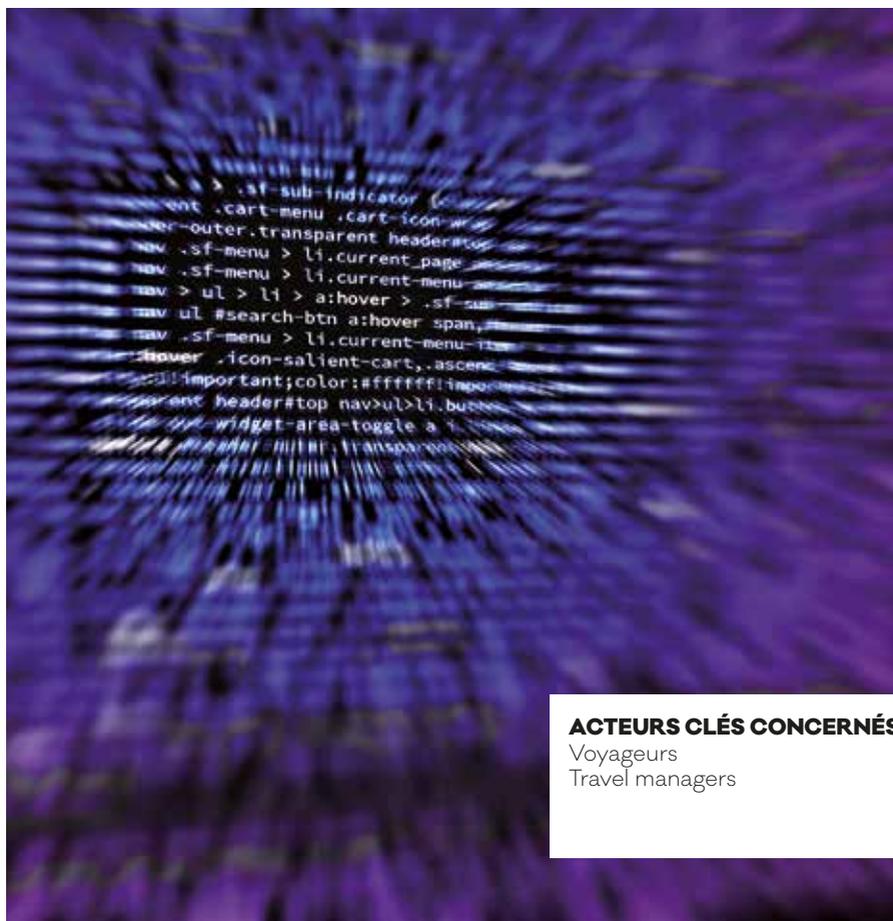


LA PROTECTION DE LA DONNÉE

PRINCIPAUX ENSEIGNEMENTS

- La **sécurité des données est un enjeu majeur** pour les entreprises et leurs collaborateurs.
- **Plusieurs types de risques sont à distinguer** : stratégie de l'entreprise / espionnage industriel / vols de données bancaires / blocage des systèmes en vue d'une demande de rançon.
- Le **risque zéro n'existe pas**.
- La **définition d'une stratégie et l'identification des risques** sont primordiales.



ACTEURS CLÉS CONCERNÉS
Voyageurs
Travel managers

CE QU'IL FAUT SAVOIR

On peut définir « la sécurité économique » 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 économique*, préfecture de Seine-Maritime).

Pourquoi et comment protéger ses données ?

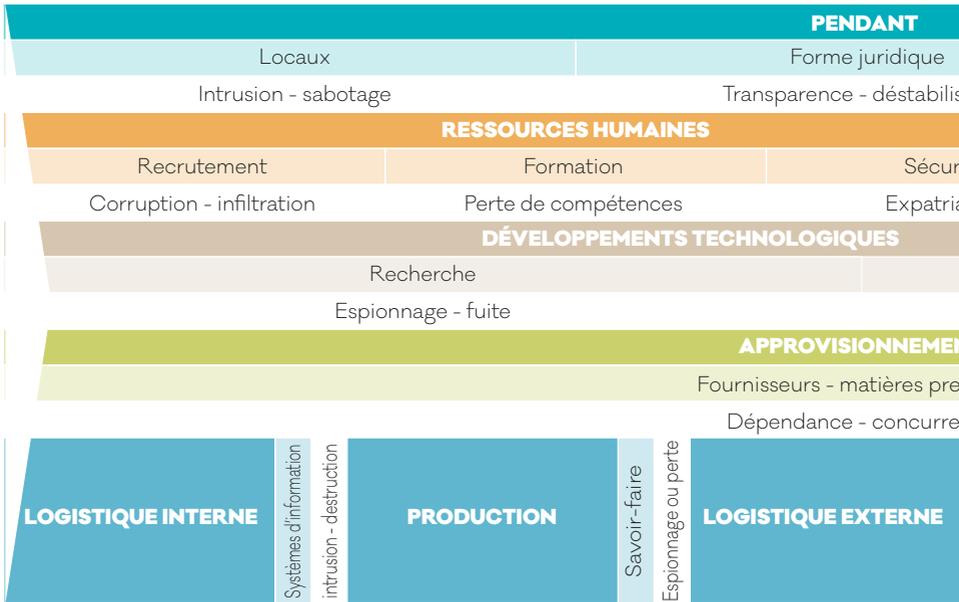
Même si ce sujet est de plus en plus présent dans l'actualité et qu'un nombre toujours plus grand de personnes prend conscience de l'importance et de la sensibilité des données personnelles, il y a encore beaucoup trop d'internautes qui sous-estiment la valeur de celles-ci. Entre les données marchandes pour les entreprises, celles stratégiques sur les utilisateurs, le vol de données bancaires et l'espionnage de masse des gouvernements, **il devient plus que nécessaire d'apprendre à sécuriser sa vie numérique**. Il existe d'ailleurs des gestes simples pour se protéger un minimum et s'éviter bien des soucis.

Les grandes et moyennes entreprises sont souvent très avancées en matière de sécurité (mises à jour régulières, antivirus, pare-feu...). Les comportements des collaborateurs peuvent pourtant mettre en péril ces mesures avec la navigation et les achats sur le web ou l'ouverture d'emails et de pièces jointes (apprenez à être méfiant sur les courriels et pièces jointes reçus qui peuvent être des virus)².

En plus des problèmes de virus, les principaux risques liés à la sécurité sont les suivants (Cf. schéma ci-dessous).

En matière de protection des données, la première étape consiste à repérer les informations stratégiques et les risques associés de l'entreprise.

Figure 1 : Lecture «intelligence économique» des risques liés à la chaîne de la valeur (rapport au premier ministre, Bernard Caravon, 2003)



Il faut donc faire l'inventaire de toutes ses informations sensibles ou confidentielles (orientations stratégiques, actions d'influence, fichiers et prospects clients, listes des fournisseurs, contrats, données comptables, paies, dossiers du personnel, organigramme détaillé de l'entreprise, brevets, plans, procédés de fabrication, codes sources, résultats de veille concurrentielle...) et recenser les ressources du système d'information de l'entreprise (ordinateurs fixes et portables, accès à internet, messageries électroniques, logiciels, clefs USB, *WiFi*, *Bluetooth*, téléphones fixes et portables, télécopieurs, photocopieurs, armoires et locaux d'archivage...).

Quelques règles limitent les risques de perte de données et confortent votre sécurité informatique :

- **distinguez les profils utilisateurs** à l'intérieur de l'entreprise et les droits d'accès associés ;
- choisissez des mots de passe de huit caractères alphanumériques (hors dictionnaire et noms propres), **renouvelez-les régulièrement et ne les communiquez à personne** ;
- **utilisez des logiciels de protection et mettez-les à jour** : anti-spam, antivirus, *firewall* (pour un besoin standard, la solution proposée par le fournisseur d'accès internet peut convenir) ;
- **activez les procédures de sécurité intégrées** (authentifications, chiffrements, listes d'équipements « amis » autorisés) **pour les réseaux sans fil** (*WiFi*, *Bluetooth*, téléphonie mobile) et désactivez par défaut les fonctions de liaison sans fil ;
- **effacez les données en mémoire** après usage d'un photocopieur numérique ;
- stockez les informations sensibles sur **un poste informatique non connecté à internet** ;
- **sauvegardez régulièrement vos données** et placez ces sauvegardes à l'abri (tentatives d'intrusions, incendies et inondations) dans un local extérieur à l'entreprise.

Lors des déplacements professionnels, quelques règles spécifiques peuvent être appliquées.

