Comment sécuriser l'information de l'entreprise ?

Pour la PME, la sécurité économique recouvre des réalités très variées, souvent complexes et imbriquées. On peut la définir comme « l'ensemble des moyens actifs et passifs assurant la sauvegarde du patrimoine industriel, informationnel et immatériel de l'entreprise ainsi que ses activités » (Source : Guide de la Sécurité Economique, Préfecture de Seine- Maritime). Il est clair qu'en ce domaine il n'existe pas de risque zéro : tout l'enjeu pour l'entreprise est donc de réduire les risques à un niveau acceptable sans entraver son fonctionnement. Dans cette fiche, nous vous proposons quelques bonnes pratiques pour sécuriser votre information.

1. La première étape consiste à repérer les informations stratégiques de l'entreprise ainsi que les risques associés. Il faut donc faire l'inventaire de toutes ses informations sensibles ou confidentielles (orientations stratégiques, actions d'influence, études de concurrence, fichiers clients et prospects, liste des fournisseurs, contrats, données comptables, paie, dossiers du personnel, organigramme détaillé de l'entreprise, brevets, plans, procédés de fabrication, codes sources, résultats de votre veille concurrentielle…) et recenser les ressources du système d'information de l'entreprise (ordinateurs fixes et portables, accès à internet, messagerie électronique, logiciels, clefs USB, Wi-Fi, *Bluetooth*, téléphones fixes et portables, télécopieurs, photocopieurs, armoires et locaux d'archivage…).

Il faut également prendre conscience des menaces qui pèsent sur votre entreprise : vols d'informations, de savoir-faire et de secrets de fabrication, contrefaçon et atteintes à la propriété intellectuelle, pertes de données après sinistre ou après une erreur de manipulation, intrusions dans le système informatique, mise hors service des ressources informatiques, débauchage de salariés, risque financier par prise de capitaux extérieurs, mise en cause au plan légal et actions de justice, atteintes à l'image de marque…

Sans sombrer dans la paranoïa, il ne faut pas se croire à l'abri sous prétexte qu'on est une petite entreprise ou que son secteur est peu concurrentiel.

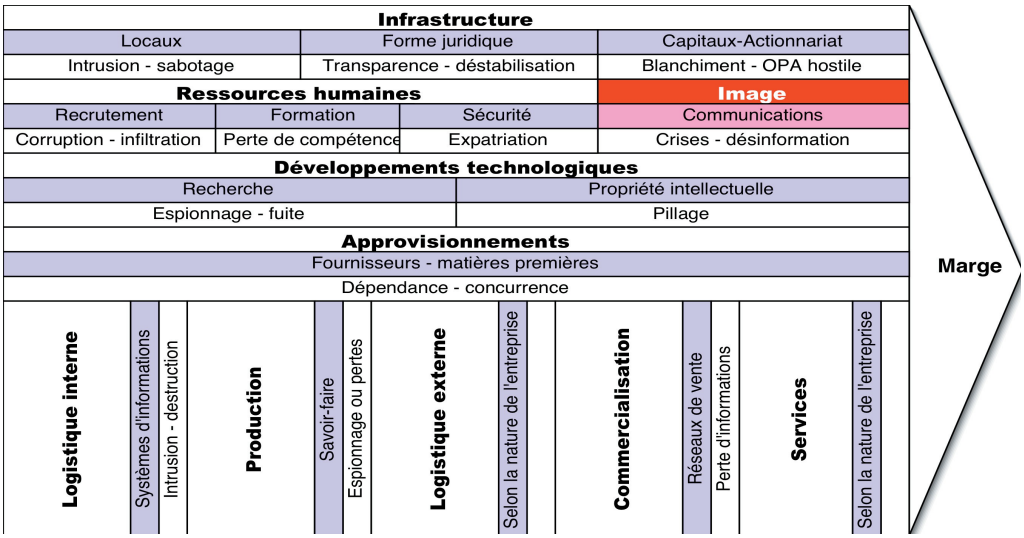

Figure 1 : Lecture « Intelligence économique » des risques liés à la chaîne de la valeur (Rapport au Premier Ministre, Bernard Carayon, 2003)

2. Lorsque l'on a ainsi pris conscience de ce que l'on avait à protéger et des menaces auxquelles on est confronté, on peut adopter au quotidien des règles de conduite simples et les adapter aux situations rencontrées.

A l'accueil

• contrôler l'identité des visiteurs ;
• éviter de faire venir au même moment les visiteurs qui n'ont pas à se rencontrer ;
• éloigner le standard de la salle d'attente et éviter que les visiteurs puissent entendre des informations confidentielles (noms de clients ou fournisseurs).

Lors de visites ou séjours dans l'entreprise

• faire porter un badge d'identification aux visiteurs et s'assurer qu'ils restent toujours accompagnés ;
• éviter de laisser à portée de vue des informations confidentielles (posées sur le bureau, affichées au mur, au tableau de la salle de réunion, sur l'écran d'ordinateur…) ;
• organiser des parcours de visite qui ne dévoilent aucune information sensible (équipements spécifiques, capacités de production, laboratoires…) et prévoir à l'avance les documents à remettre aux visiteurs ;
• bien encadrer le personnel non permanent (stagiaires, intérimaires, prestataires…) et ne pas les laisser accéder aux informations et lieux stratégiques.

Au téléphone

• se méfier des interlocuteurs inconnus et ne pas leur répondre sans au préalable vérifier leur identité et la vraie finalité de leur appel ; au besoin, demander d'envoyer un écrit de confirmation (courrier ou fax avec en-tête de l'entreprise, mail d'entreprise) ;
• éviter de tout dire au téléphone (ses nouveaux projets, sa politique tarifaire, sa stratégie, ses parts de marché) et demander à rencontrer votre interlocuteur.

En déplacement

• ne pas avoir de conversation de travail dans les transports (taxi, voiture de location, avions, trains, métros…) ni dans les lieux publics (salles d'attente, restaurants, hôtels, salons professionnels…) ;
• ne pas dévoiler tous ses projets à ses fournisseurs, ni à ses clients : ils sont, tout comme pour vous, une source intéressante pour les concurrents ;
• avant de faire une intervention publique, s'assurer que ses présentations ne contiennent pas d'informations stratégiques ;
• éviter de sortir des documents confidentiels hors de l'entreprise ; si on a en a vraiment besoin, les stocker sur une clef USB que l'on garde sur soi et utiliser des codes (prix, devis, …) pour les rendre moins compréhensibles ;
• prévoir un portable réservé aux déplacements extérieurs que l'on transporte dans un sac discret plutôt que dans le sac d'origine du constructeur.

Dans l'entreprise

• lors d'un recrutement, vérifier les diplômes et l'expérience du candidat pressenti auprès de sources extérieures (cabinets de recrutement, anciens employeurs, organismes de formation) et inclure des clauses de confidentialité dans son contrat de travail ;
• sélectionner et travailler avec des partenaires (sous-traitants, prestataire informatique, cabinets d'étude de marché, d'audit, d'assurances, sociétés de traduction, transporteurs, sociétés de nettoyage…) dans un cadre contractuel ;
• s'assurer du bon fonctionnement des fermetures des locaux (portes, fenêtres) et les utiliser ;
• regrouper et protéger ses clefs de service (armoire ou coffret à clefs) ;
• rester discret sur les mesures de protection et les dispositifs d'alarme mis en place dans l'entreprise ;
• ne pas jeter tels quels des documents pouvant contenir des données sensibles (les détruire) ou des supports informatiques dont le contenu pourrait être récupéré ;
• s'assurer que les documents promotionnels, le site internet, les blogs de salariés ne laissent pas filtrer des renseignements confidentiels utiles à la concurrence ;
• définir une stratégie appropriée de propriété industrielle pour protéger ses innovations, produits ou savoir-faire (marque, secret industriel, brevet) et penser à protéger son nom de domaine (adresse internet de l'entreprise).

Sécurité informatique

• distinguer les profils utilisateurs à l'intérieur de l'entreprise et les droits d'accès associés ;
• choisir des mots de passe si possible de 8 caractères alphanumériques (hors dictionnaire et noms propres), les renouveler régulièrement et ne les communiquer à personne ;
• utiliser des logiciels de protection et les mettre à jour : anti-spam, antivirus, firewall (pour un besoin standard, la solution proposée par le provider Internet peut convenir) ;
• pour les réseaux sans fil (WiFi, *Bluetooth*, téléphonie mobile), activer les procédures de sécurité intégrées (authentification, chiffrement, liste d'équipements « amis » autorisés) et désactiver par défaut les fonctions de liaison sans fil ;
• après usage d'un photocopieur numérique, effacer les données en mémoire ;
• stocker les informations sensibles sur un poste informatique non connecté à internet ;
• sauvegarder régulièrement ses données et placer ses sauvegardes à l'abri (tentatives d'intrusion, incendies et inondations) dans un local extérieur à l'entreprise.

3. Par-delà ces bonnes pratiques, on peut aller plus loin et bâtir une politique de sécurité globale qui prenne en compte toutes les étapes du cycle de vie de l'information (acquisition, création, communication, stockage, mise à jour, destruction). Cette politique de sécurité couvrira des aspects variés, tels que :

- nomination d'un responsable sécurité et identification des responsabilités dans l'entreprise,
- classification des informations en fonction de leur degré de sensibilité (rares, vulnérables, stratégiques),
- définition des règles d'accès (bâtiments, informatiques, internet…),
- rédaction et diffusion de procédures de sécurité quotidiennes,
- communication des mesures à adopter en cas d'incendie,
- rédaction et diffusion d'une charte précisant les usages autorisés des équipements informatiques et de communication mis à la disposition des collaborateurs,
- gestion des risques et politique d'assurances,
- organisation d'une cellule de crise et d'un plan de continuité d'activité...

Bien sûr, on adaptera cette politique à sa situation et on veillera à ne protéger que ce qui doit l'être : il ne s'agit pas de tout verrouiller. On veillera particulièrement au facteur humain : il est ainsi essentiel d'obtenir l'appui de la direction de l'entreprise et de mettre en œuvre des actions de sensibilisation et de formation du personnel. Enfin, cette politique de sécurité doit également être suivie dans le temps, malgré les changements de personne, d'équipements ou d'organisation.

A quel service de l'Etat s'adresser en cas de problème ?

Gendarmerie nationale
• Vous êtes victime d'un vol, d'une extorsion,
• Vous vous sentez exposé, vulnérable.
Direction centrale du renseignement intérieur (DCRI)
• Vous souhaitez être sensibilisé à la protection de vos informations et savoir-faire,
• Vous pensez être la cible d'ingérences étrangères,
• Vous êtes confronté à une menace spécifique (dérives sectaires, atteinte à la réputation...),
• Vous détenez un renseignement de sécurité.
Direction de la protection et de la sécurité de la défense (DPSD)
• Vous devez élaborer des mesures de protection de vos installations,
• Vous désirez une sensibilisation ou un soutien en matière de protection du patrimoine industriel.
Cible particulière : entreprises travaillant pour la défense nationale

Pour aller plus loin :

- Portail de la Sécurité informatique (ANSSI)
- Guides de l'Institut de sécurité de l'information du Québec (ISIQ)
- CLUSIF
- IE et Protection du Patrimoine (MADIE – Association HEC)