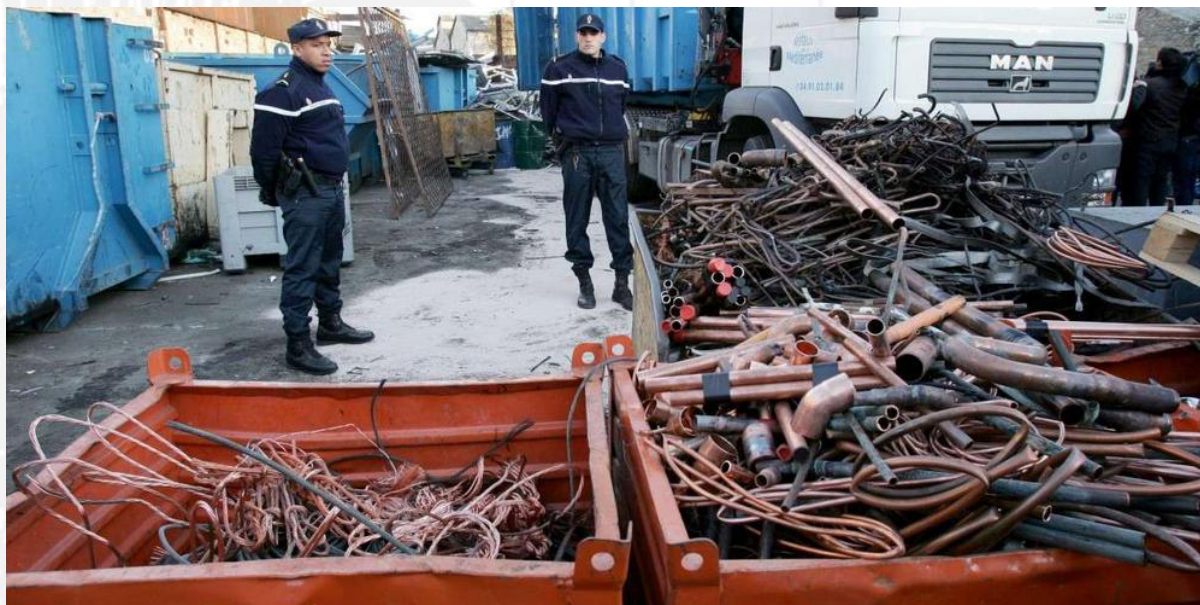


INTRUSION ET LA MALVEILLANCE



Sûreté ou sécurité ?

La SÉCURITÉ consiste à mettre en œuvre des moyens afin de prévenir les défaillances humaines et techniques (sprinkler, plans de circulation, exercices d'évacuation, ...). La SÛRETÉ, en revanche, a pour objectif de prévenir les actes de malveillance délibérés (attentats, intrusions, occupations des locaux, espionnage industriel, cyberattaques, vols de biens, kidnappings, vandalismes, agressions verbales et physiques...).

Toute entreprise, quelle que soit son activité ou sa taille, est potentiellement une cible d'acte de malveillance.

La sûreté en entreprise qui a pour objectif de garantir sa pérennité et la protection de ses collaborateurs, est un véritable enjeu pour les chefs d'entreprise. Il devient en effet essentiel de mettre en place un dispositif de management des risques sûreté visant à réduire les menaces et les actes de malveillance.

Les systèmes de management des risques sûreté en entreprise

Ainsi, au même titre que l'évaluation des risques sécurité, c'est le rôle de chaque entreprise d'identifier les besoins en sûreté et d'évaluer les menaces internes et externes, de développer des politiques, des plans, des procédures et des moyens de protections afin de pouvoir maîtriser ces menaces.

Quels sont les intérêts d'une telle politique de sûreté en entreprises ?

- La protection de leurs collaborateurs ;
- La protection de leurs données et de leur image de marque ;
- La protection de l'environnement (pollutions de l'air, de l'eau, ...).

Quels sont les points essentiels pour la mise en œuvre d'un système de management des risques ?

- Réaliser une évaluation des risques : quelles sont les cibles de mon entreprise ? Quels sont les scénarios de malveillance potentiels ?...
- Déployer des moyens de protections : moyens humains (ex. : gardiennage), technique (ex. : vidéosurveillance), procédures, information et formation du personnel, exercices de confinement, ...
- Assurer une veille sûreté permanente et contrôler régulièrement les moyens de protection mis en place.

Quels sont les chiffres de la sûreté ?

Selon le "Traité Pratique de Sûreté Malveillance" du CNPP (2018) :

- 77% des accidents liés à la malveillance se caractérise par un incendie ;
- 7 816 vols de métaux ont été recensés en 2015, en France ;
- 67% des entreprises en 2018 ont été touchés par un « événements cyber »

Sûreté en entreprise : que dit la réglementation ?

La Norme

Contrairement à la sécurité, la sûreté en entreprise n'est pas encore normée... mais cela devrait très prochainement changer avec le projet de norme managériale ISO 22342 sur le plan de sûreté.

Le Code du Travail

Ce dernier encadre les moyens à mettre en œuvre, par les entreprises, dans le cadre de l'obligation de sécurité et de sûreté des employés (article L. 4121-1 du Code du travail).

Le Code pénal

Si un employeur ne respecte pas son devoir de protection en manquant au respect des règles de sûreté et de sécurité relevant du Code du travail et que ce manquement cause un préjudice, il peut s'exposer à des sanctions pénales (amendes et peines d'emprisonnement).

Dans le cas des sites Seveso

La réglementation concernant la protection des sites classés Seveso est plus précise, notamment, avec l'accord du 18 juillet 2016, relatif à la santé, à l'amélioration des conditions de travail, à la sécurité et à la sûreté, qui aborde la notion de « dossier de sûreté » que toutes entreprises extérieures prestataires de sites classés Seveso devront fournir.

Dans le cas des cyberattaques

Pour y faire face, la réglementation a mis en place une organisation qui regroupe les opérateurs d'importance vitale (OIV), privés ou publics.

Ce sont les opérateurs qui de part leur activité et en cas de cyberattaque mettraient en péril les habitants ou paralyseraient la France (exemples : activités tels que la santé, l'eau, l'électricité et le gaz, l'alimentation, les hydrocarbures, les transports, les télécommunications, l'industrie, la finance, le nucléaire, ...).

Si une entreprise fait partie des OIV, elle est informée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et doit donc répondre à des obligations en matière de sécurité informatique.

Par ailleurs, l'article 22 de la loi de programmation militaire (loi n° 2013-1168 du 18 décembre 2013), impose aux OIV le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent : les systèmes d'information d'importance vitale (SIIV).

Face aux multiples menaces de malveillances auxquelles font face les entreprises, il devient donc important d'anticiper et de maîtriser les risques de malveillance afin d'en limiter les conséquences. Au même titre que la sécurité, les entreprises doivent mettre en place une organisation permettant de prévenir les risques de sûreté en entreprise.

Les 5 règles d'or pour prévenir les actes de malveillance

Règle n°5 : renforcement des contrôles d'accès

Grâce à la technologie actuelle, des solutions innovantes avec un contrôle d'accès renforcé existent. Infrarouge, digitale ou à carte. Seules des personnes habilitées peuvent avoir accès :

- filtre par personne autorisée, habilitée,
- et/ou par zone
- et/ou par période horaire
- avec traçage nominatif des différents mouvements.

Règle n°4 : mettre en place un système anti-intrusion

Alarme anti-intrusion, vidéosurveillance, système de détection de chaleur... Il est important d'installer selon vos besoins des systèmes de protection permettant d'intervenir rapidement en cas d'intrusion. Un dispositif avec un système de vidéosurveillance permet d'agir encore plus vite.

Règle n°3 : protéger les accès

Isoler les zones sensibles, limiter les stockages à l'air libre, installer des clôtures avec un ajout de barbelé au besoin... Réfléchissez comment matériellement, vous pouvez délimiter les accès afin d'empêcher l'intrusion et donc les actes de malveillance.

Règle n°2 : sensibiliser les forces de polices à vos installations dites « sensibles »

Lors de leur ronde, les forces de Police seront à même de surveiller plus efficacement s'ils sont au courant de certaines installations sensibles. Informez-les, ils pourront ainsi avoir un regard plus vigilant sur certaines zones.

Règle n°1 : réaliser un audit de vos failles pour mettre en place un plan d'action et de prévention

Avant de mettre en place ces règles, il est primordial de dresser un état des lieux, de définir vos besoins et d'établir un plan de recommandation permettant d'optimiser les investissements.

Des mesures pour lutter contre l'incendie doivent aussi être prises en compte car malheureusement lors d'un acte de malveillance, les accidents se soldent souvent par un incendie.