CHUUUT ! Les murs ont des oreilles et des yeux ! Les ordinateurs aussi.

© Gorodenkoff / Adobe Stock

Préservez l'intelligence et la connaissance de votre entreprise !

Il ne suffit pas de protéger ses biens matériels contre le feu, la malveillance ou encore les risques naturels, pour assurer l'avenir économique de votre entreprise. Tout le monde pense aux dommages aux bâtiments, aux équipements, aux stockages et processus de fabrication, mais les risques extra-financiers et « immatériels » peuvent tout autant peser sur la pérennité d'une entreprise. Grand groupe, start-up, petite ou moyenne entreprise (PME), ou même organisme de recherche, tous sont exposés à la perte de données, du résultat de recherches ou à la diffusion incontrôlée de leur savoir-faire.

Une bonne gestion implique de protéger tous les atouts économiques, technologiques et scientifiques de l'entreprise ou de l'organisme, afin de réduire les risques de captation, de diffusion et d'exploitation frauduleuse ou malintentionnée. Quelles sont les conséquences du vol ou de la perte de données, de brevets, d'une propriété intellectuelle, du vol par un acteur extérieur malveillant, un concurrent ou un candidat investisseur inamical ?

Ces données ou informations circulent sous forme de « bruits », d'articles, voire de communiqués. Une veille attentive peut les dépister et générer une réaction correctrice de votre part. Mieux vaut les éviter et débusquer les sources possibles. Est-ce un simple bavardage intempestif ou une interview mal dirigée, la réponse à une question illégitime de personnes extérieures ?

La gestion des informations internes et externes constitue la pierre d'angle de toute politique de protection de vos connaissances tant technologiques, économiques que financières.

UN PLAN COORDONNÉ DE GESTION DES INFORMATIONS

La sécurité économique ne peut se limiter à quelques mesures techniques ou organisationnelles ponctuelles. Son efficacité dépend de la mise en place d'une véritable politique de préservation de ses intérêts, de son savoir-faire et de son capital d'informations – à l'instar du plan global de prévention et de sécurité au travail, ou de prévention des incendies.

Le plan repose sur des mesures organisationnelles et comportementales basiques, chaque risque ou vulnérabilité fera l'objet d'un plan d'action et de procédures spécifiques.

Mesures organisationnelles :
- Établir un diagnostic général avec identification des risques, des menaces et des vulnérabilités.
- Affecter des moyens humains, financiers, matériels, etc. adaptés.
- Nommer un responsable de la sûreté et de la sécurité des systèmes d'information.
- Impliquer l'ensemble du personnel via des procédures adaptées.
- Définir des objectifs prioritaires et suivre leur réalisation au travers d'audits et de tableaux de bord.
- Mettre à disposition du personnel, des supports de communication et de sensibilisation, simples, accessibles à tous et actualisés.
- Mettre en place des actions de sensibilisation et de formation adaptées à chaque département ou service.
- Organiser un dialogue régulier entre les responsables sûreté/intelligence économique et les cadres dirigeants.

Mesures comportementales :
- Se rendre accessible et à l'écoute sur toutes les questions de sécurité formulées en interne.
- Ne jamais sous-estimer l'importance d'un fait inhabituel ou d'un incident de sécurité.
- Faire remonter tout fait inhabituel ou incident au responsable.

IDENTIFIER LES DONNÉES ET INFORMATIONS PRIORITAIRES À PROTÉGER

Les multiples sources d'informations disponibles dans une entreprise ne peuvent être contrôlées de la même manière, faute de provoquer la paralysie. Une analyse devra au préalable identifier les sources et les types d'informations (données) vraiment essentielles, qu'elles soient produites en interne ou qu'elles émanent de tiers (fournisseurs, clients, partenaires financiers, etc.).

Mesures organisationnelles :
En concertation avec l'ensemble de l'équipe de management – tous les services ou départements sont impliqués :
- collecter et identifier les types de données/informations détenues ;
- identifier la sensibilité des informations en fonction du préjudice potentiel pour la vie de l'entreprise (impact faible, moyen, fort) en cas de divulgation, perte ou destruction.

  Questions à se poser :
  La perte, la destruction ou la divulgation de cette information sont-elles de nature à engendrer ... :
  - ... un dommage pour l'activité concernée ou le déroulement d'un projet ?
  - ... un impact financier ou technique ?
  - ... un impact sur le personnel ?
  - ... un impact en matière d'image et de réputation ?
  - ... une incidence sur la confiance des actionnaires ou des banques ?
  - ... une perte de confiance d'un client ou d'un partenaire important ?
  - etc.

- évaluer la fréquence de réalisation du risque, et préciser son impact humain ou technique.

  Questions à se poser :
  - Qui a accès à cette information - en interne et en externe ?
  - Les droits d'accès à l'information sont-ils régis (très limités, restreints, libres) ?
  - Comment cette information est-elle conservée ? Une sauvegarde régulière est-elle
  - prévue ?
  - L'information doit-elle être transportée sur un support numérique ou autre ?
  - Comment les échanges d'informations sont-ils opérés ?
  - etc.

- analyser les résultats et les transposer dans un tableau selon le niveau de risque potentiel ;
- appliquer à chaque type de données les mesures de protection définies dans le plan de gestion de l'information (accès, diffusion, reproduction, archivage, destruction, etc.). Les informations les plus sensibles doivent bénéficier d'une protection renforcée.
- revoir et actualiser régulièrement l'analyse et les mesures de protection envisagées ;
- Cette démarche est commune aux autres procédures de prévention et de sécurité en cas de sinistres (incendie, inondation, catastrophe naturelle, etc.).

Tableau 1 : Exemple de grille d'estimation de la criticité

			IMPACT / GRAVITÉ				
			Catastrophique	Majeur	Modéré	Mineur	Insignifiant
			5	4	3	2	1
PROBABILITÉ D'OCCURRENCE / FRÉQUENCE	Très forte	5					
	Forte	4					
	Moyenne	3					
	Faible	2					
	Très faible	1					

ÉVALUATION DES RISQUES :

- Rouge : niveau de risque trop élevé. Le risque est présumé trop important et sa maîtrise est problématique. Il convient de réduire le risque à un niveau acceptable, en formulant des propositions de réduction complémentaires tel un plan de protection adapté qui permet de sortir de la zone rouge, assorti de mesures de gestion de l'information (accès, diffusion, reproduction, archivage, destruction, etc.). Les informations les plus critiques doivent toujours faire l'objet d'une protection renforcée ;
- Jaune : niveau de risque élevé. Il convient de réduire le risque à un niveau plus faible ;
- Vert : niveau de risque intermédiaire. Les mesures de maîtrise des risques sont jugées acceptables. Une démarche d'amélioration continue reste cependant pertinente en vue d'atteindre, dans des conditions économiquement acceptables, un niveau de risque aussi bas que possible ;
- Gris : Niveau de risque moindre.

Source : La sécurité économique au quotidien - voir références en fin d'article.

GÉRER LES ARCHIVES PAPIER ET NUMÉRIQUES

Au même titre que les documents vivants, les archives sont sources d'informations pour qui recherche des informations techniques, commerciales ou humaines sur vos activités.
Outre les archives obligatoires, d'autres formes de documents comme les notes manuscrites, courriers électroniques, fichiers numériques, bordereaux, rapports et synthèses, méritent votre attention et la mise en place de mesures de protection.

Mesures organisationnelles :
- plan de classement et d'archivage des documents dont le contenu est jugé sensible ;
- formation du personnel à la gestion et à la sécurité des sauvegardes des documents (niveau de sensibilité, durée de vie) ;
- procédure de suivi et de traçabilité de la consultation des différents documents archivés ;
- externalisation des archives numériques – imposer par contrat les conditions de traitement et de divulgation aux différents partenaires ;
  - conditions et clauses spécifiques prévoyant la conservation et/ou la destruction sécurisée des disques durs, du matériel informatique (serveur, ordinateur, imprimante, télécopieur, tablette...)

Note :
En raison des possibilités actuelles de travail à distance, sensibiliser le personnel au danger des supports d'archivage privés. Mieux vaut les interdire, et fournir et gérer des supports vérifiés par vos soins.

Mesures techniques :
- locaux sécurisés et adaptés pour la conservation de documents papier et de supports numériques (contrôle des accès, conditions climatiques intérieures (humidité, température, ventilation), systèmes de protection contre les incendies adaptés, contre l'inondation, selon les conclusions de l'analyse des risques) ;
- les données les plus sensibles sont conservées séparément dans une chambre forte, un coffre-fort. Les copies et backup sont conservés dans des lieux séparés ;
- mettre à disposition un broyeur à coupe croisée pour détruire de manière sécurisée les documents sensibles (papiers, CD, DVD, etc.).

Veiller à la destruction sécurisée des documents :
- s'équiper d'un broyeur à coupe croisée pour détruire les supports d'informations sensibles sur papier, CD, DVD, etc.) ;
- documents sensibles (papiers, CD, DVD, etc.) ;
- équiper les postes de travail d'un logiciel d'effacement sécurisé ;


© VZ_Art / Adobe Stock

- détruire de façon sécurisée les mémoires internes des équipements informatiques en fin de vie ou en fin de contrat (imprimante, fax, photocopieur, etc.) ;
- détruire de façon sécurisée les prototypes et résidus de matériaux innovants mis au rebut.

MAÎTRISER LA COLLECTE DES INFORMATIONS ET DE LA COMMUNICATION

La maîtrise de l'information sous-entend la maîtrise de la communication. Mal maîtrisée, elle peut conduire à une fuite d'informations stratégiques et préjudiciables. Il faut toujours évaluer la sensibilité des informations communiquées sur le plan professionnel ou personnel, interne et externe. Cette maîtrise implique la mise en place d'une structure et la définition claire des devoirs, et responsabilités des différents intervenants au sein des cellules de communication au sein de l'organisme.

Mesures organisationnelles :
- une communication doit être dirigée :
  - quelle(s) fonction(s) ou personne(s) est/sont autorisée(s) à s'exprimer et communiquer en fonction du type de communication ou d'informations ?
- une communication doit être maîtrisée :
  - évaluer si la demande de visite ou d'interview est légitime et s'inscrit dans la stratégie d'activités ou de communication de l'entreprise ;
  - avertir préalablement la direction et/ou le responsable de la communication de toute demande de contacts avec les médias (presse, ou rédacteur d'un site internet ou médias sociaux). Certaines demandes peuvent aussi émaner d'analystes, d'enquêteurs ou de concurrents par exemple. Les interlocuteurs sont-ils légitimes ?
  - faire préciser le thème et l'objectif de la visite ou de l'interview. Si possible, demander à connaître les questions à l'avance et s'assurer d'un droit de relecture avant publication ;

- peser les conséquences, positives mais aussi négatives, des informations communiquées (orales ou écrites).

- préparer les messages à divulguer lors d'événements (salons, conférences, lancement de produits, colloques etc.) ;
  - fixer les objectifs et les préciser à vos collaborateurs ;
  - identifier les informations sensibles et éluder les questions hors contexte ;
  - ne communiquer que les informations utiles à l'activité, aux objectifs ou aux relations professionnelles ;
- limiter les coordonnées personnelles sur les cartes de visite, signature électronique, etc. aux informations strictement nécessaires ;
- sensibiliser les collaborateurs aux risques de demandes urgentes, inhabituelles ou hors procédures. Celles-ci peuvent cacher une manœuvre détournée pour obtenir une information sensible. Prévoir une procédure d'urgence ;
- mettre en place une procédure de communication d'urgence, validée par l'entreprise, pour diriger la réaction à un message négatif ou inapproprié ;
- s'assurer de la légitimité des démarches d'audits, de contrôle, de réparateurs ou de visiteurs ayant besoin d'accéder à des données confidentielles ou sensibles :
  - vérifier l'identité des intervenants auprès des administrations, organismes de contrôle ou fournisseurs, auxquels ils prétendent appartenir ;
  - fixer un rendez-vous préalable, demander la carte professionnelle, … ;
  - exiger une lettre de mission.

- veiller à la réputation de l'entreprise :
  - vérifier ce qui se dit ou s'écrit sur votre entreprise, ses dirigeants ou ses employés.
  - Effectuer une veille régulière sur les principaux médias et réseaux sociaux ;
  - toujours réagir et de manière concertée aux dénigrements, « cyberattaques » ou toute autre critique à l'encontre de l'entreprise ;
  - corriger l'information et tenter d'identifier la source.

Jeanine DRIESSENS
ANPI - Information & Media Center

Source : Cet article est largement inspiré de « La sécurité économique au quotidien » - Ministère de l'économie et des finances et de la relance (France) - Service de l'information stratégique et de la sécurité économiques (Sisse) - Direction générale des Entreprises (DGE) / Novembre 2021 Fiches A1, A3, C3 et F1

© Thapana_Studio / Adobe Stock