CHAPITRE 5 : LA PROTECTION DU PATRIMOINE IMMATERIEL

I- Les formes de menaces

Par menace, on entend tout acte malveillant commis à l'encontre d'une entreprise avec la ferme intention de mettre en danger son organisation, ses salariés, sa réputation ou de s'approprier de manière illégale une partie de ses biens ou de ses droits de propriété.

Il existe différentes formes de menaces auxquelles les entreprises sont soumises qu'elles soient des multinationales ou des PME.

1- L'atteinte à la réputation

La réputation est un actif essentiel pour l'entreprise pouvant représenter jusqu'à 70% de sa valeur. Or, la réputation des organisations est extrêmement fragile pout trois raisons :

- Dans une économie du savoir, l'entreprise est particulièrement vulnérable aux agressions informationnelles.
- A l'ère des TIC, la guerre de l'information fait rage et la réputation des entreprises est malmenée par la généralisation des nouveaux medias (réseaux sociaux, blogs, SMS…), rendant les attaques plus rapides et plus agressives.
- Le nombre important d'organisations cherchant à lui nuire

La réputation de l'entreprise peut donc être facilement entachée. Les attaques s'expriment généralement par des appels au boycott ou des rumeurs disséminées sur le Net…

2- Les vols et sabotages des installations

Les vols représentent la majorité des actes criminels et dépassent numériquement les autres infractions.

3- Les escroqueries économiques et financières

L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale afin de s'approprier des fonds, des valeurs ou un bien quelconque.

Le développement du commerce en ligne et des messages électroniques a fortement contribué à l'évolution des escroqueries.

4- La contrefaçon

La contrefaçon est une atteinte au droit de la propriété intellectuelle. Il s'agit d'imiter l'apparence d'un produit dans le but de faire croire au consommateur qu'il achète le produit original

5- Les fuites d'information

La fuite d'information quel que soit la forme qu'elle revêt, a pour fondement d'intéresser un concurrent ou un individu souhaitant nuire à l'intérêt de l'acteur ciblé.

6- La cybercriminalité

Elle désigne l'ensemble des infractions pénales commises via les réseaux informatiques, et plus particulièrement Internet.

II- La protection des données

Face aux différentes menaces identifiées, l'entreprise se doit de mettre une stratégie de protection de l'information.

La protection de l'information est aussi appelée **sécurité économique.** Les firmes sont confrontées à leurs concurrents sur le marché. Elles doivent intégrer dans leurs stratégies un processus de sécurité économique de leur patrimoine informationnel (patrimoine immatériel) comprenant la surveillance et la protection de savoir-faire ainsi que leurs techniques clés.

Le capital immatériel renferme le capital savoir, la gestion des connaissances et leur utilisation. Les synergies qui en résultent animent une intelligence collective qui favorise la prise de conscience des salariés face aux opportunités et menaces d'un environnement où « l'économiquement pur » devient de plus en plus minoritaire.

Ce patrimoine est constitué d'éléments de l'entreprise transmissible d'un employé à un autre ou d'un service à un autre. Ce sont entre autres les savoirs, savoir-faire, les pratiques, les clients, les partenaires, la marque…

Pour être compétitives, les entreprises doivent protéger leur patrimoine immatériel, car les actifs immatériels sont de puissants facteurs de croissance dans les économies modernes.

Le processus de sécurité économique (S.E) consiste d'une part à identifier les éléments à protéger ainsi que les menaces tant externes qu'internes qui peuvent peser sur le patrimoine de l'entreprise et d'autre part à faire comprendre que ce patrimoine est de plus en plus immatériel, qu'il nécessite des savoirs faire spécialisés, et que certaines circonstances de crise mal maitrisées peuvent engendrer des pertes considérables.

La sécurité économique permet à l'organisation de freiner l'efficacité du dispositif d'intelligence économique de ses concurrents. Elle comprend les étapes suivantes :

- **Classification de l'information** : identification des informations sensibles
- **Protection des accès** : définition des règles de mesures d'accès physiques et logiques
- **Surveillance du dispositif anti fuite** : mise en œuvre de solution de sécurité
- **Sensibilisation** : implication des collaborateurs
- **Contrôle et détection** : surveillance des vecteurs de fuite