

PROTECTION DU PATRIMOINE DE L'ENTREPRISE

Afin d'aller au-delà de la veille stratégique, vers une véritable démarche d'intelligence économique, il convient, entre autres, de protéger son patrimoine. Cette démarche s'inscrit dans l'axe de la Loi Carayon qui, en mai 2004, recommande la protection de l'information économique.

Par «patrimoine», il faut entendre l'ensemble des biens matériels et immatériels de l'entreprise dont particulièrement le patrimoine informationnel.

En particulier, il s'agit pour l'entreprise :

- d'assurer la protection de ses savoir-faire méthodologiques spécifiques, différenciateurs. *Exemple : savoir-faire spécifiques d'un cahier des charges pour la réalisation d'un produit*
- de protéger l'information à valeur ajoutée générée dans le cadre d'études sur projets ou de synthèses thématiques.
- de protéger l'information à caractère économique de l'entreprise

La protection du patrimoine est l'affaire de tous et doit être inscrite dans la culture d'entreprise. Afin qu'elle soit effective, il est nécessaire de sensibiliser le personnel de l'entreprise :

- à la valeur de l'information et aux avantages compétitifs qu'apportent une exploitation formalisée de la ressource informationnelle dans le cadre d'une démarche de veille stratégique ;
- aux risques encourus par les fuites d'informations au profit de son environnement concurrentiel. Sur cette thématique, la Direction de la Surveillance du Territoire (DST) propose des interventions de sensibilisations auprès des entreprises.

Ceci implique une Direction volontairement engagée. Elle s'implique et apporte son soutien.

Ceci nécessite par ailleurs que le personnel se sente concerné par la vie de l'entreprise, qu'il soit impliqué dans son développement et qu'il ait une vision minimale de sa stratégie.



LA METHODOLOGIE

DIRECTION

Obtenir de la Direction un soutien nécessaire pour la mise en place d'une politique pérennisée et les moyens correspondants.

IDENTIFICATION DU PATRIMOINE SENSIBLE

Il convient de définir le périmètre limitant l'application de la protection. Définir en particulier des niveaux de confidentialité pour ne protéger que ce qui doit être protégé.

IDENTIFICATION DES MENACES

Identifier les menaces propres à l'entreprise et évaluer les risques qui y sont liés.

CLASSIFICATION DE L'INFORMATION

Ne protéger que l'information nécessaire.

ORGANISATION

Mettre en œuvre une Formation/Information pour que cette culture s'installe dans l'entreprise.

MISE EN PLACE DE BONNES PRATIQUES

Se référer à la norme ISO 17799.

LES REGLES DE BASE, sans tomber dans la paranoïa !

A l'accueil

- identifier les visiteurs ;
 - ne pas afficher les visiteurs du jour, ne pas présenter la liste des récents visiteurs ;
 - éviter de laisser des documents -autres que publicitaires ou revues généralistes- en salle d'attente : tarifs, rapports d'activité, publications spécifiques... ;
 - éloigner le standard de la salle d'attente : éviter que les visiteurs puissent capter les noms et les conversations d'éventuels clients ou fournisseurs.
- organiser des circuits spécifiques des visiteurs : les lieux stratégiques ou les installations qui pourraient trahir des savoir-faire confidentiels à ne pas montrer ;
 - s'assurer que les visiteurs restent toujours accompagnés ;
 - bien encadrer le personnel non permanent (stagiaires, intérimaires...) : vérifier préalablement leur identité ; ne pas les laisser accéder aux informations et lieux stratégiques.

Lors de visites ou séjours dans l'entreprise :

- éviter de laisser à portée de vue des visiteurs des documents internes à l'entreprise (sur le bureau, affichés au mur, sur les dossiers classés dans l'armoire ouverte...) : factures, devis, projets... ;
- bien gérer les visites de personnes étrangères à l'entreprise : vérifier l'identité des visiteurs (surtout étrangers) : D'où viennent-ils? Qui sont-ils? Qui visitent-ils et pourquoi ?; au besoin, la visite peut se limiter à la projection de transparents dans une salle de réunion ;

Au téléphone :

- se méfier des interlocuteurs téléphoniques inconnus et ne pas leur répondre sans au préalable vérifier leur identité et la vraie finalité de leur appel : au besoin, demander d'envoyer par fax avec en-tête de l'entreprise, la confirmation de la demande ;
- se méfier (davantage encore) si votre interlocuteur se présente comme un stagiaire d'école ou un organisme chargé de faire un état du marché ou un état des techniques ;
- éviter de tout dire au téléphone : ses nouveaux projets, sa politique tarifaire, sa stratégie, ses parts de marché... ; provoquer plutôt une rencontre.

En déplacement :

- rester prudent dans ses propos lors de conversations professionnelles à l'extérieur de son entreprise, qui pourraient être entendues par des tiers intéressés (lors des déplacements en transports en commun -avions, TGV...-, en taxis ou dans des lieux publics -salons, congrès, restaurants, hôtels-...);
- ne pas trop dévoiler ses projets à ses fournisseurs, ni à ses clients : ils sont, tout comme pour vous, une source intéressante pour les concurrents ;
- éviter dans la mesure du possible de sortir des documents confidentiels hors de l'entreprise ; le cas échéant, ne jamais laisser de documents (papier ou électroniques) confidentiels sans surveillance (par exemple sur le siège passager de sa voiture pendant que l'on effectue une course, si rapide soit-elle) ou à portée du regard d'autrui (dans le train ou au restaurant) ;
- ne pas laisser, en particulier à l'étranger, de documents sensibles dans les chambres d'hôtel en son absence ;
- ne pas se laisser entraîner dans des discussions passionnées -mais imprudentes- avec des personnes étrangères à son entreprise.

Dans son entreprise :

- former ses collaborateurs ;
- mettre à jour le règlement intérieur ;
- mettre sous clé tout document sensible quand ils ne sont pas utilisés ;
- s'assurer que les documents promotionnels ou revues internes ne laissent pas filtrer de renseignements confidentiels utiles à la concurrence ;
- ne pas jeter tels quels à la corbeille de documents pouvant contenir des données sensibles (les détruire) ou des supports informatiques endommagés dont le contenu pourrait néanmoins être récupéré ;
- ne pas laisser son bureau ouvert en cas d'absence même de courte durée ;
- maîtriser son patrimoine documentaire (archivage) ;
- connaître et mettre en œuvre les règles de propriété intellectuelle et industrielle

Avec ses partenaires :

- sélectionner et travailler avec des partenaires, sous-traitants et prestataires dans un cadre contractuel : ceci est valable pour tous les acteurs collaborant avec l'entreprise et susceptibles d'accéder à des informations confidentielles, que ce soit des cabinets d'étude de marché, d'audit..., des sociétés de traduction, des transporteurs..., et autres sociétés de service intervenant pour l'entreprise.

LA SECURITE INFORMATIQUE

Il est également indispensable d'assurer la protection physique de l'information qui, lorsqu'elle est stockée sans précautions sur le disque dur d'un ordinateur relié à un réseau ou non, peut être lue, copiée, modifiée ou détruite localement ou à partir d'un poste de travail distant sans que, trop souvent hélas, le propriétaire s'en aperçoive.

LES LIENS UTILES

Vous pouvez retrouver une liste de sources à l'adresse suivante, rubrique «Protection du patrimoine» : www.cieouest.com/ressources

Ce Mémento a été réalisé par le
CLUB INTELLIGENCE ÉCONOMIQUE DE L'OUEST

avec le soutien de l'ADIT.

Il traduit les travaux d'atelier conduits par :

F. Busnel - *Securitiel*
JP. Busquets - *Spécialiste en propriété industrielle*
A. Constant - *EDF*
H. Jehan - *Réussir SAS*
B. Marie - *Web Interactive*
V. Parise - *Innovation Process*
M. Taouji - *ENSICAen*
S. Tisserand - *Atlantique Immobilière des chemins de fer*

Le site internet du club
d'intelligence économique
de l'Ouest : www.cicouest.com

Le Club réunit essentiellement
des PME/PMI et des groupements d'entreprises
du Grand Ouest pour :

- échanger des expériences dans des domaines de la veille stratégique et de l'intelligence économique
- élargir son réseau relationnel dans le cadre de rencontres thématiques organisées
- se former aux outils et méthodes relatifs à la veille et à l'intelligence économique
- mener des démarches de veille collective
- promouvoir la veille et l'intelligence économique

