# 02/05/2012

Intelligence économique

**Intelligence Economique : Introduction**

25/04/2012

Idée de l’IE :

HRIE : Haut Responsable Intelligence Economique. Ce poste était occupé par Alain Juillet, qui

a quitté ses fonctions en 2009 (il avait commencé en 2005. Avant ce poste n’existait pas, il n’y

avait pas de coordonnateur). Le poste s’est alors trouvé vacant. Et plutot que d’avoir ce poste

rattaché au 1er Ministre (ministère de la Défense), on a décidé de changer le poste : Délégué

Interministériel à l’IE (DIIE), et de le rattacher au Président de la République. Aujourd’hui et

depuis fin 2009, c’est Olivier Buquen.

Décret 17 septembre 2009 : création du poste de DIIE, placé auprès du ministère de

l’Economie. Olivier Buquen a pris ses fonctions le 1er octobre 2009 (nommé).

3 axes / éléments en IE :

● veille stratégique,

● sécurité du patrimoine économique,

● lobbying (influence) au niveau économique.

**Pourquoi mettre en oeuvre une démarche d’IE dans une entreprise ?**

Ce concept a émergé au début des années 1990, à cause des 3 éléments suivants.

A cause de la mondialisation des échanges qui a placé les entreprises dans une situation de

concurrence internationale. Pose problèmes dans les PME et PMI. Concurrence la plus apre est

celle des anglo saxions, et non pas de la Chine. Contexte de **guerre économique**.

Développement exponentiel des NTIC : Nouvelles Technologies de l’Information et de la

Communication -> émergence de l’ère du numérique.

NSA : CIA technologique.

Information est devenue plus abondante, plus accessible, matière première stratégique que

les entreprises doivent pouvoir maitriser. Pb de la veille. Savoir la sélectionner. Avantage

concurrentiel si on sait la maitriser.

Information blanche (ou ouverte) : celle qu’on peut trouver sur Internet != info grise obtenue de

façon plus ou moins légale (par Internet) != info noire (ou fermée) qui est très illégale. On ne

parlera dans ce cours que de l’information blanche.

Ouverture généralisée des marchés et des pays émergents font apparaitre de nouveaux

concurrents, y compris au stade de la recherche et de l’innovation technologique.

Face aux nouveaux défis, les entreprises et notamment les PME doivent s’adapter et intégrer

l’IE à leur stratégie pour accroitre la compétitivité et pour protéger leur savoir-faire (si on pique

nos affaires, les autres vendent pareil et moins cher, on doit licencier, et ça porte atteinte à la

cohésion sociale).

DIIE : coordonne action de l’état au niveau national, à répercuter au niveau régional notamment

à la CCI, puis au niveau des entreprises.

*[ nouvelle législation sur la protection des secrets des affaires, élaborée ds le cadre d’un gros*

*projet avec les administrations, les représentants des entreprises (medef, afep, cgpme, cci).*

*Volet préventif : instaurer un “secret entreprise” : donner la possibilité aux entreprises d’identifier*

*formellement leurs informations clés -> fichier client, projet d’innovation ou d’acquisition, et*

*sera estampillé “secret entreprise”, et va mettre en place des mesures de protection pour ces*

*informations. Ces protections relèvent du bon sens : déposer les documents dans des coffres,*

*crypter les fichiers, avoir une liste de destinataires restreinte.*

*Volet répressif : création d’une nouvelle incrimination pénale : délit de violation de secret*

*d’affaires.*

*Ce texte a été présenté à l’Assemblée Nationale par le député Bernard Carayon (spécialiste*

*français IE) le 23 janvier 2012, adopté à l’unanimité. Il devrait être définitivement voté*

*prochainement. ]*

**Comment mettre en oeuvre l’IE ?**

***1. La compétitivité***

L’information constitue un élément de compétitivité de l’entreprise, parce que le chef

d’entreprise a besoin d’informations concernant ses propres activités pour :

● connaitre son positionnement sur le marché .

○ ex : entreprise de production de protection électrique.

○ Enjeux stratégiques : surveiller l’apparition d’une technologie de substitution

éventuelle, rester technologiquement leader

○ Actions : veille sur les brevets, sur les publications scientifiques, sur les

colloques, sur les salons)

○ Résultats : Identification des solutions concurrentes, des nouvelles applications,

des opportunités pour de nouveaux produits, aider le chef d’entreprise à la prise

de décision.

● identifier ses forces et ses faiblesses.

○ importance quantitative de la concurrence, et qualitative.

● détecter les opportunités.

● gérer la stratégie de développement de l’entreprise.

○ ex : entreprise de mécanique.

○ Enjeux : défendre la performance commerciale de l’entreprise sur des marchés

concurrentiels, assurer la croissance de l’entreprise et le déploiement sur de

nouveaux marchés.

○ Actions : construction d’une méthode de veille commerciale, valorisation de

l’information disponible au sein de l’entreprise, formation d’un pilote pour

coordonner toute cette information, et sécurisation du système d’information.

○ Résultats : meilleure connaissance de la concurrence et des marchés,

prospection pour les opportunités commerciales, amélioration de la remontée

d’information sur la concurrence (attente des clients)

● lancement de nouveaux produits et services

○ ex : société innovante dans le domaine des lasers médicaux a adopté une

démarche d’IE et à partir d’une action de veille, cette société a pu identifier

et approcher des secteurs de la chirurgie esthétique, et a été en mesure

de concevoir une nouvelle offre. Stratégie de propriété industrielle. A pris

contact avec les services spécialisés de l’Etat (DCRI : Direction Centrale des

Renseignements Intérieurs) *[ comme le MI5 et le MI6 en Angleterre ]*

● S’implanter sur de nouveaux marchés : l’entreprise doit s’informer sur le dispositif de

soutien aux entreprises pour le commerce extérieur. Se familiariser avec les formalités

réglementaires requises à l’importation ou à l’exportation en provenance ou en direction

des pays clients ou fournisseurs.

● S’adapter aux évolutions de l’environnement de l’entreprise (concurrence, législation,

normes, modes de consommation).

● Nouer des coopérations et des partenariats (mise en oeuvre de projets labellisés au sein

de pole de compétitivté -> développement d’une coopération scientifique, technologique,

commerciale)

● accroitre son influence : l’information peut être utilisée comme levier d’action, permettant

de promouvoir les intérets de l’entreprise dans un cadre légal (communication

d’influence, utilisation d’internet). Inversement, l’entreprise doit etre vigilente face à

l’emploi à son détriment de ses méthodes (les rumeurs, voire la désinformation (illégal :

raconter des trucs faux mais qui peuvent passer pour vrai) ~ diffamation), pbs par

rapport à l’image de l’entreprise.

***2. La sécurité***

L’information est également un élément de sécurité de l’entreprise. Sécurité capitale pour

le développement et la perrennité de l’entreprise. L’amélioration de la protection physique

de l’environnement de l’entreprise nécessite la mise en oeuvre de méthodes éprouvées et

l’affectation de moyens humains, financiers et techniques.

La situation au sein des entreprises françaises s’est nettement améliorée au cours des 10

dernières années mais il y a encore des progrès à réaliser : 73 % des entreprises de moins de

200 salariés estiment qu’il y aurait des conséquences sérieuses s’ils ne pouvaient pas se servir

de leurs outils informatiques pendant moins de 24h.

L’entreprise doit savoir communiquer tout en sécurisant son patrimoine informationnel pour :

● travailler en toute **confiance** avec ses collaborateurs dans l’entreprise, et à l’extérieur

avec ses partenaires. Cet objectif suppose de mettre en place un ensemble de

dispositifs et de procédures techniques, administratives, juridiques qui vont former la

politique de sécurité de l’entreprise.

○ inventorier les risques et les menaces potentiels.

○ protéger le système informatique et les données sensibles (nomination d’un

responsable SI, charte informatique, contrôle d’accès, actualisation des logiciels,

sensibilisation du personnel). Le SI de l’entreprise est vital car il structure

l’ensemble des aspects de son activité (comptabilité, salaires, achats, fichiers

clients et fournisseurs, factures, nouveaux produits, contacts partenaires, …)

○ moyens matériels de protection adéquats (grilles aux fenetres, mettre des

badges aux visiteurs, …)

○ introduire des clauses de confidentialité dans les contrats de travail.

○ établir un plan de continuité d’activité (prévention) en cas de dysfonctionnement

grave ou de situation de crise.

○ évaluer régulièrement le dispositif mis en place

● communiquer clairement et avec cohérence sur son activité, ses projets et sa stratégie.

● être en capacité de se défendre contre des concurrents qui utilisent des méthodes

déloyales (écrasement de drones sur des serveurs Michelin) -> piratage d’informations,

espionnage économique, contrefaçons (pbs avec la législation internationale...)

Exemples : Depuis des semaines, un inconnu circulait dans les différents services de

l’entreprise sans être inquiété en se faisant passer pour un salarié du laboratoire.

Des attaques qui modifient la présentation et le contenu du site de l’entreprise, qui en bloquent

l’accès -> perte de confiance de certains clients.

En cas d’agression, il faut impérativement porter plainte.

**Conclusion** : L’entreprise doit définir et mettre en oeuvre une politique d’IE pour maitriser,

protéger ses activités, et en assurer la perrennité. L’application d’une telle démarche nécessite

d’établir des liens avec des services spécialisés (de l’Etat ou de cabinets privés).

Les formations de l’Etat se font à l’IHEDN (Institut des Hautes Etudes de Défense Nationale)

pour se sensibiliser à la défense nationale, l’INHESJ (Institut National des Hautes Etudes de la

Sécurité et de la Justice).

***Olivier Buquen***

Sa maxime : “Il faut sensibiliser les salariés sur la nécessité de protéger le patrimoine de leur

entreprise, et ainsi de protéger leur emploi”.

Diplomé de l’ESEC, de Sciences Po Paris et de Harvard.

DIIE depuis 1er octobre 2009, préfet du Morbihan depuis le 8 février 2012.

Sa définition de l’IE : “L’IE a un objectif : la compétitivité. Elle s’articule autour de 3 axes :

● la ***collecte*** de l’information économique stratégique et ses étapes :

○ la veille,

○ l’analyse,

○ le traitement,

○ la diffusion

● l’***influence***, notamment la défense des intérêts français dans les instances

internationales

● la ***protection*** de l’information stratégique et au-delà de l’ensemble du patrimoine

économique, technologique et scientifique.

L’information collectée permet de prendre les bonnes décisions pour être compétitif. L’influence

implique le développement à l’exportation pour soutenir la compétitivité. Pour le 3è axe, il s’agit

de protéger la compétitivité.”

Pour l’Etat, la première mission de la DIIE (Délégation Interministérielle d’IE) a été d’élaborer et

de formaliser une politique publique d’IE : la stratégie de l’Etat en matière d’IE. Elle a fait l’objet

d’une communication au Conseil des Ministres en décembre 2010, et cela a débouché à une

circulaire interministérielle du Premier Ministre.

Dans cette circulaire, le Premier Ministre rappelle que l’action de l’Etat en matière d’IE s’articule

aussi autour de 3 axes :

● la ***veille stratégique*** : l’Etat collecte des informations pour son propre compte et pour

favoriser la prise de décision des dirigeants de l’Etat en matière économique.

● le ***soutien à la compétitivité*** au travers de la valorisation de la recherche publique au

profit des entreprises françaises et européennes, via le développement de l’influence de

la France dans les instances internationales, et grâce au soutien à l’export.

● la ***sécurité économique*** : l’Etat recense et analyse les attaques et les agressions

subies par les entreprises ou des établissements de recherche français. Il sensibilise et

forme ces entreprises pour leur faire prendre conscience de l’existence des risques pour

qu’elles s’en protègent et réduisent leur vulnérabilité.

C’est la mission de l’Etat, et la DIIE est à la tête du dispositif. Il y a des correspondants dans

l’ensemble des ministères, un coordonnateur régional auprès de chaque préfet de région, et

dans certains ambassades.

Il y a aussi des directions, des services dont une partie des missions est consacrée à l’IE et qui

contribue à l’action de l’Etat : la DGI (Direction Générale des Industries), DGA (de l’Armement),

la DCRI, la DPSD (Direction de la Protection et Sécurité de la Défense), la Gendarmerie

Nationale, la DG du Trésor.

prochaine fois : organisation de l’IE dans l’entreprise.

Partiel le 13 juin.

# L’organisation de l’IE dans l’entreprise.

L’IE est une démarche qui concerne toutes les entreprises. Elle doit pérenniser ses activités en protégeant toutes ses informations sensibles (savoir-faire, fichiers clients). Elle doit être également attentive aux initiatives des concurrents et être réactive en veillant à ce que les infos utiles parviennent aux décideurs.

Si le facteur taille de l’entreprise n’a pas d’influence sur la nécessité de mettre en place une démarche d’IE, il jouera sur la façon dont va s’organiser l’IE et les moyens qui y seront alloués.

3 modèles d’organisation :

1-L’IE est confiée à un responsable spécialisé au sein de l’entreprise.

L’entreprise s’est dotée d’une équipe spécialisée dirigée par un responsable à l’IE, rattachée à la direction générale ou à la direction de la stratégie. L’équipe est composée d’informaticiens, d’analystes des risques et de spécialistes de la veille. Ce schéma correspond aux entreprises qui disposent de ressources humaines et financières importantes.

2-L’IE est confiée à une personne qui a d’autres responsabilités au sein de l’entreprise.

L’IE est une activité confiée à l’un des collaborateurs ayant une responsabilité d’une unité opérationnelle de l’entreprise (directeur international ou DSI par exemple). La personne chargée de cette mission occupe des fonctions transversales dans l’entreprise et rattachée à la direction générale.

3-Le schéma type dans les PME

Beaucoup d’entreprises appliquent des démarches partielles d’IE (sans en avoir forcément conscience). La pratique d’IE est alors morcelée, elle n’est pas structurée, elle est partagée par plusieurs collaborateurs sans que la circulation d’infos ne soit organisée. La mise en place d’une démarche d’IE dans une PME, cad la mise en place d’une stratégie organisée et efficace relève souvent des dirigeants. La fonction peut, selon la taille de l’entreprise, être partagée entre plusieurs personnes. Dans ce cas, l’une des personnes peut être désignée comme animateur de groupe.

Avec des moyens limités, la TPE pourra profiter progressivement à la mise en place de la démarche d’IE. L’étape importante est l’identification initiale des besoins et leur hiérarchisation. Elle pourra se faire accompagner par les acteurs publics spécialisés à l’échelon régional en matière d’IE (DRRI, Référent IE de la Gendarmerie Nationale).

Les PME ayant des intérêts communs peuvent aussi se regrouper pour partager et mutualiser certaines informations pour bénéficier de la mise en place d’une démarche globale d’IE.

La taille de l’entreprise va donc commander la démarche d’IE.

# Les enjeux stratégiques et les besoins en information de l’entreprise.

La pléthore d’informations est un frein plus qu’une contribution réelle à la prise de décision. Afin de pallier ce risque et la perte de temps associée, il est indispensable pour l’entreprise de définir en amont et de manière précise quels sont ses besoins en information. Cette étape implique que l’entreprise mène une véritable réflexion sur les principaux aspects de son activité et des objectifs qu’elle souhaite atteindre. Ce n’est pas de la collecte d’informations que doit découler la définition de l’axe stratégique mais le contraire. La détermination des besoins en infos passe par l’identification des enjeux à long, moyen et court terme.

Comment ?

Quel environnement pour l’enteprise ⬄ Quelles forces et faiblesses de l’enteprise ?

Quelles opportunités et menaces pour l’entreprise ?

Quelles startéfies pour l’enteprise ?

Quel plan d’actions à court, moyens long terme ?

Identification des besoins en infos ?

Mise en place de la collecte de l’info

Traitement de l’info.

Le processus d’indentification des besoins en infos est un processus itératif, c’est-à-dire qu’il est permanent et qu’il suppose la possibilité d’une remise en cause. Il faut vérifier périodiquement is les hypothèses de l’environnement varient et quel est leur impact sur le positionnement de l’entreprise. Parrallèlement, le traitement de l’information collectée va modifié la perception de l’entreprise et peut amener de novueaux besoins en infos.

L’analyse de l’environnement de l’entreprise.

Nouveaux entrants, Concurrents, Marché client, Produits de substituants, Evaluation technologique, Tendances sociétales, Tendances politiques, Tendances juridiques, normatives, Tendances économiques, Fournisseurs.

L’objectif est de retenir 3 à 4 axes déterminants pour le développement de l’entreprise.

1. Avez-vous une vision précise de vos concurrents sur votre marché ? (identité, taille, rentabilité, positionnement, présence à l’internationale, axe de développement, nouveaux acteurs, …)
2. Avez-vous une connaissance suffisante des évolutions technologiques de votre secteur ? (degré d’importance de la maitrise technologique, probabilité d’apparition de nouvelles technologies (NTIC), …)
3. Avez-vous identifié les principaux facteurs d’influence du comportement de vos clients ? (marché domestique, marché international)
4. Connaissez-vous les grandes tendances économiques, sociétales, législatives susceptibles d’avoir une influence sur la croissance de votre secteur d’activité ?

Il s’agit ici de questions à se poser quant à l’environnement de l’entreprise.

Le positionnement de l’entreprise dans son environnement avec ses forces et ses faiblesses.

Quelle est votre vision à long terme pour l’entreprise ? (plus de 3 ans)

Quelles sont les actions à mettre en œuvre à court terme pour atteindre les objectifs ?

Disposez-vous des compétences nécessaires (forces, faiblesses, vulnérabilité) et quelles sont les connaissances à acquérir ou renforcer pour réaliser votre projet ?

2 types de besoins d’information :

1. Les besoins en informations permanents pour permettre à l’entreprise de surveiller l’environnement du marché et qui vont contribuer à la réalisation des objectifs de long terme. Ex : Quelle va être l’évolution technologique de mon marché en France et sur le marché européen ?
2. Les besoins en information ponctuels pour répondre à une question qui se pose pour mettre en œuvre les axes stratégiques. Ex : Quels sont les partenaires qui peuvent m’accompagner dans le développement de ma nouvelle technologie ?

La hiérarchisation des besoins est en fonction de leur importance pour la compétitivité de l’entreprise ou de leur caractère d’urgence ou des moyens de l’entreprise. Il faut communiquer en interne sur les besoins en information de l’entreprise afin de favoriser sa collecte et son traitement par les collaborateurs.

# La collecte de l’information

LA définition des objectifs stratégiques à moyen et long terme permet à l’entreprise de définir précisément ses besoins en informations et de s’engager dans le processus de collecte.

De la qualité et de la fiabilité des infos collectées dépendra la valeur ajoutée apportée au processus de décision de l’entreprise. En permettant d’éviter les écueils de la surinformation ou de la désinformation. La collecte de l’information doit être appréhendée sur le long terme comme un processus structuré, systématique mais aussi évolutif (capable de prendre en compte l’émergence de nouveaux besoins).

Le recueil d’information doit impliquer les salariés qui devront être sensibilisés aux enjeux stratégiques de l’entreprise et de ses besoins. L’efficacité de la veille passe par le partage des infos. Mais en interne comme à l’extérieur, le chef de l’entreprise devra faire attention à conserver le caractère confidentiel de certaines de ses recherches.

La formalisation des axes de recherche de l’information.

En fonction de l’identification des besoins, il est nécessaire de traduire ces demandes d’information en thèmes et en questions clairs et précis, triés et classés en fonction des différentes sources d’information sollicitées et de définir les terminologies et les mots-clefs.

L’identification des sources d’information fiables et pertinentes adaptées aux moyens et aux problématiques de l’entreprise.

1. Quelles sont les sources d’information en interne ?
   1. Les documents internes (tableaux de bords, documents de gestion, CR de réunion, études marketing, rapports du SAV, bilans et pièces comptables, rapports d’étonnement)
   2. Les fichiers (clients, fournisseurs)
   3. Le traitement des demandes externes (courriers et courriels, sites web)
   4. Les CV transmis.
   5. Les personnels (commerciaux, acheteurs, production, responsables SAV)
2. Quelles sont les sources d’informations externes ?
   1. Les clients (leurs attentes et réclamations)
   2. Internet (la presse généraliste et spécialisés en ligne, les sites internet des clients et des fournisseurs, les forums et les blogs (avis d’expert et consommateurs), les bases de données gratuites ou payantes, les réseaux sociaux)
   3. Les fournisseurs d’informations (la presse, les centres de documentation, les bases de données structurées)
   4. Les partenaires, les sous-traitants, les financiers
   5. Les institutions (administration, organisations professionnelles, réseaux consulaires)
   6. Les clubs et les associations
   7. Les manifestations (colloques, salons)
   8. Les experts (centres techniques, consultants privés)
   9. Les documents des concurrents (les plaquettes publicitaires, les rapports d’activités, les communiqués de presse)
   10. Les sources fortuites (lieux publics)

Organiser la collecte d’information

1. L’implication forte du chef d’entreprise qui aura la fonction de coordinateur de la collecte.
2. Il faut désigner une personne responsable de la collecte et lui allouer du temps pour mener le projet.
3. Il suffit d’évaluer le coût de la recherche et de l’adapter aux capacités de l’entreprise.
4. Faire ou faire faire ? Cela concerne les compétences disponibles, le coût et la confidentialité des informations recherchées.
5. La sensibilisation des salariés à la collecte des informations. Il faut :
   1. Expliciter les enjeux à court, moyen et long termes de l’entreprise
   2. Expliciter les objectifs et les résultats attendus de la collecte
   3. Fixer des objectifs précis aux salariés impliqués selon leurs compétences et leur fonction dans l’entreprise.
6. Développer une culture de la collecte d’information (capacité à s’interroger).
7. Valorisation de la participation aux recueils et au partage de l’information (Favoriser les retours d’expériences).
8. Expliquer les règles déontologiques (cadre juridique de la collecte d’information).

Quel type de dispositif mettre en place ?

Chaque entreprise doit mettre en place son propre dispositif adapté à sa taille, à sa structure, au nombre de ses salariés impliqués dans la démarche, à ses circuits d’informations, à sa culture. Un minimum d’organisation s’impose.

Dispositif de veille permanent.

Une élaboration de questionnaires de collecte selon les fonctions des personnels.

La mise en place d’un système de veille via internet à partir des sources préalablement identifiées.

L’élaboration de fiches standardisées pour le tri et le classement des informations collectées à partir de sources internes et externes.

Il faut définir quelles informations devront être diffusées : comment, pourquoi, à qui, quand ?

Une révision périodique des sources d’informations et des objectifs de la veille.

Pour résumer : il s’agit de répondre aux besoins en informations stratégiques (l’identification des infos qui auront un impact direct sur l’évolution de l’environnement de l’entreprise et sur son positionnement stratégique)

Dispositif de veille temporaire

Il concerne un sujet avec des questions précises. Un plan de recherches précis avec des points à traiter, des sources à utiliser, un destinataire, des délais.

Il s’agit de répondre à un besoin d’information ponctuel.

Quels outils pour la mise en place d’une surveillance permanente ?

Les flux :

* S’informer de l’actualité sur les sites sélectionnés en utilisant des lecteurs de flux
* La détection de changements sur une page web ordinaire.

Les alertes (recherche à partir de mots-clefs) : Les newsletters.

La collecte d’informations et la confidentialité.

Pour les sujets particulièrement sensibles à diffusion retreinte, il faut limiter le nombre de collaborateurs impliqués dans la collecte. Il faut être particulièrement vigilant dans la collecte d’informations auprès de sources humaines externes (Il doit y avoir une sensibilisation permanente des salariés sur les infos qui ne doivent en aucun cas être divulguées, même pour obtenir une information en retour). Il faut scinder la recherche d’informations en plusieurs sujets et diversifier les contacts. Il faut préparer son entretien en ayant pesé à l’avance les questions à poser.

En ce qui concerne la recherche d’informations sur internet, il faut utiliser une connexion banalisée (un abonnement à un FAI grand public) et supprimer régulièrement les cookies de son ordinateur.

# L’exploitation et la capitalisation de l’information

Les informations brutes qui sont collectées (internet, presse, contact direct, téléphone) ne pourront être exploitées comme instrument d’aide à la décision que si elles ont fait l’objet d’un traitement préalable (validées, fiables, structurées, hiérarchisées) pour obtenir un produit finis et fiable. C’est cette phase d’exploitation qui donne à l’information et à la collecte sa valeur ajoutée.

Sans cette étape essentielle, les prises de décisions et les orientations stratégiques du chef d’entreprise peuvent s’avérer difficiles à réaliser (surabondance d’informations brutes non analysées partant dans les tous les sens, incohérentes et impertinentes) voire constituer une menace pour les activités et le développement de l’entreprise (s’il y a mauvaise décision fondée sur des infos incomplètes, erronées, non fiables).

Une fois que l’info brute aura été valorisée, elle devra être capitalisée tout en demeurant accessible et facilement exploitable.

Traitement et analyse de l’information collectée

On distingue 2 étapes :

1. Le traitement puis l’analyse de l’information :
   * Il s’agit de trier les informations et de ne retenir que celles qui sont pertinentes, qui correspondent au besoin d’informations stratégiques qui ont été identifiées en amont. Il s’agit d’éliminer celles qui ne sont pas pertinentes. Il est possible de soumettre les infos pertinentes à la critique en cas de doute de manière à s’assurer de cette pertinence.
   * Valider les infos retenues. Evaluer leur exactitude, leur fiabilité. Quelle est la source de l’information ? Est-elle crédible ? Cette info peut-elle être recoupée ? Dans la pratique, on qualifie les infos en s’aidant d’une échelle d’évaluation : Infos fiable, peu fiable, non fiable. On peut également s’appuyer sur une compétence externe (l’appui d’un expert) pour des infos techniques
2. L’analyse de l’information
   * Donner du sens à l’information. Ne pas avoir de préjugés.
   * Organiser, structurer, hiérarchiser et rapprocher les infos. Toutes ces infos sont-elles importantes ? Vont-elles dans le même sens ?
   * Utiliser des outils d’analyse : les forces, les faiblesses, les opportunités, les menaces.
   * Repérer les éventuels signaux faibles et leur donner une signification.
   * Interpréter et synthétiser les principaux résultats de l’analyse. Quelle est la tendance ? Quels sont les risques ? Quels sont les signaux d’évolution de l’environnement ?
   * S’interroger. Ai-je en ma possession aujourd’hui tous les éléments pour prendre une décision ?

Au terme de l’analyse, une nouvelle collecte d’informations peut se révéler nécessaire si les résultats ne permettent pas de répondre aux besoins d’informations stratégiques qui ont été identifiés :

* Les informations sont partielles, mal ciblées et non actualisées. Les sources et les outils de collecte de l’information doivent être ajustés.
* L’analyse a permis d’identifier des besoins d’informations complémentaires. C’est un aspect positif.

L’information doit être formatée pour être assimilable par la personne à qui elle est destinée et elle doit être accessible. Les résultats issus de l’analyse sont des outils servant à des prises de décisions stratégiques. Pour cela :

* Il est indispensable que les résultats de l’analyse soient bien compris et assimilés par les personnes à qui ils sont destinés. A cette fin, il est souhaitable que les résultats s’accompagnent de recommandations simple, claire et d’arguments construits.

Les décisionnaires doivent pouvoir accéder aux infos issues de l’analyse. La phase de collecte puis d’analyse est un investissement en temps et doit pouvoir être valorisée par les décisionnaires.

La conservation des infos dans l’entreprise est indispensable. Elles enrichissent le patrimoine informationnel, la mémoire de l’entreprise, au même titre que les comptes rendus des réunions et les fichiers clients. Cela permet de retrouver une information pertinente et déjà validée.

La capitalisation des connaissances sera organisée par un classement des documents sur des supports papiers ou numériques (les classeurs, intranet, bases de données, cd-rom, disques durs,…) selon un dispositif d’archivage efficace, cad offrant des avantages organisationnels (temps d’accès réduit) et économiques (coûts réduits)

La classification des documents et leur disponibilité dans l’entreprise prendra en compte le degré de sensibilisation des informations. Un document d’analyse qui concerne des éléments relatifs à la stratégie d’entreprise ne devra être accessible que par les collaborateurs directement impliqués.

16/05/2012

## Sensibilisation du personnel à la protection des informations sensibles.

Toute entreprise est exposée au risque de perte ou de détournement d’informations (vol de support informatique, interception de communications, manipulations,…)

La protection des informations sensibles doit être une préoccupation majeure des acteurs de l’entreprise (les collaborateurs, les cadres dirigeants, les membres des organes sociaux). Il est essentiel que chacun ait conscience de la sensibilité et de la vulnérabilité des infos qu’il détient, des pratiques frauduleuses existantes et de la nécessité d’une diffusion maitrisée de cette information en interne (mais en externe aussi). C’est une prise de conscience qu’il convient de développer au sein de l’organisation. Il s’agit de définir une politique de défense de l’information adaptée aux besoins de l’entreprise.

1. Les informations sensibles

Il s’agit d’informations dont la divulgation procurerait ou réduirait un avantage à leurs concurrents ou à leurs partenaires. (R&D, travaux d’innovation, savoir-faire technologique, contenu d’offres commerciales, structure des comptes, fichiers clients, fonctionnement de l’entreprise).

Les informations encadrées par des exigences légales et contractuelles (secret des affaires). Il faut veiller à bien identifier les informations qui, prises individuellement son peu sensibles, mais constituent ensembles une information confidentielle.

Les réponses à les appels d’offres, les enquêtes, les sondages, les interviews, les salons, les déplacements, la diffusion d’informations à des actionnaires, les négociations commerciales, les échanges d’informations avec les partenaires de l’entreprise, l’utilisation d’internet. Il faut formaliser un référentiel de bonnes pratiques pour encadrer le comportement des salariés de l’entreprise dans ces situations. Il faut sensibiliser et former les salariés à la protection des informations sensibles de l’entreprise.

Il faut expliquer la notion d’informations sensibles aux salariés et les objectifs des mesures prises pour protéger l’information. Elles sont différenciées en fonction des personnels et de leurs responsabilités afin de faciliter l’acceptation et l’application de règles parfois contraignantes.

Organiser une sensibilisation permanente via des formations en fonction des personnels, des notes régulières, des réunions en interne, la diffusion des bonnes pratiques, l’affichage des précautions à prendre dans les zones sensibles, les écrans de veille affichant ces pratiques.

1. La responsabilisation du personnel.

Il s’agit d’inclure des clauses spécifiques dans les contrats de travail. Il faut prévoir des clauses de confidentialité dans les relations avec les contacts externes. Il convient de recueillir l’engagement des salariés à respecter les règles de sécurité du SI. Il faut contrôler régulièrement le respect des règles, notamment de protection des infos, et la connaissance des dispositions pratiques inscrites dans le règlement intérieur (les conditions de circulation sur le site, l’utilisation des moyens de communication et les SI, les sanctions éventuelles).

1. Les outils juridiques
   1. Le contrat de travail des salariés

Les clauses de confidentialité qui restent valables après la rupture du contrat (Les clauses de restitution des données confidentielles et de non-concurrence)

* 1. L’engagement de confidentialité

L’engagement de confidentialité à faire signer le plus largement possible (aux fournisseurs, clients, sous-traitants, prestataires extérieurs (maintenance, nettoyage, restauration, surveillance,…), sociétés d’assurance, fournisseurs d’accès et hébergeurs, stagiaires, intervenants occasionnels,…)

* 1. Le contrat de confidentialité

Lors de la mise en place d’un partenariat (collaboration, sous-traitance, prestation de services). Ce contrat constituera un engagement réciproque sur la sécurité que chacun apportera aux informations confiées par son ou ses partenaires.

\**Principaux points à retenir pour la rédaction d’un contrat de confidentialité dans le cas d’un partenariat\**

* Indiquer les principales informations sensibles qui seront échangées ou partagées.
* S’accorder sur le niveau de classification des informations et s’assurer que chacun donne la même signification aux dénominations
* Convenir des mesures de protection à mettre en place à mettre en relation avec le niveau des informations à protéger
* Contrôler la mise en place des mesures de sécurité et leur efficacité
* Déterminer des responsabilités relatives à la protection des informations communiquées.
* Obligation de résultats ou de moyens en matière de protection de l’information.
* Contrôler la diffusion des informations sensibles en interdisant l’accès à ceux qui n’ont pas à en connaitre ou en imposant des règles de confidentialité.
* Définir des procédures d’habilitation des personnes qui auront besoin d’en connaitre dans le cadre du contrat
* Préciser pour le personnel du partenaire qui est autorisé sur le site les autorisations d’accès qui sont accordées.
* Les moyens de communications mis à disposition et leurs conditions d’utilisation.
* La perte ou la destruction d’informations sensibles est le fait dans 80% des cas de maladresse internes ou de l’absence de processus de sauvegarde qui soit fiable.

Référentiel de bonnes pratiques pour les salariés.

L’élaboration et la diffusion de bonnes pratiques est indispensable pour prévenir le risque humain dans la perte d’informations sensibles. Cela permet d’identifier les situations dans lesquelles les salariés doivent rester attentifs aux respects des règles de protection des informations sensibles de leur entreprise.

Les comportements dans l’entreprise.

Mettre sous-clés les ordinateurs portables et fermer les bureaux. Verrouiller les postes de travail à l’aide d’un mot de passe complexe changé régulièrement. Les fax, les courriels : l’utilisation est à proscrire pour les informations les plus sensibles. Pour les informations moins sensibles, limiter les échanges au strict nécessaire. L’usage de fax sécurisés, l’usage de signatures et de chiffrement pour la messagerie et internet. Veiller à l’effacement des disques durs des photocopieuses et fax, notamment lors de maintenance. Un personnel de confiance doit toujours être présent.

Ne pas jeter les documents comportant des informations sensibles à la poubelle sans les avoir détruits.

1. L’accueil des visiteurs (clients, fournisseurs, prestataires).

Le visiteur est potentiellement un espion.

* 1. Avant la visite
* Se faire communiquer l’identité et la fonction des visiteurs
* Répertorier les informations qui pourront être portées à la connaissance du visiteur et celles qui ne pourront pas être divulguées.
* En cas de visite des locaux, établir un parcours qui évite les zones sensibles
* Dans le local où se déroule une réunion, ne pas laisser en évidence des documents sensibles.
  1. Pendant la visite
* Remettre un badge identifiable au visiteur.
* Les accompagner et les faire accompagner en permanence.
* Ne remettre que des documents indispensables.
* Les raccompagner jusqu’au point d’accueil
* Tenir à jour les badges individuels d’accès et veiller à les récupérer à la fin de la visite

1. L’accueil des stagiaires
   1. Avant le stage

* Vérification complète du CV (obligatoire pour les ressortissants étrangers)
* Accueil des stagiaires encadré
* Définir le contenu du stage et désigner un tuteur
  1. Pendant le stage
* Veiller à ne pas laisser un accès sans contrôle et/ou sans surveillance à l’intranet et aux documents.
* Veiller au respect des horaires et des lieux autorisés
  1. Après le stage
* L’examen approfondi des travaux du stagiaire visant à vérifier la non-divulgation de données jugées stratégiques ou sensibles (communication du rapport de stage).
* La rédaction d’un rapport par le tuteur.
* Supprimer les droits d’accès et le badge après sa sortie

1. La communication à l’extérieur de l’entreprise.
   1. Les salons
      1. Avant le salon

* Définir des informations qui pourront ou non être diffusées sur le salon
* Identifier les besoins d’informations et définir la façon de les obtenir (Rencontre sur le stand avec le partenaire ou le concurrent, l’acquisition de plaquettes de communication, la participation à une présentation organisée sur le salon)
* Etudier la disposition du salon, la place des exposants (concurrents) et les opérateurs présents et ceux qui ne le sont pas
* Limiter au strict minimum le nombre de documents ou matériel sensible
* Préparer les axes de réponses sur les sujets délicats
  + 1. Pendant le salon
* Ne pas laisser sans surveillance les matériels à risque (prototypes, maquettes)
* Profiter du salon pour collecter des informations stratégiques (prises de notes, plaquettes, rencontres fortuites)
* Eviter les conversations téléphoniques dans les trains.
* Faire preuve de discrétion à l’hôtel et au restaurant.
* Faire attention aux anonymes et aux faux journalistes (fouilles merde)
* Lors de la fermeture du salon, faire place nette sur le stand et vérifier l’ensemble des matos et docs
* Ne pas placer sur les stands des stagiaires inexpérimentés.
  + 1. Après le salon
* Suivre les réactions dans la presse ou sur internet.
* Etablir un rapport de visite qui répertorie les informations stratégiques collectées, les nouveaux contacts, les infos techniques sur les produits, les nouveaux matériaux et le diffuser aux collaborateurs concernés.

1. Les relations avec les fournisseurs et les clients.

Il faut une sensibilisation renforcée pour les acheteurs et les commerciaux qui ont une relation ancienne avec les interlocuteurs.

Limiter au strict minimum les infos diffusées.

1. L’utilisation des ordinateurs portables.
   1. Prévenir les risques de vols ou de copie

* Garder toujours son ordinateur près de soi
* L’équiper d’un cadenas et/ou d’une alarme.
* Utiliser un mot de passe complexe mêlant caractères numériques et alphanumérique changé régulièrement.
* Ne pas le mettre à disposition pour une présentation (risque de copie via une clé USB en quelques secondes)
  1. Réduire les conséquences d’un vol
* Transport des données sensibles via des supports amovibles (CD, clé USB) séparés de l’ordinateur portable.
* Chiffrer le disque dur
  1. Précautions d’utilisation
* Dans un espace public, travailler uniquement sur des informations non confidentielles et utiliser des filtres opaques
* Désactiver tous les moyens de communication offerts par votre portable (wifi, Bluetooth)
* Mettre à jour des correctifs de sécurité avant de le reconnecter sur le réseau de l’entreprise

1. Les déplacements
   1. Les principales règles de sécurité

* Emporter uniquement les pièces d’identité et les documents administratifs nécessaires.
* Tout documents, carnets d’adresses, agendas, notes, badges, papiers en-tête de la société peut être volé et/ou dupliqué
* Ne jamais aborder d’aspects confidentiels en dehors de l’entreprise (dans les transports, les clubs,…)
* Ne jamais laisser de documents confidentiels sans surveillance, même quelques minutes.
  1. A l’hôtel
* Ne jamais laisser de documents sensibles dans sa chambre sans surveillance
* Ne pas mettre de documents ultra confidentiels dans le coffre de la chambre ou de l’hôtel
* Ne pas aborder de sujets confidentiels au téléphone

## Sécurité du Système d'information

Dans 80% des cas, ce sont les maladresses internes volontaires ou non ou l'absence de sauvegardes fiables qui sont à l'origine de la perte ou de la destruction d'information sensible. Le reste du temps, ce sont des actes externes malintentionnés. Le risque sur le système d'information s'est accru avec le développement du travail à distance et des nouvelles technologies. L'entreprise doit consillier la nécessité de communiquer des infos et de préserver certaines d'entre elles en mettant en place une politique de SSI. Pour être efficace, cette politique doit s'appuyer sur la mise ne place de moyens techniques. Son efficacité reposera sur la structure de l'entreprise et sur les comportements individuels.

1. Que protéger ?
   1. Le système d'information comprend :

* Le ou les serveurs réseaux
* Des postes de travail informatiques (fixes ou mobiles)
* Les applications (OS, sw...)
* Les infrastructures de communication et de télécommunication (réseaux locaux, liaisons inter-sites, le réseau téléphonique, l'accès à internet...)
  1. Les informations sensibles détenues par l'entreprise

Ce sont les informations dont la divulgations procurerait un avantage à la concurrence ou aux partenaires, ou réduirait l'avantage dont dispose l'entreprise tel que la R&D, les travaux d'innovation, le savoir faire technologique, le contenu d'offres commerciales, la structure des comptes financiers, les fichiers clients, les projets de développement, le fonctionnement de l'entreprise. Les informations les plus sensibles devront faire l'objet de procédures renforcées.

1. Quels sont les risques pesant sur le système d'information ?

* Les vols
* La destruction de données
* Les captations d'informations
* L'indisponibilité du système

Tout cela avec une origine qui peut être externe mais souvent interne (négligence, malveillance...)

1. Quelles sont les vulnérabilités du SI ?

* Les modes d'accès au réseau de l'entreprise
* La protection insuffisante des serveurs
* Les équipements nomades
* La messagerie non protégée

1. La formalisation d'une politique de protection du SI

* La désignation et la formation d'un responsable SSI
* La formation et la sensibilisation permanente de l'ensemble des salariés à la protection des informations sensibles
* Il faut établir une charte avec les règles de bonne pratique quant à l'utilisation du SI /
* Confidentialité et renouvellement des mots de passe
* Verrouillage de l'ordinateur
* Gestion des courriels
* Déclaration de tout incident
* Sauvegarde et suppression des données les plus anciennes
* Installation de tout nouveau logiciel interdite sans autorisation.
* Des règles d'utilisation pour internet (téléchargement...)

Il faut encore l'engagement de la responsabilité des utilisateurs avec une charte d'utilisation annexée au règlement intérieur ou un document qui renvoie au règlement intérieur pour les sanctions.

1. Quelles procédures de sécurisation du SI ?
   1. L'authentification
      1. Déterminer les droits d'accès au SI

Différencier selon les responsabilités des salariés et les statuts des autres personnes qui peuvent avoir accès au SI (stagiaires, personnels temporaires, prestataires extérieurs). Qui a le droit de faire quoi ? De savoir quoi ?

* + 1. La gestion des codes d'accès et des mdp

Il faut attribuer les mdp suffisamment sécurisés (un agrégat de caractères alphanumériques) et les renouveler régulièrement (tous les 3 mois). Ne pas oublier de les supprimer lors des départs des individus

* + 1. Configuration des postes par le responsable de la SSI
  1. Sécuriser les information et le Système

5.2.1 Logiciels et matériels de sécurité

Antivirus, antispyware, firewall, antispam pour les serveurs et les postes informatiques.

5.2.2 Sécurisation des échanges

Internet, wifi par le chiffrement des données les plus sensibles.

5.3 .3 Pour les données très sensibles

Utiliser un matériel non connecté au réseau.

5.3.4 Application des mises à jour et correctifs des logiciels

5.3.5 Controle régulier de la config des firewall.

5.3.6 Veille sur les nouveaux virus et les logiciels espions

* 1. La sauvegarde
     1. Définir le type de données à sauvegarder

Selon quelle périodicité et pour quelle durée. Il faut revoir périodiquement le périmètre de sauvegarde.

* + 1. Dupliquer les sauvegardes

Répartir les infos confidentielles sur plusieurs supports

* + 1. Sécurisation des lieux de sauvegarde

Conservation des supports mensuels et annuels en dehors de l'entreprise.

5.3.4 Il faut un contrôle du fonctionnement des sauvegardes

5.3.5 Il faut s'assurer du cryptage des données sauvegardées chez un prestataire.

* 1. Contrôle de la bonne utilisation du SI par les salariés

Le contrôle est nécessaire, l'entreprise étant responsable de la protection de son SI. Ces mesures doivent être transparentes, connues de tous, faire l'objet d'une discussion collective, faire preuve de précision, définir clairement les procédures concernant les messages privés.

* 1. La gestion des incidents
     1. Détection des vulnérabilités et anomalies le plus en amont possible
     2. Les instances à alerter en cas d'attaque informatique

La gendarmerie, la DCRI, l'OCLCTIC (Office Central de Lutte contre la Criminalité liée au TIC), la Brigade d’Enquête sur les Fraudes au TIC

* + 1. Prévoir des solutions de secours en cas d’indisponibilité du SI (assistance dépannage, mise à disposition de matériel de secours)

5.6 Le recours à la sous-traitance

* + 1. La santé du prestataire
    2. Les clauses de confidentialité
    3. Les dix points clés du contrat de sous-traitance.   
       - Mention dans le document contractuel de l'ensemble des documents (cahier des charges)

- Description précises des prestations

- Le régime de l'obligation du prestataire (Les moyens ou les résultats)

- Le prix des prestations (les critères d'évolution des prix)

- L'établissement du montant des pénalités

- Définition du statut et de la propriété des matériels et logiciels

- Étendue de la responsabilité

- Limitation du préjudice réparable

- Cession de droit

- Juridiction compétente en cas de litige

1. Les enjeux juridiques

6.1 Le risque de mise en cause civil ou pénal de l'entreprise induite par le comportement de ses salarié

6.1.1 L'utilisation malveillante des moyens de communication électroniques et informatiques

(Les moyens de messagerie, les forums avec des contenus diffamatoires à l'égard de tiers)

6.2.2 Le téléchargement de documents ouvrant droit à des poursuites pénales (pédophilie, incitation à la haine raciale, droits d'auteurs...)

6.2.3 La contrefaçon

L'utilisation de copies illicites de logiciels ou d’œuvres protégées sans autorisation des ayants droits.

6.2.4 Le traitement de données nominatives sans autorisation (cf CNIL)

6.2.5 Le non respect du secret des correspondances privées.

* 1. En cas de défaut de protection de son SI

La responsabilité de l'entreprise peut aussi être engagée :

* + 1. Par ses partenaires extérieurs (atteinte à leur SI), non respect des engagement de livraison ou de confidentialité
    2. Par ses actionnaires et ses salariés (mise en cause du dirigeant pour faute de gestion)

La responsabilité du chef d'entreprise peut être mise à en cause en cas de non-respect des procédures dans la mise en place d'un processus de cyber-surveillance des salariés (cf CNIL)

L'entreprise est soumise à la nécessité de veiller à l'intégrité, à la confidentialité, la disponibilité et la traçabilité de ses informations, de mettre en place les moyens adaptés tant d'un point de vue technique qu'organisationnel (procédure et encadrement du comportement humain)

L'image de l'entreprise

Toute entreprise peut être victime d'une atteinte à son image. Elle peut être multiforme :

* Dénigrement des produits et des services
* L'appel au boycott
* La mise en cause des dirigeants
* La diffusion d'informations erronées
* L'utilisation malveillante du nom de l'entreprise, de ses marques
* Détournement de sa communication (slogan)
* La défiguration du site internet
* La mise en ligne d'un faux site.

Plus les entreprises sont vulnérables, plus elles interviennent sur des secteurs en relation directe avec le consommateur. Ces attaques ternissent la réputation de l'entreprise et peuvent aller jusqu'à sa mise en péril de sa santé économique.

Il faut disposer d'une veille stratégique sur la réputation de l'entreprise. => rapidité de la réaction de l'entreprise.

Il faut agir contre les nuisances relevée.

1. La veille sur la réputation de l'entreprise
   1. Il faut organiser la collecte permanente de l'information véhiculée sur l'entreprise
      1. Sur internet

* Identifier les sources pertinentes (site de presses, concurrents, blogs => moteurs de recherche spécialisés wikia, technorati, les sites des ONG, les réseaux sociaux, les sites collaboratifs comme wikipédia, les forums...
* Définir des mots clés avec différentes orthographes, le noms des responsables, le nom de l'entreprise, les marques, le nom des concurrents et de leurs dirigeants. L'interrogation des sources identifiées doit être régulière.
* Il faut un paramétrage d'alertes via des outils informatiques (google alerts, flux rss)
  + 1. Dans la presse nationale et régionale et dans la presse spécialisée
    2. Collecte via le réseau commercial

Afin d'identifier et de répondre à d'éventuels mécontentement.

1.2 Renforcer le dispositif de veille lors des périodes particulièrement sensibles

* La sortie d'un nouveau produit
* Une restructuration
* La transmission de l'entreprise
* Le départ d'un collaborateurs
* …

1.3 Contrôler systématiquement les communications écrites de l'entreprise

Afin de maîtriser tout risque d'interprétation qui serait préjudiciable à l'image de l'entreprise.

1.4 Contrôler les sites web qui pointent vers le site de l'entreprise

Le fait d'établir un lien vers un autre site sans autorisation peut être considéré comme portant préjudice.

1. Agir contre les nuisances relevées

Avant d'entreprendre toute action, toute riposte il est important de s’interroger au préalable sur la capacité de nuisance de l'auteur de l'attaque. C'est cela qui va déterminer l'ampleur de l'action à mettre en place.

* Les actions de riposte progressives à mener en fonction de l'ampleur de l'attaque et de sa diffusion :
  1. Élaborer une stratégie de réponse
* Expliquer pourquoi on est dénigré ? Pourquoi les informations sont fausses ?
* Quelles sont les cibles ? Qui faut-il convaincre
  1. Identifier les auteurs de la nuisance et les contacter pour demander la suppression des propos litigieux et éviter une propagation rapide via internet.
  2. Contacter les hébergeurs de sites dont la responsabilité juridique peut être mise en cause
  3. Répondre aux informations diffamatoires ou préjudiciables diffusées sur les sites, les blogs et les forums de discussion.
  4. Communiquer en interne pour l'entreprise
  5. Utiliser le site internet de l'entreprise pour démentir les faits et pour argumenter.
  6. Mettre en place une véritable communication de crise vis à vis de l'ensemble des partenaires de l'entreprise et des média.
  7. Entamer une procédure juridique. Quels sont les principaux recours juridiques ?
* Le droit de réponse (Art. 6-IV de la loi sur la confiance de l'économie numérique du 21 juin 2004)
* La diffamation et les injures (Art. 29 de la loi du 29 juillet 1881 sur la liberté de la presse)
* La responsabilité éditoriale des hébergeurs de sites (Art. 6 de la loi sur la confiance de l'économie numérique du 21 juin 2004)
* La contrefaçon de marques (Art. L716-1 du code de la propriété intellectuelle)
* Action judiciaire contre le parasitisme dont le cyber-squatting d'une marque ( dépôt de nom de domaine similaire à la marque)
* Concurrence déloyale, parasitaire et dénigrement.

NB : Afin d'être sur de choisir la procédure appropriée, il est important de prendre conseil auprès d'un expert juridique.

Il est également nécessaire d'avoir déposé les noms liés à sa dénomination sociale et à ses marques dans les différentes extensions.

Protection par la propriété industrielle ou le secret

L'innovation contribue au succès des entreprises et quand elles sont détentrices d'un savoir-faire spécifiques, elles s'exposent à un risque de pillage de leurs innovations et de contrefaçons (10% du commerce mondial) et détruit 30 000 emplois chaque année en France :

* Les produits alimentaires et les boissons
* L’électroménager
* Les jouets
* Les médicaments
* Les pièces détachées pour automobiles.

Afin de protéger son patrimoine immatériel, l'entreprise doit définir une véritable stratégie de protection de ses innovations.

1. Définir les objectifs de la stratégie de protection des innovations.

* Quels sont les savoir-faire qui doivent être protégés ? Ceux dont la perte implique une perte de compétitivité de l'entreprise
* Comment les protéger ? La protection par la propriété industrielle ou le secret
  1. La propriété industrielle
     1. Les principaux outils de la propriété industrielle
* Le brevet. Il protège les innovations techniques et donne à son titulaire le monopole de son exploitation (pendant 20 ans ou 25 ans dans le cadre de médicaments
* Les dessins et les modèles. Protection du design des produits avec un monopole d'exploitation pour une durée minimale de 5 ans prolongeable tous les 5 ans jusqu'à 25 ans.
* Les marques. Assurance d'exploitation du monopole de la marque pendant 10 ans renouvelable indéfiniment
* L’enveloppe Soleau : elle permet de constituer une preuve de la création d'une idée ou d'un projet mais n'offre pas de protection.
  + 1. Outre la protection des innovations, la propriété industrielle contribue aussi à la valorisation de l'entreprise
* Valorisation financière
* Concession de licences
* Cession de titres
* Valorisation de l'image auprès des fournisseurs, des clients et des financeurs.
  1. Le secret industriel ou de fabrication

Le savoir-faire de l'entreprise est tenu caché des concurrents. Il est indispensable en cas d'invention non-brevetable.

* + 1. Brevet ou secret ?

Le brevet :

En guise de protection juridique, il y a un monopole d'exploitation opposable à tous.

En guise de coût, ils sont potentiellement élevés. Mais ils sont également une source de revenu par la concession de licence.

La divulgation des informations est élevée, c'est la condition de validité du brevet. Elle donne accès aux concurrent à l'information technologique de l'entreprise 18 mois après le dépôt du brevet.

Le secret :

En guise de protection juridique, la protection légale est limitée. Il faut faire attention à mettre en place des mesures de protection (systèmes de sécurité, clauses de confidentialité) pour prouver le caractère confidentiel du savoir-faire. En guise de coût, ils sont plus faible mais il faut prévoir des coûts internes.

La divulgation des information est exclue  et permet de conserver le caractère confidentiel.

* + 1. Sur quelles zones géographiques ?

La protection industrielle est possible à l'étranger :

* Pour les brevets au niveau européen (danger CHINE !)
* Pour les dessins et modèles, au niveau communautaire
* Pour les marques, à l'international et au niveau communautaire

1. Éviter la contrefaçon
   1. Surveiller ses brevets et ses marques par une veille technologique et concurrentielle

Pour s'assurer que personne n'utilise son invention sans autorisation (publication et presse spécialisée, salon professionnels, site internet, bdd sur les titres de propriété industrielle...)

* 1. Chercher à repérer le plus en amont possible les signaux des contrefaçons

Baisse de l'activité par la perte de marché, dégradation inexpliquée de la notoriété.

* 1. Mettre en place des mesures de protection

Inclure des clauses dans le contrat de travail des salariés, mettre en place un système de sécurité

* 1. Bien gérer ses droits de propriété industrielle

Suivre les délais auxquels les titres sont soumis. Renouveler ses marques et noms de domaine.

* 1. Surveiller les titulaires de licence afin d'éviter un manquement de leur part.
  2. Avoir recours au service des douanes afin d'identifier d'éventuels contrefacteurs.

Ils ont le pouvoir de retenir des marchandises afin de permettre à l'entreprise de saisir les autorités judiciaires à condition qu'une demande d'intervention ait été préalablement déposée par l'entreprise.

La demande d'intervention :

* Elle sert à attirer l'attention des douanes sur un produit suspect
* C'est l'unique procédure pour obtenir une saisi par les douanes dans les cas de contrefaçons présumées de dessins et modèles de marques ou d'atteinte à un brevet
* Elle permet de disposer de 10 jours ouvrables pour saisir les autorités juridiques compétentes.

C'est indispensable pour permettre aux douanes d'agir contre la contrefaçon.

* 1. Poursuivre les éventuels contrefacteurs

Code de la propriété intellectuelle.

* + 1. La contrefaçon

C'est un délit au même titre que le vol. Elle est passible de sanction :

* Pénales (Amande de 300 000€, 3 ans de prison ferme ou 500 000€ et 5 ans de prison en bande organisée, fermeture totale ou partielle de l'établissement qui a servi à commettre l'infraction)
* Civiles (Dommages et intérêts versés aux titulaires des droits, destruction de la marchandise et du matériel, publication de la décision.)
* Douanières (Confiscation des objets et des moyens de transport et des objets qui ont servis à masquer la fraude + amandes)
  + 1. Lutte contre la contrefaçon sur internet

Le 20 février 2009, le secrétaire d'état chargé de l'industrie et de la consommation a lancé une mission pour lutter contre la contrefaçon sur internet. La mission est chargée de mettre en place des engagements entre plateformes de e-commerces titulaires des marques et associations de consommateurs. Cette lutte se développe.

Il existe une loi « modernisation de l'économie » qui propose des mesures de simplification de la procédure de dépôt de brevets.