Annoncer le retour à la normale et remercier ses soutiens.
  - ⇨ Rebondir - si cela est possible - en valorisant le comportement de la structure face à l'adversité.

Annexe D - Services officiels pour vous aider

La liste proposée est loin d'être exhaustive. Il existe à tous les niveaux - européen, national, local – de nombreuses structures publiques, professionnelles, syndicales, privées pouvant apporter des informations ou une aide afin de mieux maîtriser et protéger les informations utiles à votre entreprise.

- **A accéder aux informations économiques utiles**

Le réseau **Minéfi au service des entreprises (MSE)** est un service offert par le ministère de l'économie, des finances et de l'industrie aux entreprises, et en particulier aux PME. Il s'appuie sur un portail Internet - **http://www.entreprises.minefi.gouv.fr** - et des réseaux de correspondants appartenant aux différents services extérieurs du ministère en charge d'apporter des réponses aux questions posées par les entreprises.

Les principaux indicateurs, chiffres clés, études conjoncturelles et sectorielles, liens vers d'autres sources de référence du ministère de l'économie, des finances et de l'industrie sont disponibles sur : **http://www.minefi.gouv.fr/minefi/chiffres/index.htm**

Le portail des **chambres de commerce et d'industrie** : **http://www.cci.fr** permet d'accéder à des informations économiques par thèmes, par région.

L'Union des Chambres de Commerce et d'Industrie Françaises à l'Etranger regroupe et anime les 110 CCI Françaises à l'Etranger (CCIFE) dans plus de 75 pays : **http://www.uccife.org**

Ubifrance, l'agence française pour le développement international des entreprises, - **http://www.ubifrance.fr** - présente l'ensemble des produits et services du dispositif public d'appui au développement international. Elle expose les opportunités à l'international et aide les entreprises à les transformer en développement commercial.

- **A mettre en place ou développer un dispositif d'intelligence économique**

Le site du **Haut Responsable chargé de l'intelligence économique** - **www.intelligence-economique.gouv.fr**/ - est à la fois une vitrine pour l'intelligence économique pratiquée en France, un carrefour pour accéder directement à de multiples informations utiles et un tremplin renvoyant vers d'autres sites Internet spécialisés et d'autres sources d'informations pertinentes.

Le ministère de l'intérieur organise les différentes démarches d'intelligence économique soutenues par l'Etat en région. Un correspondant "intelligence économique" a été désigné au sein de chaque **préfecture de région**.

Les **chargés de mission défense économique** (CMDE), placés auprès des trésoriers-payeurs généraux de région, sont des spécialistes de l'intelligence économique. Dans le cadre des missions partenariales de la défense économique, ils peuvent apporter leurs connaissances aux entreprises et tout particulièrement aux plus petites d'entre elles. *Leurs coordonnées figurent dans les informations communiquées par chaque trésorerie générale de région sur le site MSE.*

Les **directions régionales de l'industrie, de la recherche et de l'environnement** (DRIRE) - **http://www.drire.gouv.fr** - peuvent renseigner et aider les entreprises industrielles dans leur pratique d'intelligence économique.

Le portail **http://www.portail-intelligence.com** des **Chambres de commerce et d'industrie** propose à toute entreprise française, quelque soit son activité ou son implantation géographique, d'accéder à un ensemble de services utiles contribuant à la réussite de sa démarche d'intelligence économique.

- **A protéger vos informations**

Les **Chambres de Commerce et d'Industrie** (CCI) - **http://www.cci.fr** - organisent des opérations pour sensibiliser les dirigeants de PME à la sécurité des systèmes d'information : enjeux économiques, juridiques et informationnels, mesures de protection/prévention, audits, diagnostics.

- **Les intrusions intempestives**

La Direction de la Surveillance du Territoire (DST) est un service de recherche du renseignement de sécurité disposant de pouvoirs de police judiciaire. L'une de ses missions est de protéger le patrimoine économique et scientifique français.
La DST est implantée en région et dispose de numéros de téléphone permettant aux entreprises de la contacter. Pour plus de renseignements : Téléphone : **01 49 27 49 27** ou **01 45 77 95 82**.

L'O.C.L.C.T.I.C. Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication anime et coordonne l'action des d'enquêteurs spécialisés en criminalité informatique (E.S.C.I.) répartis dans les dix-neuf Services Régionaux de Police Judiciaire.
Téléphone : **01 40 07 69 49,** contact : **oclctic@interieur.gouv.fr**

La Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information (BEFTI) apporte son concours aux enquêtes concernant des infractions commises au moyen d'outils informatiques. Téléphone : **01 40 79 67 50.**

Le département informatique-électronique de la division criminalistique de **l'Institut de Recherches Criminelles de la Gendarmerie Nationale** (IRCGN) s'occupe des affaires concernant l'informatique et l'Internet dont les escroqueries sur le Web, les intrusions dans les systèmes d'information, le piratage de logiciels, etc. Sur le territoire, chacune des trente sections de recherches (SR) de la gendarmerie dispose d'au moins un "gendarme-internet". Contact : **info@gendarmerie.defense.gouv.fr**

- **La propagation de virus**

L'une des missions de la **Direction Centrale de la Sécurité des Systèmes d'Information** (DCSSI) - **http://www.ssi.gouv.fr/fr/dcssi/index.html** – du Secrétariat général de la défense nationale, placé sous l'autorité du Premier ministre, est d'évaluer, d'alerter et de fournir des moyens pour prévenir des menaces pesant sur les systèmes d'information. La DCSSI dispose du centre opérationnel de la SSI (COSSI), en veille 24 heures sur 24, tous les jours de l'année.

Le **CERT-IST** : Computer Emergency Response Team - Industrie, Commerce, Tertiaire - **http://www.cert-ist.com** - est une association loi 1901, qui a pour vocation d'assurer à ses adhérents des services de prévention des risques et d'assistance au traitement d'incidents. Le Cert-IST est un centre d'alerte et de réaction aux attaques informatiques pour les entreprises françaises.

Le **Club de la sécurité de l'information français (CLUSIF)** est une association dans laquelle les acteurs de la sécurité des systèmes d'information, issus de tous les secteurs d'activité de l'économie, se rencontrent et mettent en commun leurs réflexions. A ce jour, le CLUSIF rassemble plus de 600 membres, aussi bien des utilisateurs que des offreurs. Son site est le **http://www.clusif.asso.fr.**

- **La contrefaçon**

Conformément aux accords de l'Organisation mondiale des douanes (OMD) et à la réglementation communautaire, les agents des **Douanes - http://www.douane.gouv.fr** - disposent du pouvoir de retenir aux frontières, les marchandises contrefaisant les droits des sociétés (droits d'auteur et droits voisins, dessins et modèles, marques, brevets) ayant sollicité leur intervention.

La Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF) - http://www.finances.gouv.fr/DGCCRF **- participe avec les autres services compétents de l'Etat (police, gendarmerie, douanes) à la lutte contre les contrefaçons sur l'ensemble du territoire.**