



Cette fiche pratique vous est présentée par

**SHFD**

Le service du Haut Fonctionnaire de la Défense

## Intelligence économique stratégique et protection des données de l'entreprise



Si l'intelligence économique est une pratique ancienne, elle a été érigée en 2004 en véritable politique publique par le Gouvernement à la suite de la parution - mi 2003 - du Rapport « Intelligence économique, compétitivité, et cohésion sociale » rédigé, à la demande du gouvernement, par le député Bernard CARAYON, et se traduit notamment par la nomination d'un Haut Responsable de l'Intelligence Economique en janvier 2004.



En 30 ans, les entreprises sont passées d'une culture dominée par la technique à une culture de la connaissance. Aujourd'hui **une entreprise doit s'organiser pour obtenir de l'information, la faire circuler et lui donner du sens afin d'anticiper les évolutions et de les transformer en avantage concurrentiel décisif.**



Dans un contexte où la mondialisation a accru la concurrence et où l'explosion des technologies a modifié la création de la valeur, l'information est devenue un élément stratégique de l'entreprise. Ainsi pour définir sa stratégie commerciale, l'entreprise doit non seulement acquérir une bonne connaissance de ses clients, mais aussi s'intéresser à : ses concurrents, ses fournisseurs, ses circuits de distributions, aux évolutions technologiques, réglementaires ou normatives de son secteur d'activité ainsi que de ses activités connexes, ...



**Parallèlement l'entreprise doit protéger sa propre information c'est-à-dire son patrimoine.** Elle ne peut plus ignorer que ses brevets, ses marques, ses savoir-faire, son image, ses partenariats, la valeur de ses collaborateurs, son modèle d'organisation, de développement, ses projets stratégiques, représentent une part importante de la valorisation de son actif.



L'utilisation massive et diversifiée des moyens de communication, l'organisation en réseau qui se généralise, l'externalisation de fonctions (logistique, informatique, comptabilité, etc...) sont autant d'opportunités d'intrusion dans l'entreprise et de captation de son savoir.

**Une démarche d'intelligence économique menée par une entreprise comprend donc deux volets :**

- d'une part, l'acquisition de l'information via une Stratégie d'Intelligence Economique ;
- d'autre part, la protection de son patrimoine notamment par la Sécurisation de son Système d'information en tant qu'outil de stockage, de transmission des éléments de son patrimoine informationnel.



### Stratégie d'intelligence économique

L'intelligence économique peut se définir comme la maîtrise de l'information stratégique.



L'IE est ainsi l'outil qui permet à un acteur économique d'être plus compétitif que ses concurrents grâce à une stratégie globale et des décisions éclairées par les bonnes informations au bon moment.

Les enjeux d'une stratégie d'intelligence économique pour l'entreprise sont de saisir les retombées positives que l'information génère, que ce soit lorsqu'elle permet d'anticiper les menaces (arrivée de nouveaux concurrents, évolution de la réglementation, identification d'une rumeur la concernant, etc) ou d'orienter son développement (demande de nouveaux produits ou services, identification de nouveaux partenaires, conquête de nouveaux marchés, obtention d'un avantage compétitif, etc).

**SHFD**

**La maîtrise de l'information nécessite que coexistent, au sein de l'entreprise, une culture de partage et de protection - vis-à-vis de l'extérieur - des informations.**



Ainsi une stratégie d'intelligence économique reposera à la fois sur la mobilisation et l'implication des salariés de l'entreprise et sur l'animation de réseaux internes et externes et sur un dispositif de veille (cellule d'intelligence économique, chargé de mission, structure extérieure) capable :

- d'extraire les bonnes informations: c'est à dire de discerner, dans la masse des informations disponibles internes et externes, ce qui est essentiel et stratégique.
- de les valoriser : c'est à dire de combiner les informations essentielles pour identifier les opportunités (évolution de ses marchés, développement de partenariats, amélioration de son image, etc ) et les menaces (arrivée de nouveaux produits, de concurrents, évolution des réglementations, de la normalisation, campagnes de désinformation, divulgation d'informations sur son activité, sa stratégie, etc) ;
- d'orienter leur diffusion : c'est à dire de transmettre la bonne information, à la bonne personne, au bon moment.

#### Rôle d'une cellule IE ou cellule de veille :

En tant qu'outil d'aide à la décision dans le cadre d'une stratégie commerciale ou plus globalement de protection ou de développement de l'entreprise, elle apportera les prestations et les produits suivants : des informations brutes, des informations élaborées, l'accès à l'information, la diffusion sélective d'informations, la capitalisation des connaissances.

La cellule peut également réaliser des dossiers thématiques (par produits, par pays ou par domaines), proposer une synthèse de presse (hebdo, mensuelle, annuelle), préparer les missions des employés de l'entreprise (il est important d'utiliser les missions aussi comme des sources d'informations), couvrir les salons professionnels (cf. l'élaboration d'un plan d'actions).

Il appartient aux cellules d'intelligence économique d'être à l'écoute de la moindre menace, d'anticiper la détérioration d'une image, de contre-attaquer dès qu'une fausse information circule et de sensibiliser les dirigeants et les collaborateurs à la nécessité du partage et de la gestion de l'information.

Afin de lui permettre de toucher l'ensemble de l'entreprise, d'entretenir sa réactivité, d'exploiter efficacement ses recherches, il est recommandé de placer la cellule sous l'autorité directe du responsable de l'entreprise.

**Exemple de stratégie intelligence économique :** Société S. – Société d'ingénierie de haute technologie comprenant 500 salariés. Son activité est la conception et l'accompagnement des grands projets industriels (AIRBUS, fusée ARIANE, SNCF ...).

L'objectif de la démarche IE : La recherche d'informations concerne aussi bien les marchés que les technologies. L'objectif de l'entreprise est en effet de mieux cerner les besoins de ses clients et de proposer des produits qui intègrent les dernières innovations. La Société S. souhaite aujourd'hui renforcer la veille vers les nouveaux métiers ce qui permettrait d'accroître son développement.

Cette Société a mis en place une démarche d'IE impliquant tous les départements de l'entreprise. Le président de cette Société jugeant que les métiers deviennent de plus en plus complexes, a en effet estimé plus efficace de confier la veille à chaque département en fonction de ses compétences et de responsabiliser ainsi l'ensemble des collaborateurs de la Société.

#### Conseils aux entreprises :

© Une stratégie d'intelligence économique suppose une organisation et une culture d'entreprise facilitant la circulation d'informations dans le cadre d'un travail en réseau rénovant le fonctionnement hiérarchique classique.

Il est recommandé de mobiliser l'ensemble des salariés et de les encourager à participer à la démarche en rendant compte et en faisant circuler, dans l'entreprise, l'information obtenue lors notamment d'un déplacement, d'une réunion ou d'un contact téléphonique.

*Par exemple, vous voulez pénétrer un marché étranger :*

- . *identifiez les sujets à traiter (concurrence, réglementation, habitudes de consommation, circuit de distribution, etc) ;*
- . *définissez les informations qui doivent rester confidentielles et prenez des mesures pour les protéger ;*
- . *mobilisez l'ensemble de vos salariés, certains on peut-être des connaissances sur ce marché (parce qu'ils y ont travaillé, séjourné, parce qu'ils connaissent quelqu'un qui ...(effet réseau), parce qu'ils se passionnent pour la culture de ce pays, etc...*
- . *diversifiez vos sources d'informations et les recouper*
- . *faites (éventuellement) appel à des spécialistes*
- . *analysez les expériences similaires, identifiez (en amont) les structures d'appui possibles, etc....*



© L'exploitation d'informations provenant du réseau Internet peut constituer une vulnérabilité pour l'entreprise. L'utilisation de moteurs de recherche, la consultation de sites laissent des traces par exemple qui peuvent renseigner sur les domaines d'intérêts de l'entreprise ses concurrents ou bien des personnes malveillantes. Ainsi, une recherche d'informations peut se retourner contre l'entreprise.

Il est donc recommandé aux entreprises d'éviter de se connecter toujours aux mêmes serveurs, aux mêmes sources (Google, Altavista, wanadoo...), sachant que l'information proposée aura très souvent un point de vue partiel en étant par exemple influencée par l'origine du moteur, et, au contraire de confronter les informations obtenues de sources différentes. Internet restant une vaste zone d'informations, de désinformation et de rumeurs.

Une formation aux techniques de recherche d'informations, voire le recours à des professionnels (veilleurs, courtiers en informations, ...), sont fortement conseillés pour des recherches complexes ou concurrentielles.

## La sécurisation des systèmes d'information

On entend par **système d'information** d'une entreprise tout moyen dont le fonctionnement fait appel à l'électricité et qui est destiné à élaborer, traiter, stocker, acheminer, présenter et détruire l'information. Il s'agit notamment des Systèmes informatiques (intranet), de l'Internet (le site Web), et des Systèmes de télécommunications (postes téléphoniques, standard PABX, fax), y compris les photocopieurs numériques qui font aussi fax.

**Les systèmes d'information détiennent maintenant l'essentiel du patrimoine immatériel de l'entreprise : les dessins et modèles, le fichier du personnel, les contrats, les prospectus, les plans stratégiques de l'entreprise, les fichiers clients, etc ... les systèmes d'information deviennent donc des cibles privilégiées !**

Il existe en effet toutes sortes d'attaques possibles via le système d'information de l'entreprise, telles que l'attaque virale via la messagerie (activation d'un virus dans une pièce jointe), le détournement d'une ligne téléphonique via un PABX, le sabotage du site Internet de l'entreprises via la navigation sur Internet, la prise de contrôle du système informatique à l'insu de la victime, également par des manipulations informatiques telles que les chevaux de Troie, les zombies (= un logiciel installé dans le micro à pirater qui permet de masquer l'attaque par un virus), la désinformation telle que la diffusion d'un faux mail, notamment.

Les risques majeurs résident donc dans l'utilisation de moyens informatiques - tels qu'un PC - connectés au réseau et dans le fait de laisser son PC allumé sans surveillance (80 % des malveillances sont commises en interne).

**Ces attaques peuvent causer aux entreprises de graves préjudices, parfois irréversibles -divulgarion ou destruction de données ou bien atteinte à son image.**

**Une enquête menée en 2001 dans le département de la Sarthe** a montré que les agressions d'entreprises ne sont pas un mythe : dans le cadre d'une enquête auprès de 700 entreprises de plus de 20 salariés des secteurs de l'industrie, des services, et du BTP, les 149 questionnaires récupérés révèlent 217 agressions (certaines entreprises ont été victimes de plusieurs agressions) dont

- 55 cas d'intrusion
- 12 cas de piratage
- 15 cas de divulgation de rumeurs

### LES ENTREPRISES GUADELOUPEENNES ET LA SSI

D'après une enquête réalisée auprès des sociétés de sécurité informatique exerçant en Guadeloupe, le niveau de sécurisation des systèmes d'information est faible dans les entreprises. Les chefs d'entreprise ont conscience des risques qu'ils courent mais le coût induit par une sécurisation de leur système d'information est jugé encore trop élevé. En conséquence, tant qu'ils n'ont pas fait l'objet d'une attaque ou d'un incident mettant en péril leurs données, ils n'investissent pas !

Or, selon ces sociétés de sécurité informatique, il existe un réel problème en matière d'intrusion et de sauvegarde des données informatiques de l'entreprise, accru par les conditions climatiques instables et humides de l'île et par le manque de prévoyance des sociétés d'hébergement guadeloupéennes qui proposent la conception de sites Internet sans y prévoir de systèmes de protection - par exemple serveurs mandatés (proxy) et/ou logiciels pare-feu (firewall) .



## Quelques conseils aux entreprises :

© Mettre en place des moyens pour sécuriser son système d'information, c'est mettre en place des moyens de protection de l'information, de détection des attaques et de réactions aux agressions. Il est par exemple important de protéger les connexions téléphoniques ou informatiques externes à l'entreprise par un firewall (= logiciel permettant de filtrer les données provenant d'Internet.). Si le coût financier de cette démarche peut être relativement important pour une petite entreprise, il faut le relativiser en le rapprochant du coût induit par la détérioration ou la perte de données.

Il est également important d'être vigilant sur toute proposition formulée par les professionnels en matière de conception d'un site Internet de l'entreprise. Par exemple, il faut veiller à ce que la proposition de prestation prévoise aussi un volet protection du site et définisse clairement l'engagement et la part de responsabilité du prestataire.

© Il ne suffit pas d'acquérir les bonnes informations par une démarche d'intelligence économique, il faut aussi savoir les protéger. Il faut par exemple protéger son ultime offre de prix, que l'on soit PME ou grande entreprise répondant à un appel d'offre international. Dans la mesure du possible, il faut éviter d'utiliser un fax, un téléphone, une messagerie électronique non sécurisés pour transmettre des informations sensibles.

© Dans le domaine de la Sécurisation des Systèmes d'Information, il est indispensable d'investir aussi dans la formation. Le recours aux moyens techniques tels que le Firewall doit s'accompagner de la formation du personnel de l'entreprise à la sécurité et la sûreté de l'information de l'entreprise.

© Enfin, il convient d'attirer l'attention sur la part de risque que recèle un système d'information mal protégé, y compris pour le chef d'entreprise à titre personnel. Cette responsabilité va de pair avec la prise de conscience de ce que l'information est devenue valeur, parfois la seule détenue par une entreprise, et qu'elle est traitée par des systèmes qui fonctionnent de la façon dont les hommes les exploitent...

Ainsi, la responsabilité civile du dirigeant ou d'un salarié peut être engagée si par une faute caractérisée de sa part, l'entreprise subissait une perte de données qui lui serait très dommageable (par exemple divulgation d'un secret de fabrique ou de savoir-faire, de données particulièrement stratégiques, ou révélation d'une information confidentielle dont la diffusion prématurée désorganise l'entreprise. Ainsi l'article L.152-7 du Code Pénal prévoit : « Le fait, par tout directeur ou salarié d'une entreprise où il est employé, de révéler un secret de fabrique est puni de deux ans d'emprisonnement et de 30.000 € d'amende.

La responsabilité civile du dirigeant peut aussi être engagée par la divulgation de données personnelles ou des délits commis par le personnel à l'aide d'ordinateurs de la société, en l'absence de règlement interne encadrant l'utilisation de ces derniers,

De même sa responsabilité pénale pourrait être également retenue au titre de l'article 226-17 du Code Pénal qui réprime le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations, et notamment d'empêcher qu'elles ne soient communiquées à des tiers non autorisés.

\*\*\*