INGENIEURS ET SCIENTIFIQUES DE FRANCE

Les Cahiers

CAHIER N° 4

Conseils aux dirigeants PME-PMI

Comment protéger votre entreprise des fraudes, négligences ou malveillances

Sommaire

AVANT-PROPOS

La sécurité prend chaque jour une importance plus grande dans notre société et, en premier lieu, dans les entreprises, pour leurs dirigeants et leurs personnels.

Les professionnels s'efforcent, depuis de nombreuses années, de réagir face à ce défi et y réussissent globalement, quelle que soit l'émotion légitime provoquée par une catastrophe toujours possible puisque le « risque zéro » demeure inaccessible.

Les pouvoirs publics ont aussi pris leur part dans cette évolution en tenant compte des progrès des techniques et de points de vue diversifiés pour renforcer les lois et règlements ainsi que les contrôles qui peuvent apporter, de fait, des conseils extérieurs utiles.

Le comité d'experts mis en place par les Ingénieurs et Scientifiques de France (IESF) à la suite de la catastrophe de Toulouse du 21 septembre 2001, a réexaminé l'ensemble des problèmes posés, en liaison avec de nombreux partenaires concernés dont les administrations de l'Etat. Ses propositions sont présentées dans son rapport final disponible sur le site des IESF à l'adresse :

http://www.cnisf.org

puis à la rubrique Bibliothèque – Rapports, études – Maîtrise de la sécurité industrielle (2004)

Le président des IESF a ensuite demandé un nouvel approfondissement de cette réflexion sur la maîtrise de la sécurité afin de définir de nouvelles voies de progrès. Il est ainsi apparu que l'abondance des règles en vigueur, si justifiées soient-elles, ne facilitait pas forcément la prise en compte du facteur humain. Il est pourtant essentiel, en particulier dans les PME où, le plus souvent, l'homme est, au centre de l'Entreprise.

En outre, les professionnels de l'assurance ont fait remarquer que les conséquences des négligences, fraudes et malveillances, qu'elles soient d'origine interne ou externe à l'entreprise, étaient la cause de nombreux incidents et accidents. En France, la prise de conscience reste trop souvent limitée voire occultée. A l'opposé, dans les pays comme l'Angleterre, où les dirigeants s'attaquent directement aux problèmes en informant largement le personnel et en le faisant participer à la recherche des solutions et à leur mise en œuvre, des résultats positifs ont été obtenus.

Dès lors, le comité a estimé nécessaire d'alerter les dirigeants de PME et de leur proposer une méthode simple et adaptable à chaque cas concret ainsi que des solutions pour faire face aux risques créés par ces fraudes, négligences et malveillances. Tel est l'objet du présent document.

Il est, sans doute, nécessaire de préciser que le comité ne s'est pas tenu à une définition juridique de la PME. Il a estimé que ses propositions s'appliquaient de façon préférentielle aux structures regroupant entre 20 et 500 personnes au sein desquelles travaillent plus du quart des salariés et 27,4% des ingénieurs diplômés (Source CEFI pour 2004). Dans ces structures, les relations interpersonnelles y jouent un rôle majeur tout en nécessitant une organisation précise et inévitablement complexe. Cependant, les dirigeants d'entreprises, qu'elles soient plus petites, ou plus grandes, pourront aussi y puiser des sources d'inspirations utiles.

Je tiens à remercier tous les membres du comité qui ont apporté le fruit de leur expérience au cours de ces dernières années. Ils ont permis de réunir la documentation indispensable et ont accepté de confronter très librement des points de vue d'ingénieurs, d'experts en sécurité et en intelligence éco-

nomique, d'assureurs, d'informaticiens et de juristes.

Je remercie particulièrement les chefs et dirigeants d'entreprises, sur qui reposent finalement les progrès de la sécurité qui est aussi l'affaire de tous, qui ont accepté de témoigner sur des problèmes rencontrés en les situant dans le contexte de la vie de leur entreprise et de leurs personnels.

J'espère que ce guide sera largement diffusé et utilisé et que, rien n'étant parfait, des réactions nombreuses permettront de l'améliorer au fil des années.

Hubert Roux

Tout courrier concernant ce document est à adresser à : IESF - Président du Comité « Sécurité Industrielle » 7 rue Lamennais 75008 Paris ou par mail à mlecointe@cnisf.org

Les opinions exprimées dans ce document, n'engagent pas les organisations auxquelles appartiennent les membres du groupe de travail.

Dirigeants PME – PMI

Fraudes, négligences, malveillances mettent en péril vos entreprises
Comment lutter ?

Résumé du dossier

Vous trouverez dans ce document des réponses, témoignages et actions pratiques vous permettant d'engager des actions efficaces dans le but de protéger les biens matériels et immatériels de vos entreprises.

Dirigeants de PME, vous êtes concernés !

Soyez attentifs aux nombreux exemples cités dans la presse et autour de vous. Vous y verrez que des actes de négligences, fraudes et malveillances sont nombreux dans les entreprises.
En PME, d'autres priorités vous préoccupent. Vous vous reposez sur la taille de votre entreprise, la qualité des relations internes pour réfuter cette évidence. Pourtant, **en sous-estimant ces risques, vous fragilisez votre entreprise !**

Dirigeants de PME, vous n'êtes pas à l'abri ! Ces préjudices n'arrivent pas qu'aux autres !

Aucune entreprise n'est à l'abri, même si en France, le sujet reste encore tabou. Mais en prenez-vous la juste mesure ? Prenez connaissance de la cinquième édition de l'étude mondiale menée par Price Waterhouse en 2009 sur l'ampleur du phénomène de fraude dans les entreprises.
Tout dirigeant d'entreprise ne devrait pas se demander s'il peut être victime d'un tel préjudice, mais à quelle occasion celui-ci peut se produire.

Les conséquences peuvent être dramatiques

Négligence, fraude et malveillance revêtent différents aspects : incendie, vols, accidents, sabotage de machines, falsification de documents, copies de brevets, contrefaçon, débauchage de personnel, attaque du système informatique, … La liste est longue et les conséquences dramatiques :

- une enquête établit que, **même en étant très bien assurées, près de 3 entreprises sur 4, ne reprennent pas leur activité après avoir été victimes d'un incendie**.
- la revue Money Week indique que « **les dégâts de la cybercriminalité au Royaume-Uni sont évalués en 2009 à 30 milliards d'euros par année**, soit près de 1,9% du PIB 2009 du pays »

Négligences, fraudes et malveillances sont donc des risques élevés, pouvant provoquer pertes d'exploitation, détérioration de l'image, situations qui souvent peuvent vous être fatales.

Les principales menaces viennent autant de l'intérieur que de l'extérieur

La plus fréquente des menaces consiste à détourner du matériel de son circuit habituel. La seconde vise à détourner des fonds. Une autre forme de menace semble se répandre : le déclenchement d'incendie ou le sabotage de la production ou de machines dans un but de vengeance.
Il vous est peut-être difficile d'imaginer que cela puisse être vrai pour vous. Et pourtant !

L'efficacité des mesures de prévention repose avant tout sur votre degré d'implication.

L'implication du dirigeant est une condition impérative de l'efficacité du dispositif.
Vous devez décider de la mise en place d'une démarche dans le but de protéger vos biens. Votre implication est d'autant plus nécessaire que :

- **les donneurs d'ordre, veulent se garantir des défaillances possibles de leurs fournisseurs,**
- **l'âpreté de la concurrence fragilise votre entreprise si elle s'absente de son marché,**

Vous pouvez et devez agir selon une démarche pragmatique

Ces menaces représentent actuellement plus de 30 % du montant des sinistres. Certains pays en ont pris conscience et mis en place des plans d'actions qui ont fait régresser fortement les dommages.

La démarche pragmatique qui vous est proposée a pour objectifs de réduire les motifs d'incitation aux actions de négligences, fraudes et malveillances, et de maximiser l'efficacité de la gestion de vos risques.

Elle consiste à recenser les incidents et accidents auxquels votre entreprise a déjà été confrontée, à les analyser objectivement selon différents critères proposés, puis à faire l'analyse de la vulnérabilité de votre domaine afin de mieux définir vos politiques de sécurité et de propriété industrielle.

Armés des ces éléments, vous serez en mesure de définir vos priorités et votre plan d'actions pour maîtriser ces événements indésirables.

Cette démarche exige et justifie votre totale implication.

1 – De la nécessité d'une prise de conscience par les PME/PMI

La presse en parle

Extraits des journaux La Dépêche, L'Entreprise, Sud-Ouest et Le Progrès de Lyon (1)

Ils volent le numéro de compte de l'Elysée et tentent d'escroquer deux millions d'euros
Ils ont réussi à se procurer le numéro de compte bancaire de l'Élysée et l'organigramme de son service financier. Se faisant passer pour un membre de ce service, ils ont appelé la banque pour demander un virement de deux millions d'euros sur un compte à l'étranger, domicilié en Chine. Le banquier intrigué, a téléphoné à l'Élysée pour vérification, faisant ainsi échouer la tentative d'escroquerie. Selon le quotidien, l'Agence nationale pour les chèques-vacances est tombée dans le piège et aurait été escroquée de

Une société de meubles de 150 salariés, filiale d'un groupe. Pendant plusieurs années, le directeur général a détourné du matériel acquis par l'entreprise (mobilier, ordinateurs) et surpayé des fournisseurs contre reversement de commissions. Il s'est en outre octroyé, à l'insu du conseil d'administration, plusieurs augmentations de salaire et 2750 euros mensuels d'indemnités kilométriques.

La patronne d'une boutique-traiteur de luxe de trois salariés allait chaque soir déposer sa recette à la banque. Toujours pressée, elle demandait à son chargé de compte (le même depuis dix ans) de compléter les chèques laissés en blanc par les clients pour les mettre sur le compte de la société. Jusqu'au moment où l'employé de banque s'est mis à remplir les chèques à son ordre, détournant 53 400 euros en un an.

Vols de cuivre : c'est la ruée vers l'or rouge
En mars dernier, dans l'Armagnacais, c'est un bouilleur de cru qui se faisait délester de 500 kilos de cuivre lors d'un vol inédit : les malfrats étaient repartis avec deux alambics, soit environ 3 500 euros de matière brute pour eux, mais un préjudice de 50 000 euros pour le distillateur.

Le directeur d'une société importante, fabricant de pinces porte-électrodes et des accessoires de soudage industriel a pu constater par lui-même lors d'un salon spécialisé, en Allemagne : « des entreprises chinoises proposaient nos produits : le même nom, le même modèle, la même couleur » Et la même marque, puisque le logo de la société était lui aussi repris. « Les produits n'étaient pas exposés, mais figuraient au catalogue. » …
L'entreprise a informé l'ensemble de ses clients et prospects de la circulation de faux produits portant sa marque, tout en leur rappelant, dans ce courrier, « les dangers que représente la tentation de se procurer à vil prix de grossières copies de ses pièces ».

Dirigeants de PME, cette brochure vous concerne !

Ces quelques exemples précédents suffisent à vous montrer et vous convaincre que des actes de négligences, fraudes et malveillances peuvent survenir dans vos entreprises quelle que soit leur taille, voire même dans les sphères les plus élevés du pouvoir.
Nous avons choisi de nous adresser aux PME, car les grandes entreprises disposent, en principe, de ressources, de moyens, d'outils et de méthodes pour maîtriser de tels risques. Dirigeants de PME, vous ne disposez pas des mêmes moyens. Vous choisissez alors d'autres priorités, pensant que la dimension de votre entreprise, la connaissance de votre personnel, la qualité des relations existantes vous mettent à l'abri de ce type d'actes.
Pourtant, **un dirigeant qui sous-estime ces risques, fragilise son entreprise, quand il ne la met pas en danger de mort.**
Cette brochure s'appuie sur des aspects pratiques, des témoignages, des exemples de responsables d'entreprises ayant subi des préjudices de cette nature. Les éléments contenus dans cette brochure ne sont, bien sûr, valables qu'à leur date de parution, ce qui ne préjuge pas des évolutions pouvant survenir en matière d'exigences commerciales et de réglementation.

Vous n'êtes pas à l'abri ! Ces préjudices n'arrivent pas au'aux autres !

Aucune entreprise n'est à l'abri, même si les entreprises françaises se montrent discrètes sur le sujet, avouant rarement avoir subi des préjudices, signes d'un manque de vigilance, d'un mélange de honte, voire de pudeur et de peur.
La revue L'Entreprise **(2)** en donne des aperçus : « Vol, concurrence déloyale, détournement de fichiers, falsification de documents, usurpation d'identité, la fraude, la malveillance se manifestent sous des formes variées et produit des ravages économiques dans les entreprises. Mais en a-t-on pris la juste mesure ?

Aux Etats-Unis, le coût annuel de cette criminalité dépasse 200 milliards de dollars,
et 30 % des faillites de petites et moyennes entreprises résulteraient de la malhonnêteté des salariés. Plus proche de nous, en Belgique, selon une étude statistique récente, la moitié des petites et moyennes entreprises « se déclarent affectées par des problèmes de délinquance ». Pourquoi n'existe t-il pas de telles statistiques en France ? Simplement parce que le sujet est encore tabou et les témoignages forcément anonymes.
Ces actes sont comme la maladie : « Tant qu'on n'y a pas été confronté, on s'imagine que cela n'arrive qu'aux autres.» **(3)**. A tort, car le mal est bien plus répandu qu'on ne le pense. Verdict en 2009 : Price Waterhouse **(4)** révèle l'ampleur du phénomène dans sa cinquième édition de l'étude mondiale sur la fraude dans les entreprises, **Une grande entreprise sur deux est touchée par la fraude dans le monde.** Il en est de même en France. 43% des entreprises qui ont relevé des fraudes constatent une augmentation de leur nombre par rapport au passé.

Négligences, fraudes et malveillances sont des risques élevés pour votre entreprise, pouvant provoquer pertes d'exploitation et détérioration de l'image. Si des grands groupes peuvent survivre à ces attaques, la situation peut être fatale pour les PME.

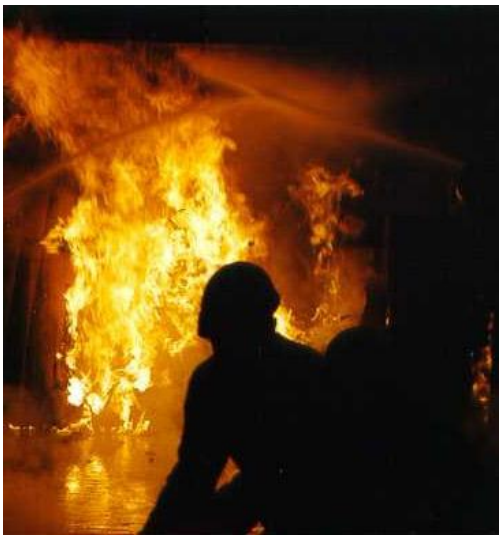
La pression au travail et la réduction des effectifs des équipes de contrôle accroissent le risque de fraude dans les entreprises. Par ailleurs, le profil du fraudeur évolue vers le middle management. Les entreprises sondées anticipent, dans l'année à venir, un accroissement de 9 points des détournements d'actifs (de 13% à 22%) et de 5 points de la fraude comptable (de 6% à 11%). La bonne nouvelle est que les dispositifs de contrôle interne détectent maintenant une fraude sur deux. La tolérance zéro est désormais de mise (85 % des fraudeurs sont licenciés).. De quoi faire réfléchir sérieusement !

Les conséquences peuvent être dramatiques

Négligence, fraude et malveillance peuvent revêtir différents aspects : incendie, vols, accidents, sabotage de machines, falsification de documents, copies de brevets, contrefaçon, débauchage de personnel, attaque du système informatique, … La liste en est longue et les conséquences peuvent revêtir un caractère dramatique. Deux exemples illustrent les conséquences possibles sur la pérennité d'une entreprise :

- en cas d'incendie, si les sinistres peuvent être tragiques sur le plan humain, ils le sont aussi sur le plan économique. D'après une enquête de l'Institut National de Recherche sur la Sécurité (INRS) : **même en étant très bien assurées, près de 3 entreprises sur 4, ne reprennent pas leur activité après avoir été victimes d'un incendie**.
- les menaces sur les systèmes informatiques sont de plus en plus fréquentes. Selon une enquête **(5)** menée en France dès 1998, les pertes engendrées, toutes catégories confondues, atteignaient 2,8 milliards d'euros. Depuis, elles ne cessent d'augmenter.

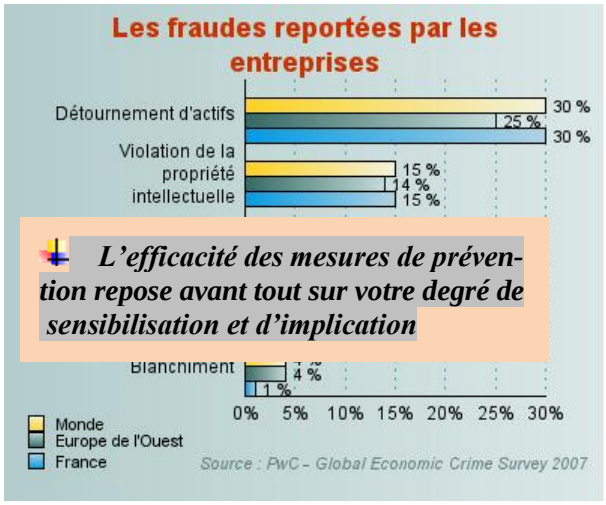
« Les dégâts de la cybercriminalité au Royaume-Uni sont évalués en 2009 à 30 milliards d'euros par année, soit près de 1,9% du PIB 2009 du pays » **(6)**



Tentative d'incendie (abna.co)

Les principales menaces viennent autant de l'intérieur que de l'extérieur

La plus fréquente des menaces consiste à détourner du matériel de son circuit habituel. La seconde vise à détourner des fonds. Une autre forme de menace semble se répandre : le déclenchement d'incendie ou le sabotage de la production ou de machines dans le but de se venger.



L'efficacité des mesures de prévention repose avant tout sur votre degré de sensibilisation et d'implication

Les personnes qui, à côté de vous, s'autorisent des écarts et mettent votre entreprise en danger ont souvent un profil de « parfait collaborateur ». Il vous est peut-être difficile d'imaginer que cela puisse être vrai. Et pourtant !

L'implication du dirigeant est une condition impérative de l'efficacité.
Même si vous êtes souvent l'homme-orchestre de votre entreprise, n'attendez pas spontanément de vos collaborateurs le même type de comportement !
Face à ces menaces, vous devrez faire front en décidant de la mise en place d'une démarche dans le but de protéger les biens dont vous avez la charge, voire même la propriété. Vous êtes donc le mieux placé, car vous disposez de la connaissance la plus globale de l'entreprise et vous êtes responsable des enjeux techniques, stratégiques et financiers.
Votre implication est d'autant plus nécessaire que des évolutions sont inéluctables pour les PME :

- **de plus en plus de donneurs d'ordre travaillant en flux tendu, veulent se garantir de la défaillance possible de leurs sous-traitants,**
- **l'âpreté de la concurrence nationale et internationale fragilise votre entreprise lorsqu'elle est absente de son marché,**
- **des banquiers et actionnaires veulent également des garanties quant à leurs enjeux financiers,**
- **les assureurs exigent une réduction des risques encourus avant d'accorder leurs garanties.**

Vous pouvez agir

Bien qu'en France, ces menaces de négligences, fraudes et malveillances soient des sujets tabous, des données fournies par des assureurs montrent que plus de 30 % du montant des sinistres portés à leur connaissance sont la conséquence de la réalisation de ces menaces.
Certains pays comme l'Angleterre ont mis en place des plans d'actions qui ont fait régresser fortement les dommages.
Vous trouverez en encadré ci-après, 10 mauvaises raisons qui pourraient, de façon insidieuse, freiner votre engagement. Rejetez ces fausses excuses et agissez vite !

10 mauvaises raisons pour choisir de ne pas agir

La mise en place d'un plan de prévention et de protection contre les négligences et la malveillance suppose une volonté forte de la direction. Mais souvent, de mauvaises raisons conduisent l'entreprise à ne pas mettre en œuvre cette stratégie. En voici quelques unes :

Le site est clôturé ou son accès peu aisé.
Le site est occupé 24h/24.
Le site est gardienné.
L'entreprise n'a jamais connu d'actes de négligence ou de malveillance.
L'entreprise ne se situe pas dans une zone sensible aux actes de malveillance.
Le climat social de l'entreprise est calme.
L'entreprise ne se connaît pas de concurrents.
Les produits de l'entreprise ne sont pas intéressants pour un marché frauduleux.
Il n'y a pas de fortes valeurs monnayables sur le site.
Les activités de l'entreprise ne sont pas réputées sensibles.

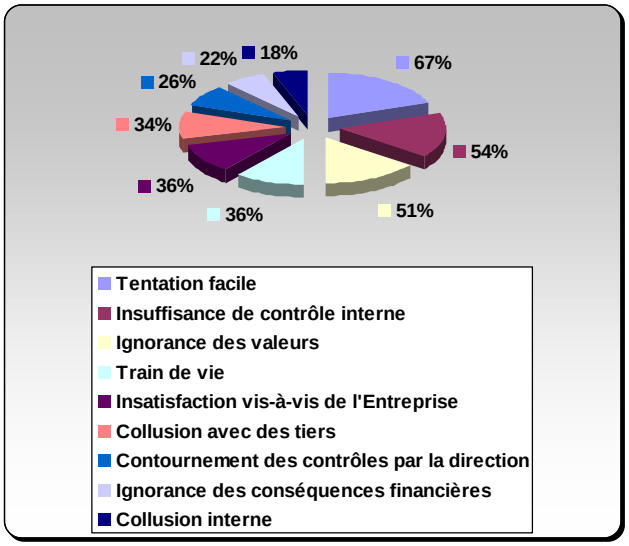
Vous devez agir

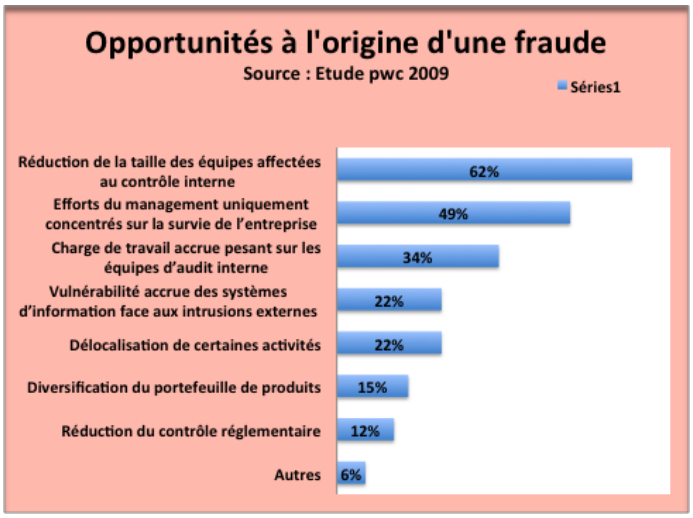
La démarche décrite ci-après, doit être conduite sous votre autorité en l'adaptant à votre entreprise. Plusieurs PME ont déjà établi leurs plans d'actions, souvent à la suite d'un préjudice. Toutefois, pour une meilleure efficacité, nous vous conseillons de vous y prendre bien avant d'être confronté à cette situation.
Il va de soi que votre démarche devra aussi respecter le droit social.

Agissez selon une démarche pragmatique

Quelles motivations poussent leurs auteurs à commettre des fraudes ? La revue Face Aux Risques **(7)** ainsi que l'étude Price Waterhouse **(4)** nous livrent ci-dessous les clés.

Motivations à commettre des fraudes





Les trois principales motivations passent par des points faibles recensés au niveau des entreprises : la tentation est d'autant plus forte que le contrôle interne est insuffisant voire défaillant et que le chef d'entreprise ne met pas en exergue les valeurs de l'entreprise. L'étude de Price Waterhouse citée ci-avant le souligne.

Par ailleurs, l'efficacité maximale permettant de détecter les fraudes provient de l'existence d'une gestion de risque et de la mise en place d'audits internes.

La démarche pragmatique proposée vise donc à :

- réduire les motifs d'incitation aux actions de négligences, fraudes et malveillances,
- maximiser l'efficacité de la gestion des risques et de l'audit interne.

Ces objectifs exigent et justifient votre totale implication. Vous devrez également veiller à expliquer à l'ensemble de votre personnel que cette politique de réduction des risques vise à pérenniser l'entreprise dans l'intérêt de tous.

Certaines situations peuvent engendrer des risques, alors même que l'entreprise n'est pas, a priori, particulièrement menacée.
Les situations peuvent être des déclencheurs d'actes qui n'auraient peut-être pas eu lieu si un minimum de prévention et de protection avait été mis en œuvre. Pour illustrer quelques unes des situations rencontrées par des PME, divers exemples vous sont présentés ci-après en encadré.

1) L'accès à l'intérieur des bâtiments est très facile : bâtiments ouverts, site non clôturé, baies vitrées en rez-de-chaussée, portes non verrouillées, etc.

Ex : *Lors d'une manifestation à Paris un pavé a atterri dans le local informatique qui était situé en rez-de-jardin à trois mètres du trottoir.*

2) L'environnement proche est propice à des accès non contrôlés : bâtiments tiers contigus, accès par les toitures, circulation de tiers en dehors des heures ouvrables, etc.

Ex. : *En passant par des toitures terrasses contiguës on a pu accéder aux dispositifs de ventilation d'un immeuble et y glisser des fumigènes, provoquant la panique.*

3) L'entreprise se situe dans une zone exposée aux actes de malveillance.

Ex. : *Actes de terrorisme dans certaines régions, zones urbaines sensibles.*

4) Le climat social de l'entreprise se dégrade et/ou des licenciements sont en cours.

Ex. : *Des employés furieux de voir mettre leur entreprise en cessation de paiement jettent des produits toxiques dans une rivière proche.*

5) Les produits de l'entreprise peuvent intéresser un marché frauduleux.

Ex. : *On a pu constater le vol de moules de fabrication (en particulier dans certains domaines proches de l'industrie automobile) pour réaliser des copies meilleur marché dans un pays tiers.*

6) Il y a de fortes valeurs monnayables sur le site.

Ex. : *Ce n'est pas forcément de l'argent mais également des plans, descriptifs de fabrication, plans de développement stratégiques, études de marchés, etc.*

7) Les activités de l'entreprise sont sensibles et peuvent intéresser des concurrents, même en dehors de la haute technologie.

Ex. : *Des études menées en Intelligence Economique ont montré que des concurrents savaient profiter d'une visite technico-commerciale pour photographier, prendre des échantillons de matériaux, ou encore envoyaient un stagiaire.*

8) Des éléments propices aux actes de malveillance sont accessibles facilement (stockages extérieurs contre les bâtiments, produits dangereux, bennes à déchets, emballages, etc).

Ex. : *Pendant les fêtes de fin d'année, des « fêtards » non contrôlés ont mis le feu à des planches d'un chantier jouxtant un hôpital en activité.*

9) Vos concurrents se livrent à des contrefaçons et des agissements parasitaires et déloyaux

Ex. : vous constatez des pertes de marchés et le développement de copies.

10) Un concurrent vous attaque en contrefaçon.

Ex. : vous recevez une mise en demeure ou une assignation vous enjoignant de cesser la commercialisation d'un produit phare.

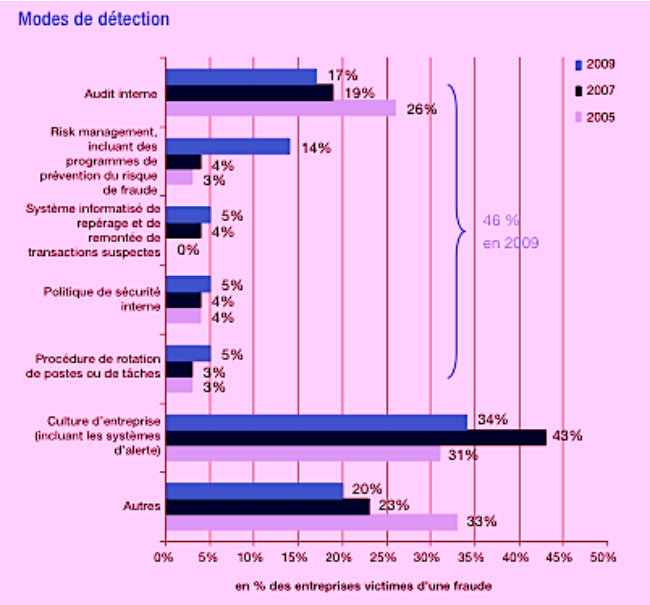
2 – Les étapes de la démarche

Recenser les incidents et accidents

En priorité, vous devez posséder une connaissance suffisante des incidents et accidents survenus dans votre entreprise.
Utilisez les sources d'informations permettant de détecter les fraudes (voir image tirée de l'étude Price Waterhouse 2009) **(4)**.
Explorez au moins la période des trois dernières années afin de :

- l'analyser selon les critères décrits ci-après,
- définir l'importance des causes attribuables à la négligence et à la malveillance, leurs conséquences pour votre entreprise.

Différents aspects seront recensés (coûts et pertes de production, voire de clients, image de l'entreprise auprès du personnel et éventuellement des clients, des voisins, des médias et des autorités locales, …).
Si votre système d'informations ne recense aucun incident, posez-vous la question de la qualité du recensement de vos informations.



Source : Etude Price Waterhouse 2009

Analyser les incidents et accidents selon différents critères.

Ce qui est en cause : personnel, immobilier, mobilier dont machines, fournitures, matières et stocks de produits nécessaires à la production ou déjà fabriqués, documentation, informatique (matériel et logiciel), biens immatériels appelés parfois invisibles ou non mesurables (savoir-faire, secrets commerciaux ou de fabrication, base de données clients, image de marque, …).

La nature de l'événement : incendie, vol, incident et accident, sabotage de machines par exemple ou falsification de documents,

L'origine de la menace :

- interne : par accoutumance au danger, inconscience, scrupules pour critiquer un collègue ou désir de nuire, espoir de gain direct ou indirect, …
- externe :
  - sans volonté de nuire (manque de connaissance de l'entreprise par certains sous-traitants,….)
  - avec intention de nuire (pour favoriser la concurrence, exercer un chantage, éliminer un concurrent, …).

Les cibles supposées : l'entreprise globalement, la hiérarchie, les collègues, un partenaire de l'entreprise, un client,

Les conséquences :

- en interne, les incidences techniques sur les équipements (coûts et délais de remise en état) et les procédés, produits, réactions du personnel,
- en externe : les réactions des clients, des donneurs d'ordre, des fournisseurs, des assureurs, des voisins, des médias et des pouvoirs publics.

Ces conséquences dépendent de la manière dont l'information a été traitée, en interne et/ou en externe et des délais de diffusion.

- au niveau des installations, des procédés, des produits,
- au niveau de l'organisation et des procédures.

Analyser la vulnérabilité de votre entreprise

Après avoir étudié les différents incidents ou accidents pouvant être causés par des actes de négligence, des fraudes ou des malveillances, et avant de pouvoir mettre en place un plan de prévention et de protection contre ces préjudices, prenez conscience des vulnérabilités de votre entreprise. Cette démarche, également applicable à l'ensemble de vos risques, a pour objectif d'identifier les cibles potentielles d'actes non souhaités et capables de mettre votre entreprise en difficulté, voire en péril.

Les points névralgiques sont les activités ou les systèmes dont l'arrêt, la mise hors service, la destruction ou la disparition aurait, pour votre entreprise, des conséquences (sociales, économiques et financières, pénales, environnementales, de notoriété, …) importantes ou très difficilement supportables et pouvant, à l'extrême, entraîner la disparition de votre entreprise. A chaque point névralgique correspondent deux critères ;

- la fréquence avec laquelle une menace peut le solliciter,
- la gravité, c'est-à-dire l'impact ou la conséquence de la réalisation de la menace sur ce point.

L'annexe 1 présente une démarche d'analyse de la vulnérabilité d'une entreprise.
Les évaluations recensées sont réunies sur un tableau à deux axes (fréquence et gravité) permettant une représentation graphique de tous les risques jugés possibles.

Définir une politique de sécurité

Cette politique doit d'abord être décidée par vous, puis mise en place par vos collaborateurs. Elle caractérise votre vision de responsable qui doit déterminer les risques acceptables ou non. Vous devez éviter d'être trop téméraire ou trop pusillanime.

Définir une politique de propriété intellectuelle

Avec la mondialisation et l'intensification de la concurrence, la maîtrise des questions de propriété intellectuelle constitue un enjeu majeur. Prendre en compte les brevets des concurrents pour éviter d'être contrefacteur, et mieux stimuler sa propre capacité d'innovation, organiser la préservation de son savoir-faire et de ses secrets industriels et commerciaux, protéger ses innovations et créations esthétiques et commerciales nécessite une volonté stratégique et une culture partagée par toutes fonctions de l'entreprise.
Pour en savoir plus : « PME, pensez PI » diffusé par la DGCIS, ou prestation Prédiagnostic de l'INPI.

Définir les priorités, décider, mettre en place, contrôler

Selon la représentation graphique (annexe 1), la politique de sécurité permet de recenser tous les risques se classant dans la catégorie des risques inacceptables et de hiérarchiser les actions à entreprendre pour ramener les niveaux de risques à des valeurs acceptables (annexe 2).
Le choix des priorités est toujours délicat puisqu'il est difficile de comparer un risque lourd de conséquences mais peu probable avec un risque fréquent mais de moindre gravité.
Le bon sens a sa place dans cette réflexion pour tenir compte du coût et de la difficulté d'éliminer un risque peu probable.
Les priorités étant clairement définies et faisant, si possible, l'objet d'un consensus, il est alors possible de sélectionner les mesures adaptées pour améliorer de façon significative la sécurité.
C'est à ce stade que l'effort de concertation, d'explication et de formation doit être développé pour que les personnels qui subiront les contraintes inhérentes à la mise en œuvre de ces mesures, aient bien conscience qu'ils en seront tous les principaux bénéficiaires.
Pour que les progrès soient durables, mettez en place des moyens de contrôle périodiques avec une bonne publicité des résultats obtenus.
La démarche qui précède est transposable à une analyse globale des risques de votre entreprise.
L'annexe 3 explicite le regard pouvant être porté sur le management des risques.

3 - Les recommandations

Recommandations générales

La démarche présentée peut avantageusement être étendue à l'ensemble des incidents et accidents les plus redoutés de façon à faire ressortir clairement l'efficacité de certaines des dispositions adoptées. Elle peut aussi concerner les difficultés éventuelles d'application de la réglementation.

Rares sont les entreprises qui possèdent les compétences ou qui disposent du temps disponible pour réaliser l'audit de vulnérabilité. Il est alors recommandé de le faire réaliser par un prestataire disposant des compétences et de l'expérience nécessaires.

Cette sous-traitance ne vous dispense pas d'un engagement personnel dès l'origine de l'action et de veiller à l'implication de vos plus proches collaborateurs.
Vous pouvez aussi, dans la mesure du possible, organiser des échanges et réflexions en commun avec certains personnels et/ou leurs représentants et recueillir des opinions externes de confrères, des assureurs, des consultants, …

Nous confirmons ici que les mesures à prendre doivent dépendre de la vulnérabilité de l'entreprise, de sa taille et de ses autres caractéristiques. L'expérience montre que certaines d'entre elles doivent être envisagées dans tous les cas. Elles sont rappelées ci-dessous :

- organisation de l'entreprise et définition des responsabilités, en particulier pour
- la sécurité et le contrôle de la mise en œuvre des consignes de sécurité décidées,
- identification des dangers et des points sensibles en veillant à des mises à jour souvent nécessaires en raison de modifications des installations ou pour tenir compte de l'expérience,
- rédaction de consignes et procédures en cas d'incident ou accident, régulièrement mises à jour,
- organisation d'exercices d'entraînement à la bonne application de ces consignes et procédures,
- prévention et protection contre les risques d'incendie et d'intrusion,
- sécurisation des systèmes d'information,
- étude et mise en place d'un Plan de Continuité des Activités (PCA),
- sensibilisation et implication permanentes du personnel. Tout événement doit être mis à profit pour relancer la motivation, rappeler certains principes et former les nouveaux entrants, y compris les temporaires,
- connaissance et respect des réglementations,
- Sensibilisation du personnel en matière de protection des secrets et de propriété intellectuelle
- prise en compte des remarques des assureurs, des donneurs d'ordres, des clients, des consultants, …

Recommandations spécifiques

Pour vous aider dans votre démarche, quelques guides et conseils sont réunis dans les annexes 2, 3, 4, 5 et 6.

Réflexions sur les mesures à mettre en place

Une fiche guide placée en annexe 2 vous aidera à recenser toutes les actions déjà réalisées ou celles qui sont à prévoir. Cette fiche présente trois types de mesures de nature technique, organisationnelle et de sécurisation de l'information, elles-mêmes classées en trois niveaux :

- *de niveau 1 (minimales),* à mettre en place, quelle que soit la sensibilité du site vis-à-vis de la malveillance,
- *de niveau 2,* à mettre en place pour sécuriser une activité assez sensible aux actes de fraude, négligence et malveillance,
- *de niveau 3*, à mettre en place lorsque l'activité est particulièrement sensible vis-à-vis de la malveillance :
- secteur stratégique pour un groupe (recherche, développement, …),
- secteur sensible (pharmacie, haute technologie, nanotechnologies, chimie, pétrolier, automobile, aéronautique, militaire, …)

Les bonnes pratiques

Cette aide est complétée par la mise à votre disposition de l'expérience acquise dans d'autres secteurs ayant déjà été confrontés à ces types d'actes. L'annexe 4 rappelle les bonnes pratiques déjà éprouvées.

La sécurité des systèmes d'information

L'annexe 5 appelle votre attention sur les systèmes d'information, l'une des plus importantes vulnérabilités émergentes. Les pirates informatiques intensifient leurs attaques contre les entreprises. Les agresseurs utilisent toutes les failles de systèmes réputés inviolables pour opérer des transactions illicites, piller des données, attenter à l'image de l'entreprise dans un but lucratif, idéologique ou par simple goût de l'exploit. Parfois, c'est un employé licencié qui le système informatique, parfois, la négligence d'un cadre entraîne la perte de données stratégiques ou leur diffusion à l'extérieur de l'entreprise.
Cette situation résulte de la vulnérabilité des entreprises qui n'ont pas toujours pris les mesures nécessaires de protection.

Cette annexe développe, d'une façon détaillée, les mesures de protection à mettre en place afin de se prémunir d'éventuelles failles.

La prise en compte du facteur humain

L'annexe 6 présente les moyens de mobiliser les femmes et les hommes de l'entreprise, par l'implication des ressources humaines : information, formation et participation. (8)

4 - Les témoignages de dirigeants d'entreprises

En annexe 7, vous trouverez des témoignages de chefs d'entreprises dévoilant leurs préoccupations en la matière, leur engagement dans la lutte contre ces préjudices et leurs conseils.

5 - Références

Index

(1) La Dépêche (extrait du 19 avril 2011) - L'Entreprise (Extraits du n° 201 de juin 2002) – Le Progrès de Lyon du 24/02/2006 - Sud-Ouest 20 avril 2011
(2) **L'Entreprise (Extraits des revues d'octobre et novembre 2005)**
(3) Gérard de Fournas, associé spécialiste de la fraude au sein du cabinet Grant Thornton (audit, expertise comptable et conseil)
(4) Enquête Price Waterhouse 2009
(5) CLUSIF (Club de la Sécurité des Systèmes d'Information Français)
(6) Money Week juillet 2011 n° 139
(7) Face aux Risques n° 422 d'avril 2006 (CNPP Edition)
(8) Formation aux risques de malveillance (CNPP)

Sites internet de référence

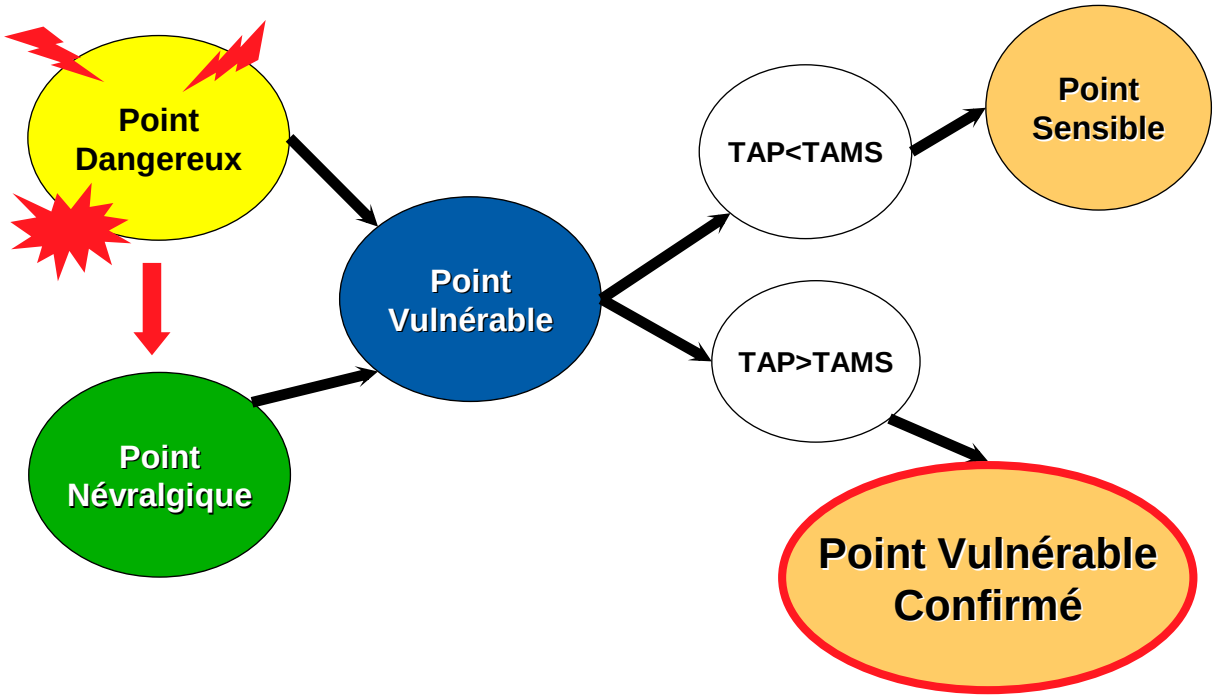
- **Centre National de Prévention et de Protection (CNPP) – CD 64 – Route de la Chapelle Réanville – Saint-Just – 27950 Saint Marcel – www.cnpp.com**
- **Association des Ingénieurs et Cadres spécialistes de la maîtrise des risques incendie, vol, environnement, sécurité et santé au travail , agréés par le CNPP (AGREPI) – 48 Boulevard des Batignolles – 750017 Paris – www.agrepi.com**
- **Club de la Sécurité de l'Information Français (CLUSIF) 30, rue Pierre Sémard 75009 Paris www.clusif.asso.fr**
- **Caisses Régionales d'Assurance Maladie (CRAM) – Pour l'Ile de France : www.cramif.fr**
- **Fédération Française des Sociétés d'Assurances - 26 boulevard Haussmann - 75 009 Paris - www.ffsa.fr**
- **Groupe d'Etudes de Sécurité des Industries Pétrolières et Chimiques (GESIP) - 22, rue du Pont Neuf - BP 2722 - 75027 Paris cedex 01 – www.gesip.com**
- **Institut pour une Culture de Sécurité Industrielle (ICSI) - 6 allée Emile Monso - ZAC du Palays BP 34038 31029 Toulouse Cedex 4 - www.icsi-eu.org**
- **Institut pour la Maîtrise des Risques (IMdR) – 12 Avenue Raspail - 94250 Gentilly – www.imdr.eu**
- **Institut National de l'Environnement Industriel et des Risques - Parc Technologique ALATA - BP 2 - 60550 Verneuil-en-Halatte – www.ineris.fr**
- **Institut National de Recherche et de Sécurité - 30, rue Olivier Noyer - 75680 Paris Cedex 14- www.inrs.fr**
- **Ministère de l'Ecologie, du Développement et de l'Aménagement Durables - 20 avenue de Ségur - 75302 Paris 07 SP - www.ecologie.gouv.fr**
- **Ministère de l'Economie, des Finances et de l'Emploi - 139 rue de Bercy 75572 Paris Cedex 12 - www.industrie.gouv.fr**
- **Ministère de l'Intérieur - Place Beauvau - 75008 Paris - www.intérieur.gouv.fr**
- **Pôle Risques - Europôle de l'Arbois - Bat. Laennec - Hall A - 13857 Aix en Provence Cedex 3 - www.pole-risques.com**

6 - Annexes

Annexe 1	**Analyse de Vulnérabilité**
Annexe 2	**Questionnaire pour évaluer la sensibilisation des PME**
Annexe 3	**Un regard global sur les risques : l'approche cindynique**
Annexe 4	**Les bonnes pratiques**
Annexe 5	**La sécurité des systèmes d'information**
Annexe 6	**Le facteur humain dans le risque**
Annexe 7	**Interview de responsables d'entreprises**

1 - Analyse de vulnérabilité

La mise en place d'un plan de prévention et de protection contre les négligences et la malveillance suppose de connaître les vulnérabilités de l'entreprise, c'est-à-dire les cibles potentielles d'actes de négligence ou de malveillance pouvant mettre en difficulté, voire en péril l'entreprise.
L'analyse de vulnérabilité consiste à identifier les points névralgiques de l'entreprise et les points dangereux qui les menacent éventuellement.



TAP : Temps d'Arrêt Probable
TAMS : temps d'Arrêt Maximal Supportable

Les points névralgiques sont les activités ou systèmes dont l'arrêt, la mise hors service, la destruction ou la disparition aurait, pour l'entreprise, des conséquences (sociales, économiques, financières, pénales, environnementales, de notoriété, etc.) importantes ou très difficilement supportables et pouvant, à l'extrême, entraîner la disparition de l'entreprise. Ces points névralgiques sont caractérisés par la gravité (G), c'est à dire l'impact ou la conséquence de la réalisation de la menace. Pour hiérarchiser les points névralgiques, nous vous proposons des classes de gravité suivantes :

G = 1	**Aucune conséquence prévisible**
G = 2	**Conséquences internes**
G = 3	**Conséquences externes**
G = 4	**Vie de l'Entreprise menacée**

L'échelle de gravité (G) peut être adaptée à la taille de l'entreprise.

Les points névralgiques sont également caractérisés par le temps d'arrêt probable (TAP), c'est à dire le temps pendant lequel le point névralgique concerné n'assure plus sa fonction normalement et le temps nécessaire pour reconstituer, éventuellement de façon dégradée, la fonction remplie par ce point névralgique.

Les points dangereux sont les activités, lieux, systèmes ou dispositions pouvant, avec une probabilité non négligeable, constituer l'origine ou l'élément primordial d'un début de sinistre. Une caractéristique des points dangereux est la fréquence (F), ou probabilité d'occurrence de réalisation de la menace. Pour hiérarchiser les points dangereux, nous pouvons considérer les classes de fréquence suivantes :

F = 1	**Très peu probable**
F = 2	**Probable**
F = 3	**Très probable**
F = 4	**Fréquent**

La fréquence (F) peut être évaluée en fonction de l'existence de mesures de prévention techniques et/ou organisationnelles.

Lorsqu'un point névralgique est touché par un ou plusieurs points dangereux, il devient un point vulnérable. Si son temps d'arrêt probable (TAP) est supérieur au temps maximal d'arrêt supportable (TAMS) par l'entreprise, il est nécessaire de mettre en place un plan de prévention pour réduire la probabilité d'occurrence (fréquence) et de protection pour réduire l'impact et les conséquences (gravité).

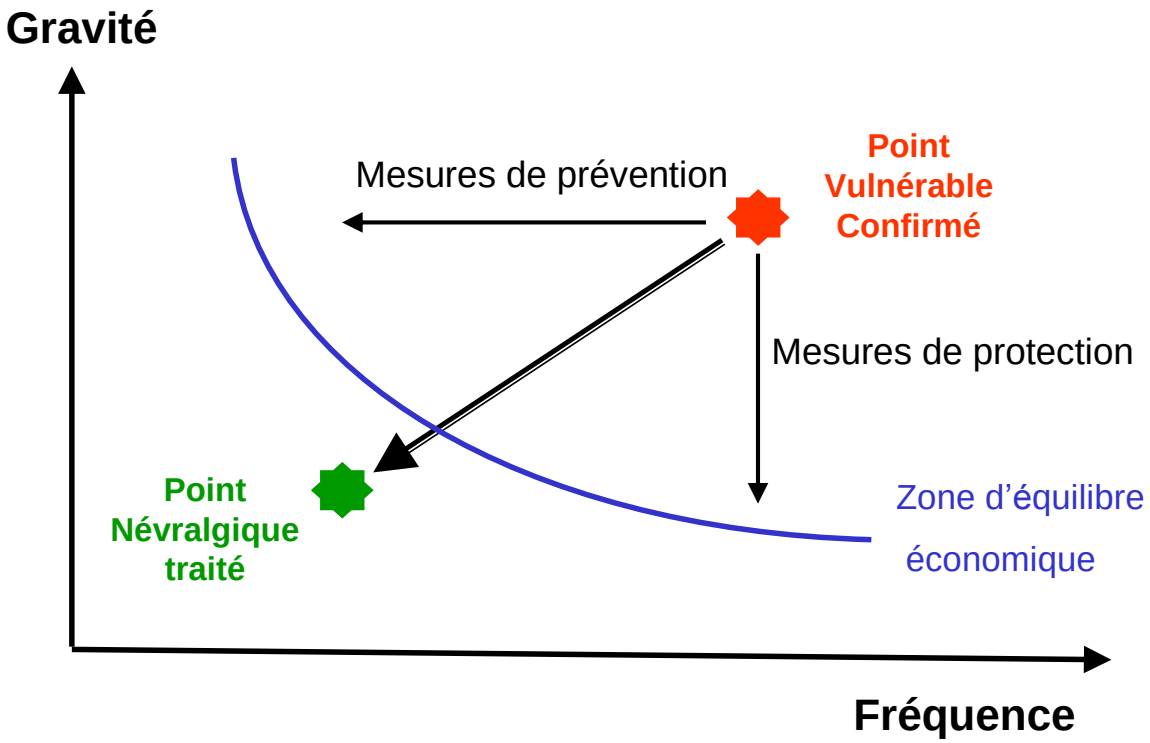
Un Plan de Continuité des Activités (PCA) est également nécessaire pour gérer la crise qui peut survenir selon différents scénarios à envisager.

Pour hiérarchiser les priorités de traitement, on peut réaliser une cartographie des risques qui est issue d'une table croisant la gravité et la fréquence.

4	**3**	**4**	**4**	**4**
3	**2**	**3**	**4**	**4**
2	**2**	**2**	**3**	**4**
1	**1**	**2**	**2**	**3**
↑ G F →	**1**	**2**	**3**	**4**

Ce qui permet de hiérarchiser les risques ainsi :

R = 1	**Risque faible**	**Pas d'action nécessaire**
R = 2	**Risque moyen**	**Action à envisager à moyen terme**
R = 3	**Risque fort**	**Action indispensable à court terme**
R = 4	**Risque catastrophique**	**Action urgente**



(1) La zone d'équilibre économique est la zone où le coût des mesures de prévention et de protection est en équilibre avec le coût des risques potentiels

Qui peut réaliser l'audit de vulnérabilité ?

Rares sont les entreprises qui possèdent en interne les compétences ou simplement le temps de réaliser l'audit de vulnérabilité. Il est alors recommandé de faire réaliser cet audit par un prestataire qui a toutes les compétences, la formation et l'expérience nécessaire. Ce prestataire peut être un consultant spécialisé ou un ingénieur prévention de la compagnie d'assurance de l'entreprise. A noter que les assureurs préconisent aux PME de faire réaliser un audit de la vulnérabilité et valorisent celui-ci en offrant une réduction substantielle de la cotisation d'assurance. La condition requise est de faire réaliser cet audit suivant un référentiel (APSAD R11) par un organisme agréé par les assureurs.
Cet audit s'accompagne d'une liste de recommandations afin de réduire l'exposition de l'entreprise vis-à-vis des risques identifiés.

2 - Questionnaire pour évaluer la sensibilisation des PME

Le questionnaire est constitué de 3 parties :

- Les mesures de niveau 1
- Les mesures de niveau 2
- Les mesures de niveau 3

Parmi ces mesures, il y a des mesures techniques, organisationnelles et de sécurisation de l'information.

Les mesures de niveau 1 sont les mesures minimales à mettre en place, quelle que soit la sensibilité du site.

Les mesures de niveau 2 sont les mesures *minimales complémentaires aux mesures de niveau 1,* à mettre en place par les dirigeants sensibilisés à ces risques.

Les mesures de niveau 3 sont les mesures *minimales complémentaires aux niveaux 1 et 2*, à mettre en place lorsque l'activité est particulièrement sensible :

- recherche et développement, …
- pharmacie, haute technologie, nanotechnologies, chimie, pétrolier, automobile, aéronautique, militaire, ….

Les tableaux suivants vous précisent les questions

Annexe 2

MESURES DE NIVEAU 1	En place	A prévoir	Sans objet
MESURES GENERALES			
Clôture totale du site (hauteur clôture 2 m minimum). Sans objet si immeuble sans terrain.			
Fermeture ou couverture des ouvrages sensibles (bâtiments, cuves, fosses, installations techniques, salle informatique, autocommutateur téléphonique, etc.)			
Portes, fenêtres, ventilations, prises d'air, trappes d'accès, construites en matériaux résistants ou protégées de façon adéquates (grilles, barreaux)			
Verrouillage systématique des accès sensibles			
Serrures de sûreté, blindages sur bâtiments ou éléments sensibles (en fonction de l'implantation géographique, la situation dans la chaîne de production ou de traitement de l'information)			
Mise en place de barrières multiples avant d'accéder aux éléments sensibles.			
Eclairage des abords pendant la nuit			
Suppression des matériels (échelles, stockages extérieurs, liquides inflammables, produits dangereux) permettant de perpétrer facilement des actes de malveillance ou d'intrusion			
Entretien des abords des bâtiments et des éléments sensibles : débroussaillage, pas de stockage (stockages, bennes à déchets, palettes vides) à moins de 10 m, voire plus selon leur volume, des bâtiments et éléments sensibles			
Limitation du stockage de matériels sensibles			
Réparation rapide des clôtures et des équipements (portes, fenêtres, serrures) endommagés			
Si nécessaire, renforcement des mesures prises en cas de tentative d'effraction ou d'effraction constatée			
Mise en place d'une signalétique appropriée vis-à-vis des risques (utilisation et stockage des produits dangereux, activités à risques, etc.) et étiquetage des produits.			
Formation du personnel, systématique et régulière, vis-à-vis des risques (produits dangereux, activités à risques, etc.)			
SECURITE DE L'INFORMATION			
Tout le réseau informatique est cartographié, y compris les modems vers les sous-traitants (télémaintenance), les autocommutateurs, les gestions techniques centralisées, les machines de reprographie numérique,			
Le réseau informatique est surveillé par des firewall et par des antivirus.			
Tous les postes de travail informatiques sont équipés d'antivirus avec actualisation régulière.			
Les postes de travail informatiques des itinérants sont équipés de firewall, d'antivirus, d'antispyware et d'authentification forte en cas de connexion sur les réseaux de l'entreprise.			
Toutes les données informatiques ou non (plans, documents sensibles, etc.).sont sauvegardées sur un lieu différent des systèmes (back-up, mirroring, bandes, etc.) et les sauvegardes sont sous contrôle d'accès.			
Les prises informatiques inutilisées sont désactivées.			
Les armoires techniques sont fermées à clé.			
Les accès aux machines informatiques se font avec des mots de passe.			

.MESURES DE NIVEAU 2	En place	A prévoir	Sans objet
MESURES GENERALES			
Entrées sur le site limitées à un nombre restreint d'accès aménagés et sécurisés (interphone, caméra, projecteur, portail électrique commandé de l'intérieur du site) et condamnation des accès non sécurisés			
Contrôle d'intrusion global ou réservé aux éléments sensibles			
Contrôles audio et vidéo permanent ou asservi à une installation de détection d'intrusion			
Contrôle d'accès sur l'ensemble du site ou réservé aux éléments sensibles			
Alarmes sonores (sirène) en cas de détection d'intrusion			
Les personnes externes sont systématiquement accompagnées sur le site			
Chiens en liberté ou en laisse sur le site			
Patrouilles de surveillance sur le site et dans les locaux (éventuellement par une société externe) avec pointage des rondes et tenue d'une main courante.			
Patrouilles de surveillance aux abords du site (société externe, police, gendarmerie)			
Visites inopinées du personnel de l'entreprise hors heures ouvrables (service de maintenance, direction)			
Réalisation de rondes par l'exploitant en heures ouvrables avec tenue d'une main courante			
Présence de gardiens en heures ouvrables, de personnel travaillant en permanence, de logements de fonction sur le site			
Formation régulière et spécialisé du personnel par un organisme extérieur.			
Stockage sécurisé des produits dangereux.			
Contrôle et surveillance du respect des règles de sécurité.			
Suivi de l'état des machines, hors maintenance, (état des organes de sécurité) et remise en état immédiat.			
SECURITE DE L'INFORMATION			
Le réseau informatique est ilôté et des sous-réseaux spécifiques sont réservés selon des secteurs (production, recherche, finances) et selon les besoins d'accès extérieurs. Ces sous-réseaux ne partagent pas entre eux des données confidentielles.			
Les applications informatiques sensibles sont implantées sur des serveurs sécurisés avec des procédures adaptées (code d'accès, chiffrement) et sont isolées par des firewall ou par un îlotage.			
Tous les systèmes d'authentification (applications informatiques, autocommutateurs, contrôle d'accès) sont gérés à partir d'un méta-annuaire sous la responsabilité de la DRH.			
Les utilisateurs du système d'information sont identifiés avec des règles sur les mots de passe (longueur, mots réservés, fréquence de changement).			
Chaque utilisateur n'a accès qu'aux applications et aux données qui lui sont autorisées.			
Pour les maintenances externes, y compris les imprimantes et photocopieuses, les données confidentielles ne peuvent pas sortir de l'entreprise (par destruction des supports de données par exemple).			
Les techniciens de maintenance en sous-traitance n'interviennent qu'en présence des utilisateurs. Les mots de passe donnés à ces techniciens sont changés dès la fin de l'intervention de maintenance.			
Un plan de continuité informatique est tenu à jour, avec des tests périodiques.			

MESURES DE NIVEAU 3	En place	A prévoir	Sans objet
MESURES GENERALES			
Contrôles audio et vidéo avec enregistrement permanent ou asservi à une installation de détection d'intrusion			
Contrôle d'accès avec enregistrement, sur l'ensemble du site ou réservé aux éléments sensibles			
Marquage des biens pour faciliter les poursuites ultérieures			
Contrôle des identités et tenue d'un registre des entrées-sorties			
Information du personnel sur la position de fermeté de l'entreprise pour poursuivre les délinquants			
Dépôt de plainte systématique en cas de tentative d'effraction ou d'effraction constatée (pas d'impunité)			
Formation du personnel et mise en place de procédures en cas de tentative d'effraction ou d'effraction constatée (gestion de crise, analyse du problème pour le retour d'expérience et l'amélioration des procédures)			
Contrôle des utilisations des produits dangereux, mise en place d'un registre d'entrée/sortie.			
Mise en place de sanctions, motivations du personnel face au non-respect des règles de sécurité.			
Formation du personnel à l'intervention d'urgence.			
Simulation régulière de cas de crise.			
SECURITE DE L'INFORMATION			
Les données sont classifiées (diffusion restreinte, confidentiel, secret défense) et les données confidentielles sont chiffrées (codées).			
Les procédures d'exploitation et de sauvegarde sont différenciées selon les degrés de disponibilité requis.			
Les moyens de secours et de redémarrage sont différenciés selon les degrés de disponibilité requis.			
Les contrats de sous-traitance informatique incluent des clauses de confidentialité.			
Les sous-traitants informatiques sont audités.			
La réglementation générale sur les fichiers nominatifs et l'intrusion dans les systèmes est connue et respectée.			
Les réglementations spécifiques éventuelles (pharmacie, chimie,…) sont connues et respectées.			
Les utilisateurs sont informés des obligations légales : fichiers nominatifs, contrats de prestation, détention d'images illégales, cryptologie, secret des correspondances, intrusion dans les systèmes informatiques.			
Tout projet informatique est élaboré avec une démarche d'assurance qualité.			
Dans chaque structure, un correspondant informatique joue le rôle de relais avec la direction des systèmes d'informations.			
Les responsables sont régulièrement sensibilisés aux règles de sûreté de l'information.			
Les nouveaux embauchés sont informés des règles de sûreté de l'information.			
Des tests périodiques d'intrusion sont effectués par des sociétés externes pour vérifier l'actualisation des logiciels et des antivirus.			
Un tableau de bord de la sécurité informatique, recensant les incidents, est tenu à jour.			
Une veille informatique est organisée pour identifier les vulnérabilités.			
Des procédures de protection des innovations et créations			
Des procédures de vérification de la liberté d'exploitation			
La gestion des droits de PI dans les partenariats			

3 - Un regard global sur les risques : l'approche cindynique

En 1987, plus de 1 500 personnes ont participé au premier grand colloque organisé sur la maîtrise des risques technologiques à l'UNESCO. Parmi les nombreuses conclusions figurait la nécessité d'une approche globale des risques et la transversalité des approches : les cindyniques ou sciences du danger venaient de naître.
Au cours de ce colloque, plusieurs insuffisances avaient été constatées parmi lesquelles ressortaient :

- Le retour d'expérience n'existe que dans le nucléaire, l'aéronautique et la chimie. Il faut donc le promouvoir dans toutes les disciplines.
- Les accidents diffus, notamment les accidents de la route, les accidents du travail et les accidents domestiques, font trop de victimes. Une prévention importante est à mettre en place à tous les niveaux des acteurs.
- Les statistiques, en particulier celles portant sur le monde entier et sur les risques éclatés, sont encore trop pauvres.
- La perception des risques n'est pas en adéquation avec la réalité.

L'étude et l'analyse d'un certain nombre de catastrophes relevant de l'espace (Challenger), du nucléaire (Tchernobyl), de la chimie (Seveso, Bhopal), du transport maritime (Titanic), du transport aérien (Ténériffe), de l'environnement (Exxon Valdez) , ont permis l'établissement d'une grille de lecture composée de dix déficits souvent à l'origine d'accidents. L'application de cette grille dans l'entreprise permettrait de prévenir un grand nombre d'accidents.

Les déficits culturels

- Infaillibilité : c'est, par exemple, le syndrome du Titanic. Tout le monde le croit insubmersible et il coule lamentablement. Ce déficit est également constaté lors de l'analyse de Bhopal ou de Challenger. N'est-ce pas un déficit fréquent chez le « chef » qui, quelle que soit l'entreprise (groupe ou PME), se retrouve dans la croyance « l'accident n'arrive qu'aux autres » ?

- Simplisme : les industriels estiment que ce qu'ils font est simple (c'est le cas de Bhopal) où la simplicité apparente d'un processus (parfois unique) de production fait oublier les risques amont-aval ou collatéraux.

- Non-communication : Scandinavian Star : personne ne parle la même langue (mécaniciens, marins, passagers), Bhopal : les ingénieurs américains ne comprennent pas les remarques des ouvriers faites en hindi. -La machine à café c'est très bien mais ce n'est pas le seul lieu de communication …

Le Titanic : images Le Télégramme

- Nombrilisme (orgueil) : Bhopal : Union Carbide se croit la meilleure entreprise du monde dans le domaine de la chimie donc ne voit pas de raison de se remettre en cause. C'est une réaction naturelle cultivée par certains dans un contexte concurrentiel qui fait dire et même parfois penser…. qu'on est le meilleur…

Les déficits organisationnels

- Subordination des fonctions de gestion de risques aux fonctions de production La sécurité est sur le même plan que la productivité Bhopal, Tchernobyl. Dans les petites PME, le plus souvent, les fonctions ne sont pas très différenciées. Aux différents niveaux les responsables ont du mal à s'imposer personnellement et mentalement cette subordination de fonctions qu'ils cumulent.

- Dilution des responsabilités. C'est le cas de Bhopal où techniciens et administratifs se renvoyaient la balle. C'est sans doute moins le cas en PME.

Les déficits managériaux

- **Absence de retour d'expérience :** Bhopal, Challenger, Tchernobyl,…Dans tous ces cas, de multiples incidents précurseurs avaient été enregistrés. Le retour d'expérience en PME devrait être mutualisé.

- **Absence d'approche globale :** Il n'y a pas d'approche globale de la gestion des risques et cela est flagrant à Bhopal, Tchernobyl, ou sur le Scandinavian Star. Le document unique (cf Code du Travail) peut, notamment, permettre des progrès en ce sens.

- **Absence de culture de sécurité :** Bhopal, Tchernobyl, Scandinavian Star. Les PME peuvent souvent utiliser les compétences des centres techniques professionnels mais celles-ci sont parfois méconnues.

- **Absence d'une gestion de crise :** Tchernobyl, Bhopal. Personne ne sait ce qu'il doit faire en cas d'accident, ce qui peut aggraver les conséquences de l'accident. Ce point est capital pour les PME dont la survie est souvent en jeu à la suite d'un sinistre.

Analyser le fonctionnement de son entreprise au travers de cette grille peut permettre de réduire à la fois les risques d'accident et les conséquences de ceux-ci lorsqu'ils surviennent.

Au-delà, d'autres facteurs comme l'inadaptation des moyens ou encore l'éthique entrent en jeu dans les causes des accidents

.

4 - Les bonnes pratiques

Certaines bonnes pratiques, moyens ou procédures peuvent réduire les possibilités d'actes de malveillance. Les recommandations suivantes, si elles ne suppriment pas totalement les risques face à la détermination de certains individus ou de certaines organisations, peuvent toutefois réduire les conséquences d'actes de malveillance ou rendre leur réalisation difficile. Ces recommandations sont partiellement extraites et adaptées d'un article de Préventique Sécurité de juillet-août 2005 rédigé par F.Mansotte.

Augmenter l'effort du délinquant potentiel

Protection des cibles, accès plus difficiles

Clôture totale du site (murs, palissades, grillages, voire bavolets et barbelés) et cohérente (même type de protection et même hauteur – 2 m – sur les clôtures et portails sur toutes les faces du terrain).

Entrées sur le site limitées à un nombre restreint d'accès aménagés et sécurisés (interphone, caméra, projecteur, portail électrique commandé de l'intérieur du site) et condamnation efficace des accès non sécurisés.

Fermeture ou couverture des ouvrages sensibles (bâtiments, cuves, fosses, installations techniques).

Portes, fenêtres, ventilations, prises d'air, trappes d'accès, construites en matériaux résistants ou protégées de façon adéquates (grilles, barreaux).

Verrouillage systématique des accès sensibles (une installation qui est prévue pour être verrouillée en permanence doit l'être en permanence).

Serrures de sûreté, blindages sur certains bâtiments ou éléments sensibles (en fonction de l'implantation géographique, la situation dans la chaîne de production ou de traitement de l'information).

Mise en place de barrières multiples avant d'accéder aux éléments sensibles.

Orientation des personnes externes

Panneaux d'information avec des messages de type « défense d'entrer » en nombre suffisant et bien placés.

Pas de fléchage excessif des éléments sensibles, à concilier avec les besoins d'exploitation et de sécurité.

Réduction des instruments propices à la délinquance

Suppression des matériels (échelles, stockages extérieurs, liquides inflammables, produits dangereux) permettant de perpétrer facilement des actes de malveillance ou d'intrusion.

Entretien des abords des bâtiments et des éléments sensibles : débroussaillage, pas de stockage (stockages, bennes à déchets, palettes vides) à moins de 10 m, voire plus selon leur volume, des bâtiments et éléments sensibles

Augmenter les risques pour le délinquant potentiel

Contrôle des entrées et sorties

Contrôle des identités et tenue d'un registre des entrées-sorties, contrôle d'accès avec enregistrement, sur l'ensemble du site ou réservé aux éléments sensibles.

Surveillance par des moyens humains

Patrouilles de surveillance sur le site et dans les locaux (éventuellement par une société externe) avec pointage des rondes et tenue d'une main courante.

Patrouilles de surveillance aux abords du site (société externe, police, gendarmerie)

Visites inopinées du personnel de l'entreprise hors heures ouvrables (service de maintenance, direction).

Réalisation de rondes par l'exploitant en heures ouvrables avec tenue d'une main courante.

Présence de gardiens en heures ouvrables, de personnel travaillant en permanence, de logements de fonction sur le site.

Surveillance par des moyens techniques

Contrôle d'intrusion global ou réservé aux éléments sensibles.

Contrôles audio et vidéo avec enregistrement permanent et asservi à une installation de détection d'intrusion.

Télésurveillance avec traçabilité des informations et des interventions éventuelles

Alarmes sonores (sirène) en cas de détection d'intrusion.

Chiens en liberté ou en laisse sur le site.

Eclairage des abords pendant la nuit (permanent ou asservi à une détection de présence)

Réduire les gains du délinquant potentiel

Elimination des cibles susceptibles d'intéresser le délinquant

Limitation du stockage de matériels sensibles.

Identification des biens

Marquage des biens pour faciliter les poursuites ultérieures et/ou pour éviter le copiage.

Etablissement de règles et de procédures

Information du personnel sur la position de fermeté de l'entreprise pour poursuivre les délinquants.

Dépôt de plainte systématique en cas de tentative d'effraction ou d'effraction constatée (pas d'impunité).

Créer et maintenir un état d'esprit propice à la réduction du risque de malveillance

Formation du personnel et mise en place de procédures en cas de tentative d'effraction ou d'effraction constatée (gestion de crise, analyse du problème pour le retour d'expérience et l'amélioration des procédures).

Réparation rapide des clôtures et des équipements (portes, fenêtres, serrures) endommagés.

Si nécessaire, renforcement des mesures prises en cas de tentative d'effraction ou d'effraction constatée.

Information et sensibilisation du personnel pour qu'il soit un acteur de la prévention du risque de malveillance.
Imagination de scénarii pour anticiper les actes possibles de malveillance.

Repérage des attitudes suspectes ou des actes de négligence.

Informer et sensibiliser le personnel aux risques dus à la négligence.

Formation du personnel aux machines et outils, mais aussi à l'ensemble des produits utilisés sur le site et à leurs interactions.

Formation des intervenants ponctuels (sous traitants, stagiaires).

Mise en place d'une signalétique appropriée et la mettre à jour régulièrement.
Étiquetage des produits.
Mise à disposition de conditionnements appropriés.

Contrôle de l'utilisation des produits, stockage sécurisé, tenue d'un registre d'entrée/sortie des produits.

Contrôles inopinés des responsables (port du casque, protections corporelles, maintien des sécurités sur les appareils, etc.)
Mise en place de sanctions et motivations.

5 - La sécurité des systèmes d'information

La malveillance en matière de systèmes d'information est en constante évolution. Les agresseurs utilisent les failles de systèmes réputés inviolables pour opérer des transactions illicites, piller des données, attenter à l'image de l'entreprise dans un but lucratif, idéologique ou par simple goût de l'exploit. Parfois, c'est un employé licencié qui « se venge » en attaquant le système informatique, parfois, la négligence d'un cadre entraîne la perte de données stratégiques ou leur diffusion à l'extérieur de l'entreprise.

Cette situation résulte de la vulnérabilité des entreprises, qui n'ont pas toujours pris les mesures nécessaires de protection, du fait que leurs budgets de sécurité informatique les ont obligés à opérer des choix, à prendre certains risques.
La cybercriminalité devient un véritable fléau économique. En juin 2011, « les réseaux de prestigieuses entreprises telles que Lockheed Martin, Sony ou Citigroup ont été piratés. Sony s'est fait dérober les informations privées de 77 millions de ses clients – pépin qui va tout de même coûter 170 M$ au géant japonais. (6)

Selon une étude, publiée en 2006 et menée par le FBI auprès de 2000 sociétés américaines, ***la cybercriminalité coûte en moyenne 24 000 dollars par an à une entreprise américaine, soit 67 milliards de dollars à l'échelle des Etats-Unis.***

Sur l'ensemble du panel, 90% des répondants ont subi une attaque au cours des 12 derniers mois. Parmi ces 90%, une entreprise sur cinq déclare avoir connu au moins 20 attaques dans le courant de l'année. Au total, 64% ont enregistré des pertes financières suite à des incidents de sécurité informatique.

Des incidents principalement causés par les virus*, dans 84% des cas, suivis par* ***les logiciels espions*** *(80%), puis les* ***tentatives d'intrusion réseau*** *(32,9%) et enfin l'analyse de ports réseaux (scan) et le sabotage de données (20%).*

Sur l'ensemble du panel, les codes malveillants ont provoqué une perte évaluée à 12 millions de dollars, contre 2,7 millions de dollars pour les intrusions réseaux et 3,2 millions de dollars pour le vol d'ordinateur.

Ces attaques proviennent d'un total de 36 pays, même si la majorité est issue soit des Etats-Unis, soit de la Chine, responsables respectivement de 26,1% et 23,9% des incidents. Face à ces menaces, les sociétés interrogées étaient équipées à 98,2% d'antivirus, à 90,7% d'un pare-feu et à 75% d'une solution globale de lutte contre le code malveillant (anti-rootkit, anti-phishing, anti-spyware…).

Selon les responsables informatiques interrogés, ***44% des intrusions étaient d'origine interne****, nécessitant de meilleures procédures de contrôle. Hormis les méthodes, les responsables informatiques se sont aussi tournés vers de nouveaux outils : 4% ont opté pour la biométrie et 7% pour des cartes magnétiques.*

L'action en justice est régulièrement menée par les sociétés attaquées, puisque 8 victimes sur 10 y ont recours. Elles se déclarent satisfaites de la décision pour 99% d'entre elles. Seules 9% ne portent pas plainte, ne sachant pas si ces pratiques sont illégales ou non et à quelle législation se référer.

Aujourd'hui, la majorité des délits concerne principalement le détournement d'informations bancaires d'internautes naïfs. Mais il existe d'autres moyens d'attaques plus subtils, comme prendre le contrôle d'un grand nombre d'ordinateurs en les regroupant dans ce qui s'appelle un *botnet*. Ceci permet au hackers de submerger les serveurs d'entreprises avec tant d'informations qu'ils ne peuvent plus fonctionner correctement. 130 milliards de spams sont quotidiennement envoyés, 92% d'entre eux proviennent des botnets. (6)

Le constat :

- la dépendance vis-à-vis du système d'information est très forte *(Perte du contrôle de la régulation d'une partie du réseau d'acheminement du gaz en Russie. Décès dans un service de réanimation suite à une coupure électrique.)*
- les savoirs sont plus largement diffusés sous forme numérique, la dématérialisation sera totale
- les acteurs sont plus nombreux, les partenariats entraînent des interconnexions de réseaux
- les autorités réglementaires généralisent les télé-déclarations
- la concurrence est exacerbée dans certains secteurs de haute technologie, les entreprises se dotent d'outils de veille et d'analyse très puissants
- la nomadisation des acteurs, le télétravail, la vente à distance, la présence d'un site internet, imposent des connexions à distance ou des échanges entre systèmes de messageries et bases de données internes de l'entreprise
- la numérisation de la communication se généralise avec la visioconférence, la téléphonie sur Internet
- l'externalisation des services informatiques, le recours à la sous-traitance (parfois off-shore)
- l'informatique est partout : dans les badges, les étiquettes des produits RFID, le téléphone, les cartes bancaires, les systèmes de certificats numériques, aussi bien dans la vie privée que dans la vie professionnelle, posant des problèmes de frontière
- le protocole internet, peu sécurisé en lui-même, a été généralisé pour gérer le réseau interne
- la large diffusion des failles techniques et des outils de piratage d'une grande simplicité d'usage

Ainsi, du vol d'information, de la tentative de déstabilisation au blocage complet du système, l'entreprise peut se trouver en danger voire disparaître en cas d'attaque de son système informatique.

QUE FAUT-IL PROTEGER ?

Les données sont-elles confidentielles ?

Il ne faut pas banaliser la confidentialité des documents ni se méprendre sur leur éventuelle exploitation par un tiers mal intentionné. On entend encore trop souvent dire que « chez nous, il n'y a pas de données sensibles, il n'est pas nécessaire de mettre en œuvre des protections coûteuses ».

La première action consiste à **élaborer une classification des données**. Lesquelles sont stratégiques, lesquelles sont réservées au Personnel de l'entreprise, lesquelles sont publiques ?
La classification des documents (diffusion restreinte, confidentiel, secret) est plus souvent le fait des entreprises publiques ou travaillant pour la Défense Nationale. Elle est moins répandue dans le privé, où l'on a tendance à déclarer tout document comme étant confidentiel : on se retrouve alors à tout protéger, tout chiffrer avec des budgets ou des contraintes d'utilisation considérables et au final…on ne fait plus rien!

En 2006, en l'espace d'un mois, un cabinet d'audit a perdu quatre PC portables aux Etats-Unis. Ces derniers contenaient des informations confidentielles sur l'identité de clients. Parmi eux, le, PDG d'une très grande entreprise, a ainsi appris que son numéro de sécurité sociale - identifiant le plus utilisé outre-Atlantique par

les organismes financiers - était en circulation sur internet.

La Direction de l'entreprise doit être impliquée pour définir en quoi consistent les données stratégiques, celles à diffusion restreinte et celles plus ouvertes. Les protections particulières pourront alors être mises en œuvre (îlotage du réseau, chiffrement des données).

En 2004, une société porte plainte pour espionnage : à la suite d'une prestation d'audit un logiciel espion a été introduit et des fichiers copiés.

Les savoir-faire critiques doivent être identifiés, formalisés afin de permettre une organisation efficace de sa confidentialité, notamment par des mesures limitant l'accessibilité aux seules personnes autorisées.

L'entreprise doit être en mesure d'identifier les innovations et créations susceptibles de faire l'objet d'un droit de Propriété Intellectuelle, afin de décider si un dépôt est pertinent pour répondre aux objectifs définis (barrière à l'entrée pour des produits concurrents, renforcement des accords commerciaux, levée de fonds, …)

QUELLE EST LA CONNAISSANCE DU RESEAU ?

Cartographier le réseau est une étape indispensable : on ne peut se contenter d'une vue partielle sur l'un des établissements ou bien sur le réseau français et ignorer la filiale anglaise ou le centre de recherche ou un sous-traitant.

On s'aperçoit que, dans bien des entreprises, le parc du matériel raccordé au réseau n'est ni exhaustif, ni tenu correctement à jour. Par exemple, certains matériels sont ignorés parce qu'ils ne sont pas gérés par la structure informatique, ou par des entités différentes, c'est souvent le cas de la Gestion Technique Centralisée (GTC), des autocommutateurs numériques (Téléphonie). Parfois les outils de collecte automatisée "oublient" les matériels de reprographie numérique (et leurs disques !), les stations reliées par des modems vers des sous-traitants.

COMMENT SECURISER SON INFORMATIQUE ?

La sécurité physique est un minimum : elle commence par une protection de la salle machine accessible aux seuls personnels autorisés, avec des éléments de sécurité incendie, dégâts des eaux, foudre, une alimentation électrique de secours, etc. A cela s'ajoute la protection du réseau de distribution de l'informatique : armoires techniques fermant à clé, prises informatiques inutilisées inactivées. Puis vient la protection du poste de travail lui-même.

Ceci constitue le minimum, mais n'est évidemment pas suffisant : il faut également se préoccuper de la sécurité dite logique (sauvegardes, flux, mots de passe, certificats,..)

COMMENT PROTEGER SON RESEAU ?

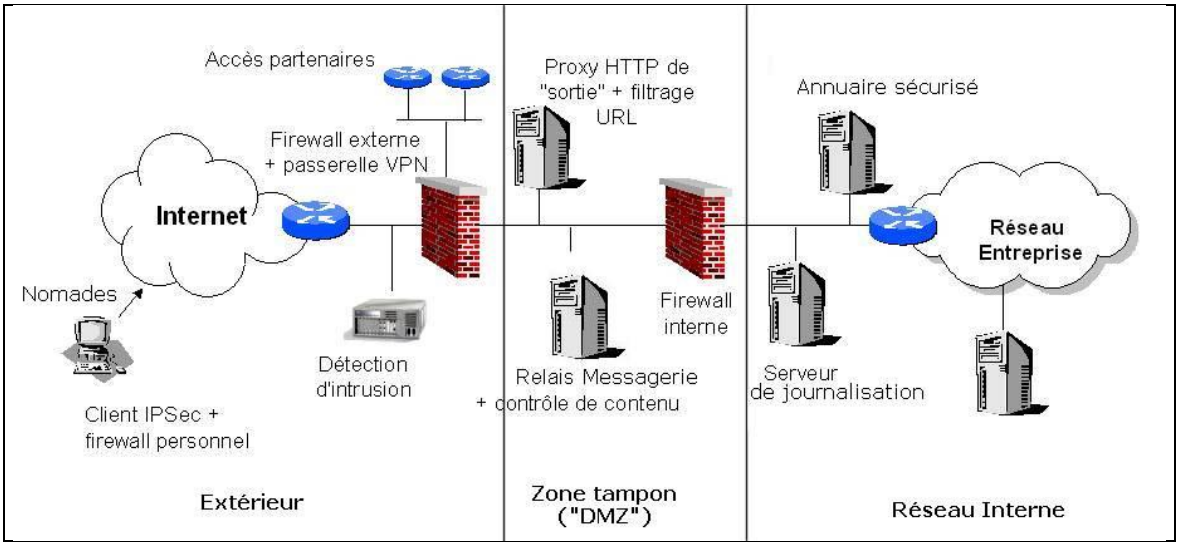
Une fois la topologie du réseau connue, il faut connaître les flux d'information et déterminer une architecture adaptée. Le plus simple est souvent de recourir à l'îlotage ou la défense périmétrique : créer des sous-réseaux identifiés (un pour tous les accès extérieurs, un pour la production, un pour la recherche,...).

Par exemple un réseau pourra n'avoir aucun lien avec les autres parce qu'il traite de données jugées très confidentielles (il faut avoir à l'esprit que l'essentiel de la menace est interne).

Installer des parades techniques : outils de surveillance du réseau (pas seulement orientés sur la disponibilité), et des systèmes de contrôle de flux ("garde-barrière" ou Firewall).

Il est prudent de n'autoriser des accès par l'extérieur (internet, bornes radio, etc.) qu'au travers d'une authentification forte (un dispositif matériel couplé au méta-annuaire) et un canal chiffré de type VPN (réseau privé virtuel).

Pour les données confidentielles circulant sur le réseau, y compris interne, utiliser des **outils de chiffrement.**



Exemple d'architecture technique sécurisée

COMMENT PROTEGER SES SERVEURS ?

La rédaction et la mise en œuvre de procédures d'exploitation et de sauvegarde des données doivent être faites selon les niveaux de disponibilité. Les moyens de secours garantissant un redémarrage dans les 24 heures ne sont pas les mêmes que ceux garantissant une disponibilité permanente du système.

Prévoir les maintenances externes : par exemple, si un support contenant des données confidentielles doit être emporté par un technicien, lors d'une maintenance on devra effectuer préalablement un formatage de "bas niveau" qui rendra les données définitivement inaccessibles ou bien interdire le départ du disque et procéder à sa destruction (penser aux imprimantes-photocopieuses à disque dur qui peuvent emmagasiner un nombre important de données).

COMMENT PROTEGER LES POSTES DE TRAVAIL ?

Installer sur tous les postes des antivirus et prévoir l'actualisation régulière.
Pour les utilisateurs de portables ou itinérants, utiliser des outils de protection du poste (firewall, anti-spyware,..) et d'authentification forte s'ils doivent se connecter à distance sur les réseaux de l'entreprise.

Prévoir des moyens de protection physique du poste, notamment les portables : tatouage, clé de mise en œuvre, câble antivol, puce électronique.
Si nécessaire mettre en œuvre des outils de chiffrement des données.
En octobre 2004, vol de plusieurs ordinateurs d'un sous-traitant de banque contenant des données confidentielles de clients.

COMMENT SECURISER LES APPLICATIONS ?

Le choix de progiciels comme la conduite de projets développés en interne ou au forfait doivent intégrer la sécurité dès le départ dans le cahier des charges.

Un Plan d'Assurance Qualité peut couvrir ces éléments.

On veillera à séparer les environnements de développement, de test et d'exploitation

Isoler (par des firewalls ou un îlotage) les applications sensibles sur des serveurs sécurisés avec des procédures adaptées (accès, chiffrement).

COMMENT SECURISER L'UTILISATION DU SYSTEME D'INFORMATION

Identifier les utilisateurs, les bases de données, les habilitations. Attribuer à un utilisateur un identifiant et un mot de passe en imposant des règles sur les mots de passe (longueur, mots réservés, fréquence de changement).

Créer un méta-annuaire sous la responsabilité de la DRH et se baser sur cet annuaire pour alimenter tous les systèmes d'authentification (applications informatiques, autocommutateurs, contrôle d'accès, etc.)

En juillet 2004, vol de fichiers sources, de données confidentielles. Un ingénieur renvoyé du centre de R&D en Inde est soupçonné d'être l'auteur du vol.

Si nécessaire, mettre en œuvre un système de signature électronique.
Elaborer une charte d'utilisation des moyens bureautiques, l'idéal étant de l'annexer au règlement intérieur (donc au contrat de travail).

Ne donner à chaque utilisateur que les applications auxquelles il a droit.

Définir des procédures particulières pour le personnel informatique et ses sous-traitants. Par exemple, celui qui détient les clés de chiffrement n'a pas d'accès aux fichiers des utilisateurs et vice versa.
Signifier au personnel informatique extérieur (maintenance, prestataires,...) qu'il devra respecter les règles de confidentialité et de sécurité informatique en vigueur, prévoir des contrats en ce sens (accords de secret) dans la pratique, il est nécessaire d'auditer ses partenaires pour évaluer leur propre niveau de sécurité

En février 2004, des portions du code de Windows NT4 sont disponibles en libre accès sur internet, un partenaire de Microsoft est identifié comme à l'origine de la fuite.

Prévoir des règles pour les interventions de maintenance.

Par exemple :

- Les techniciens de maintenance ne doivent pas - sauf accord de l'utilisateur - intervenir en dehors de la présence des utilisateurs.
- Si un mot de passe est communiqué au technicien, il doit être immédiatement modifié par l'utilisateur après l'intervention.

COMMENT ASSURER LA CONTINUITE DE L'EXPLOITATION APRES SINISTRE

Un Plan d'Urgence recensant les mesures nécessaires au redémarrage d'une production bloquée, détruite ou endommagée, doit être réalisé en partenariat avec les utilisateurs concernés et, s'il existe, doit s'intégrer dans le plan de continuité du site.

Ce plan doit comporter la liste des applications vitales tenue à jour et indiquer quelles mesures ont été prises pour garantir la continuité des traitements

Prévoir une réactualisation annuelle, sauf en cas de changement important sur le site, où il sera immédiatement rediffusé.

Ce plan doit être connu et approuvé par la hiérarchie, notamment dans la définition des applications vitales.

COMMENT SE PROTEGER JURIDIQUEMENT

En dehors de la Loi, applicable à tous (fichiers nominatifs, intrusion dans les systèmes,…) certains secteurs de l'Industrie sont soumis à des contraintes réglementaires (pharmacie, chimie, etc.).
Par exemple, outre la jurisprudence, voici quelques, textes importants :

La protection des personnes

- Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

La protection de la propriété intellectuelle

- Loi du 1er juillet 1992, loi du 10 mai 1994 (logiciels),
- Loi du 1er juillet 1998 (bases de données)
- Dernière version au 29 mai 2011

Lutte contre la malveillance

- Loi « Godfrain » relative à la fraude informatique - janvier 1988.
- Si vous êtes victime d'une malveillance informatique, vous pouvez vous adresser à divers services de l'Etat (consulter http://www.clusif.asso.fr/fr/production/cybervictime/).

La protection des correspondances

- loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications

Cryptologie

- Loi du 29 décembre 1990, la loi du 26/07/96 (Précisent la notion de moyens cryptologiques, les conditions d'utilisation)
- Décret du 19 mars 1999 (conditions de diffusion, importation, utilisation, ..)
- La loi pour la confiance dans l'économie numérique, n°2004-575 du 21 juin 2004, abrégée sous le sigle LCEN, sur le droit de l'Internet et le commerce électronique

Signature électronique

- Loi du 30 mars 2000 relative à l'écrit électronique et la signature électronique
- Décret du 30 mars 2001 et du 18 Avril 2002

Il faut être en mesure de justifier par une preuve d'achat tout logiciel présent sur un poste de travail.
Cette étude de contraintes peut se faire avec la Direction Juridique, ou des conseillers juridiques locaux, car ces obligations peuvent varier d'un pays à l'autre, si l'on envisage le déploiement international d'une application.

Veiller à la bonne information des utilisateurs concernant les obligations légales :

- fichiers nominatifs,
- contrats de prestation
- détention d'images illégales (pédophiles, portant atteinte à la dignité humaine, racistes, criminelles, à caractère pornographique, etc.)
- cryptologie
- secret des correspondances,
- intrusion dans les systèmes informatiques,
- ...

En février 2004, quatre suspects arrêtés au Japon. Ils réclamaient 28 millions de dollars pour ne pas divulguer les informations confidentielles de 4,5 millions de clients. Incidences sur l'image de marque de la société qui n'a pas pris assez de précautions pour protéger ses fichiers : Le président de l'entreprise est contraint de s'excuser officiellement après le scandale.

COMMENT PRENDRE EN COMPTE LA PROPRIETE INDUSTRIELLE

***Avant l'engagement d'un projet** : vérifier les brevets et marques détenus par les principaux concurrents pour en étudier la portée et la validité et prendre en compte les risques juridiques. Mais aussi pour enrichir les connaissances techniques et stimuler ses propres innovations.*
***Lors de partenariats et d'innovation collaborative** : organiser dès le départ les règles de propriété et d'exploitation des résultats, de partage des responsabilités, des risques et des retombés financières et la répartition des travaux.*

***Lors de l'obtention de résultats :** arbitrer entre brevet et secret, déterminer les résultats à breveter, préparer des brevets solides déposés au bon moment.*

Dans l'organisation de l'entreprise : *mettre en place des mesures de reconnaissance des inventeurs salariés, définir la politique de gestion du portefeuille de droits de propriété industrielle, sensibiliser le personnel à la protection du patrimoine intellectuelle et la lutte contre la contrefaçon.*

COMMENT ASSURER LA QUALITE DES SYSTEMES D'INFORMATION

La réduction de certains risques liés à la non-qualité (erreurs logicielles, erreurs d'exploitation) passe par une démarche qualité indissociable de la sécurité.
Imposer, par exemple un plan d'assurance qualité pour tout projet informatique contribue à la sécurité des applications (maintenance plus aisée, moins d'erreurs logicielles, traçabilité, …)

Les ***règles générales de sécurité*** doivent être formalisées et connues de tous les acteurs du système d'information.

Désigner dans chaque structure un ***correspondant sécurité informatique*** qui jouera le rôle de relais pour toute question d'actualité et éventuellement remontera des alertes sur des dysfonctionnements.

Organiser des ***réunions de sensibilisation*** périodiques avec les correspondants sécurité et les responsables utilisateurs et rappeler les règles même élémentaires.

Cette information doit également être dispensée lors d'une nouvelle embauche, procédure d'intégration, mutation.

Le personnel technique doit être particulièrement sensibilisé. A cet égard, les intervenants externes (DST, Consultants) parce qu'ils apportent une vision extérieure, sont très appréciés par les collaborateurs informaticiens.

La charte de bonne conduite leur sera régulièrement rappelée.

Procéder à des tests périodiques d'intrusion (effectués par des sociétés externes), veiller à l'actualisation des logiciels systèmes de base et des antivirus. ***Ne tenir rien pour sûr*** ni définitif, se rappeler que s'il y a une faille dans un système, elle sera un jour découverte et exploitée s'il n'y a aucun risque pour celui qui l'aura découverte.

La veille est indispensable pour anticiper et gérer les crises.

S'il existe une structure de veille dans l'entreprise, il est indispensable de travailler en étroite collaboration avec elle. Pour la partie sécurité informatique, s'abonner à une veille en vulnérabilités sera un atout important pour se protéger d'attaques extérieures.

Etablir un tableau de bord de la sécurité informatique (incidents, nature, impact, suivi des actions).

Définir chaque année un plan d'action pour impliquer les Directions dans les plans de continuité d'activité.

6 - Le facteur humain dans le risque

Comment motiver et mobiliser l'entreprise pour lutter contre le risque ?

Préambule :

L'entreprise est confrontée aux progrès techniques en constante évolution, à la concurrence dans un contexte de globalisation de notre économie mondiale, aux moyens de communication de plus en plus sophistiqués, aux aspects humains et sociaux à prendre en compte ; cela impose aux entreprises des contraintes permanentes d'évolution et d'adaptation.

Outre le fait de :

- fabriquer des produits ou de proposer des services de plus en plus performants et fiables,
- réduire de façon significative les coûts,
- s'adapter à de nouvelles règles sociales,

l'entreprise doit se prémunir contre l'insécurité des biens et des personnes qui la composent. Ce phénomène nouveau est de plus en plus important et devient une réelle préoccupation pour nos dirigeants et notamment pour ceux des PME ; c'est également une question de crédibilité et de garantie pour ses clients, fournisseurs et actionnaires.
Il est urgent d'en prendre conscience.

Tous les niveaux de l'entreprise sont concernés par le risque industriel. Il est utile de susciter la participation de chacun et de mettre en œuvre des techniques de motivation et de mobilisation applicables à l'entreprise.

La présentation qui suit n'a pas la prétention d'être exhaustive, mais elle analyse une gamme de moyens de sensibilisation que chaque entreprise peut mettre en œuvre selon ses besoins et ses spécificités. L'efficacité de leur application dépendra de la Direction Générale de l'entreprise à laquelle il revient la responsabilité de donner et de maintenir l'impulsion nécessaire. Pour obtenir une complète adhésion, il faut que la totalité du personnel, y compris les niveaux les plus modestes, puisse se sentir concernée pour y participer activement.
Pour cela il faudra appliquer des règles de communication et de bon sens basées sur
L'Information – la Motivation – la Formation.

Les acteurs internes à l'entreprise :

Dans une démarche de lutte contre le risque industriel, un certain nombre d'acteurs internes à l'entreprise doivent être impliqués dans l'action.
Tout d'abord la Direction qui a comme souci premier la réalisation de profits dont dépend la vie et le développement de l'entreprise ; mais il est maintenant reconnu que le risque industriel est un élément important à prendre en compte par les dirigeants pour la pérennité de l'entreprise.

C'est un acte de bonne gestion que représentent les actions mises en œuvre pour mieux maîtriser le risque industriel. Cela requiert la définition d'une politique en matière de sécurité et la mise à disposition de moyens et de procédures par l'introduction de normes de sécurité et de qualité.

La réalisation de cette politique sous-entend une organisation structurée, **l'encadrement** étant chargé par la direction, de développer des actions d'information et de sensibilisation jusqu'au niveau **des opérationnels**.
Dans ce cadre et quelle que soit la taille de l'entreprise, il est préférable de confier cette mission de coordination à un **responsable délégué** par la direction, à moins que celle-ci s'en charge elle même. Il conviendra à la direction de fournir à cette personne les pouvoirs et les moyens inhérents à la mission, de lui assurer un appui permanent et de réaliser un suivi des actions entreprises.

L'information :

Obtenir l'adhésion des membres d'une collectivité et les faire participer lors d'une évolution de la politique d'entreprise, passe au préalable par la mise à disposition d'informations pour que cette collectivité puisse comprendre l'intérêt de cette nouvelle politique et agir en fonction des nouveaux objectifs, afin de passer du stade de spectateur à celui d'acteur.
Exemple : Si des caméras de surveillance doivent être placées à différents endroits stratégiques de l'entreprise, la raison doit être expliquée.

Cette information doit être diffusée aux différents niveaux de l'entreprise au cours de réunions générales, de conférences spécifiques ou d'entretiens individuels, soit par le dirigeant ou son Délégué, soit par l'encadrement selon la taille et l'organisation de l'entreprise. Ces réunions sont l'occasion de présenter la politique de l'entreprise en matière de gestion des risques industriels et de préciser l'organisation mise en place pour y parvenir.

On peut également faire circuler l'information selon les différents supports de communication utilisés dans l'entreprise, mais il est nécessaire que le sujet, la présentation, le style et les commentaires soient parfaitement adaptés à l'ensemble des destinataires concernés pour obtenir leur adhésion et la motivation recherchée.
Dans le circuit de l'information, il ne faudra pas oublier le personnel nouveau, les stagiaires, les intérimaires qui sont impliqués ou concernés par le dispositif mis en place pour mieux maîtriser le risque industriel.

Lorsqu'il existe « un manuel maîtrise du risque industriel » ou « une charte de sécurité » avec les procédures inhérentes à la démarche, le document doit être accessible aux personnels de l'entreprise. Cela impose de mettre en place une procédure d'identification et d'accès à l'information réglementaire et de procéder périodiquement à une mise à jour régulière (avec un circuit de diffusion contrôlé) et à des audits de vérification des bonnes pratiques.
Ces missions incombent à la personne en charge de la démarche.

La motivation :

Même si les informations circulent correctement dans une entreprise bien organisée où le personnel est convenablement formé et motivé à se sentir responsables, il existe par la répétition et l'accoutumance aux mêmes situations un risque d'habitude qui affaiblit quelque peu la vigilance face aux dangers auxquels est exposée l'entreprise.
On pourrait dire qu'à sollicitation constante, la vigilance décroît avec le temps.
Il faut donc par des actions cycliques ou ponctuelles réveiller et entretenir les bonnes volontés détournées de l'objectif, de recadrer, de motiver de nouveau. Pour cela l'entreprise dispose de moyens qui lui sont propres et qu'elle peut facilement mettre en application :

- Prime de sécurité :
  A partir de résultats d'audit d'inspection, on distribue individuellement ou à l'équipe une prime de résultat.
- Prime de suggestion :
  Elle est accordée pour récompenser une suggestion ou proposition favorisant la vigilance dans l'entreprise en apportant un progrès dans la démarche mise en œuvre pour mieux maîtriser les risques dans l'entreprise ;
- Concours interne :
  Dans le cas d'une entreprise qui comprend plusieurs sites, il peut être institué entre eux un concours sur la sécurité suivant un règlement précis faisant intervenir le jugement d'un organisme externe indépendant. Une fois par an, la Direction remet un trophée à l'unité gagnante. De telles méthodes bien conduites sont très motivantes et débouchent le plus souvent sur des améliorations permanentes et entretiennent une culture d'entreprise face aux risques.
- Cercle sécurité :

Un cercle peut être constitué dans un secteur, un atelier, un bureau, une usine, pour discuter de problèmes touchant à la sécurité des biens et des personnes. Il examine les situations qui lui sont présentées, il étudie celles qui sont retenues et recherche des solutions, en détermine et propose les moyens et le calendrier d'exécution. Il est composé de membres de l'entreprise issus des différents secteurs et peut être piloté par le délégué en charge des risques industriels.

- Campagne d'affichage :
  Ces campagnes permettent de placer le cadre de travail sous le signe de la sécurité et peuvent créer une ambiance favorable pour retenir l'attention du personnel sur les aspects de la sécurité et des risques industriels.
- Challenges sécurité :
  L'entreprise organise chaque année un événement permettant de récompenser des initiatives du personnel en faveur de la sécurité.
  Cette démarche est l'occasion de connaître les initiatives en matière de prévention, de permettre de les partager et de les valoriser auprès de la profession toute entière.

La formation :

De nos jours, avec le développement des techniques d'information de moins en moins limitées à des contours précis, les connaissances des différentes branches de l'entreprise interfèrent et des secteurs entiers, que l'on croyait isolés dans leurs lois et règles spécifiques, sont progressivement envahis par des disciplines propres à d'autres secteurs et ce d'autant plus que les systèmes d'information sont performants et complexes. Cela pose de nombreux problèmes de sécurité et nécessite d'avoir une bonne maîtrise des aspects sécuritaire de ces équipements et systèmes.

Il apparaît donc souhaitable que sans exclusive de niveaux hiérarchiques, tous les acteurs de l'entreprise soient formés aux conséquences des risques encourus, d'être à même de pouvoir les identifier, les évaluer pour mieux les maîtriser. (8)
D'autre part, avoir une connaissance des exigences réglementaires spécifiques aux secteurs d'activités concernés ne peut que renforcer la sensibilisation et la motivation des uns et des autres dans l'entreprise et donc de lutter contre ces risques, gage de pérennité pour l'entreprise.

7 - Interview de responsables d'entreprises

7.1. Première entreprise

1 - Présentation de l'entreprise

1.1 - Quel est le secteur d'activité de l'entreprise ?
R : Agro-alimentaire

1.2 - Quelle est la taille de l'entreprise (nombre de personnes et chiffre d'affaire) ?
R : 70 personnes - 13 millions d'euros CAHT

1.3 – L'entreprise possède-t-elle plusieurs sites d'exploitation ?
R : 2 sites d'exploitation

1.4 - Le secteur d'activité est-il très concurrentiel ?
R : Oui : concurrence française et étrangère (CEE)

1.5 – L'entreprise a-t-elle des secrets de fabrication ou des informations stratégiques à protéger ?
R : Oui : procédés de fabrication développés en interne

1.6 – L'entreprise fait-elle appel à des sous-traitants partenaires pour une partie de sa production ?
R : Non

1.7 – L'entreprise exporte-t-elle une partie de sa production ou de ses services et vers quels pays ?
R : Oui : pays de la CEE (Espagne, Portugal, Belgique, Luxembourg, Suisse, Irlande)

1.8 – L'entreprise travaille t-elle avec des produits dangereux (inflammables, explosifs, corrosifs, toxiques,…) ?
R : Oui : produits de nettoyage

2 - Situation de l'entreprise vis-à-vis des actes de malveillance ou de négligences

2.1 – L'entreprise a-t-elle subi des actes de malveillance interne ou externe ?
R : Incendie en 1997 (malveillance probable)

2.2 - Quelles en ont été les conséquences internes ou externes pour l'entreprise ?
R : Destruction de l'usine

3 – L'entreprise a-t-elle été victime d'incidents ou d'accidents dus à des négligences de votre personnel ?
R : Oui

2.4 - Quelles en ont été les conséquences internes ou externes pour l'entreprise ?
R : Accidents du travail

3 - Actions de l'entreprise vis-à-vis des risques de malveillance ou de négligences

3.1 - Quelles raisons vous ont convaincu d'agir pour réduire vos vulnérabilités vis-à-vis de la malveillance interne ou externe ?
R : L'incendie de 1997
Les risques sanitaires liés à toute production agro-alimentaire tant sur le plan bactériologique que sur le risque de présence de corps étrangers

3.2 – Quelles mesures avez-vous mises en place pour réduire ces vulnérabilités ?
R : Mesures de surveillance malveillance/incendie :
Contrôles d'accès
Système de détection intrusion avec report autoprotégé vers une société de télésurveillance

Sur le premier site, système de détection incendie avec report auto-protégé vers une société de télésurveillance
Sur le second site (construit en 1999), système de détection et extinction automatique (sprinkler) avec report auto-protégé vers une société de télésurveillance

Mesures de surveillance sanitaire :

Mise en place de procédures et d'instructions de travail élaborés avec les personnels concernés
Contrôles systématiques en cours et en fin de production avec libération des lots
Matériels conçus avec un souci de faible contact avec le produit alimentaire, de facilité de nettoyage et, dans la mesure du possible, d'absence de risque de chute de corps étrangers dans le produit alimentaire
Politique forte de traçabilité : en une heure, nous sommes à même d'avertir les clients livrés avec un produit fini jugé a posteriori non-conforme
Politique HACCP et certification d'Entreprise ISO 9001 version 2000 (Entreprise certifiée depuis 7 ans)

Autres mesures :

Prise en compte des accidents du travail comme indicateur dans le cadre de la certification d'entreprise ISO 9001 version 2000
Renforcement des actions de formation et d'information en matière de sécurité et de prévention des accidents du travail

3.3 - Quelles raisons vous ont convaincu d'agir pour réduire vos vulnérabilités vis-à-vis des négligences ?

R : Sécurité des consommateurs de nos produits
Image de la société chez les clients
Bien-être de nos collaborateurs
Réduction des coûts engendrés par les accidents du travail

3.4 – Quelles mesures avez-vous mises en place pour réduire ces vulnérabilités ?

R : Test d'embauche
Répétition d'actions de formation et d'information
Analyse des risques sur les processus et sur les matériels de production (politique HACCP)
Mise en place de systèmes de protection ou d'information
Mise en place de procédures et d'instructions de travail
Contrôles quotidiens sur les matières premières et les produits finis
Contrôles périodiques et inopinés réalisés par des auditeurs internes ou externes formés sur la sécurité, l'hygiène, l'ordre et la propreté des locaux et des machines
Cahier d'enregistrement des demandes du personnel en matière d'amélioration des matériels ou des conditions de travail avec obligation de réponse écrite, dans le mois qui suit, de la part de la hiérarchie

3.5 - Quels sont les principaux problèmes que vous avez rencontrés pour réduire ces vulnérabilités ?

R : Coûts en temps passé et en investissements
Quasi impossibilité de supprimer l'acte de malveillance intentionnelle

3.6 - Quelles sont les aides ou les conseils dont vous avez bénéficié pour réduire ces vulnérabilités ?

R : Conseils techniques de la part des assureurs, des bureaux de contrôle, de la médecine du travail, de la CRAM

3.7 – Avez-vous impliqué votre personnel (formation, information) ?

R : Le personnel est constamment impliqué.
Par ailleurs nous le tenons informé, par le biais des réunions avec les représentants du personnel, de l'évolution de nos activités, des résultats économiques, des gains ou pertes de clients, des éventuelles réclamations de clients

3.8 – Comment le personnel a-t-il accueilli toutes les mesures pour réduire ces vulnérabilités ?

R : Très bien, avec le sentiment que l'ensemble de la hiérarchie est à son écoute

3.9 – Avez-vous communiqué vers l'extérieur (clients, sous-traitants partenaires, administration, assureurs) ?

R : Très peu, sauf au cours des audits des clients, de l'administration et des assureurs

3.10 - Quels conseils donneriez-vous à une entreprise qui souhaite réduire ces vulnérabilités ?

R : Impliquer sans a priori ses interlocuteurs assureurs afin de bénéficier de leurs compétences
Faire participer aux diagnostics et à l'élaboration des solutions tous les acteurs de l'entreprise sans distinction hiérarchique.
Mettre en place des indicateurs

Mettre en place une cellule de crise et définir a priori les méthodes de communication
Imaginer plusieurs scénarii de crise (incendie, acte de malveillance sur un produit, produits non-conformes commercialisés, etc.), estimer leurs conséquences humaines et financières et les moyens ou politiques éventuellement à mettre en place a priori (avant l'incident pour l'éviter) ou a posteriori (pour le traiter avec le minimum de dégâts).

7.2. Deuxième entreprise

1 - Présentation de l'entreprise

1.1 - Quel est le secteur d'activité de l'entreprise ?
R : Traitement de déchets industriels liquides et valorisation matière (vente d'équipements et prestations de service) - Stockage de produits pétroliers - Lavage interne d'unités fluviales.

1.2 - Quelle est la taille de l'entreprise (nombre de personnes et chiffre d'affaire) ?
R : 40 salariés / CA 2007 : 8 093 K€

1.3 – L'entreprise possède-t-elle plusieurs sites d'exploitation ?
R : Non

1.4 - Le secteur d'activité est-il très concurrentiel ?
R : Oui, très concurrentiel.

1.5 – L'entreprise a-t-elle des secrets de fabrication ou des informations stratégiques à protéger ?
R : Non

1.6 – L'entreprise fait-elle appel à des sous-traitants partenaires pour une partie de sa production ?
R : Oui, partenaires intervenant sur notre site.

1.7 – L'entreprise exporte-t-elle une partie de sa production ou de ses services et vers quels pays ?
R : Oui : environ 4 % - vers l'Union Européenne et les Etats-Unis.

1.8 – L'entreprise travaille t-elle avec des produits dangereux (inflammables, explosifs, corrosifs, toxiques,…) ?
R : Oui : avec des produits inflammables et corrosifs.

2 - Situation de l'entreprise vis-à-vis des actes de malveillance ou de négligences

2.1 – L'entreprise a-t-elle subi des actes de malveillance interne ou externe ?
R : Non

2.2 - Quelles en ont été les conséquences internes ou externes pour l'entreprise ?
R : -

2.3 – L'entreprise a-t-elle été victime d'incidents ou d'accidents dus à des négligences de votre personnel ?
R : Non

2.4 - Quelles en ont été les conséquences internes ou externes pour l'entreprise ?
R : -

3 - Actions de l'entreprise vis-à-vis des risques de malveillance ou de négligences

3.1 - Quelles raisons vous ont convaincu d'agir pour réduire vos vulnérabilités vis-à-vis de la malveillance interne ou externe ?
R : -

3.2 – Quelles mesures avez-vous mises en place pour réduire ces vulnérabilités ?

R : Mesures de surveillance malveillance/incendie :

Barrières infrarouges anti-intrusion et détection d'intrusion sur les clôtures
Présence d'un gardien la nuit et le week-end
Limitation des points d'entrée sur le site

3.3 - Quelles raisons vous ont convaincu d'agir pour réduire vos vulnérabilités vis-à-vis des négligences ?
R :

3.4 – Quelles mesures avez-vous mises en place pour réduire ces vulnérabilités ?
R : De la veille technique et de la surveillance.

3.5 - Quels sont les principaux problèmes que vous avez rencontrés pour réduire ces vulnérabilités ?

R : La sûreté n'est pas forcement compatible avec la sécurité

3.6 - Quelles sont les aides ou les conseils dont vous avez bénéficié pour réduire ces vulnérabilités ?

R : Assureurs et administration

3.7 – Avez-vous impliqué votre personnel (formation, information) ?
R : Le personnel est impliqué par des actions de sensibilisation.

3.8 – Comment le personnel a-t-il accueilli toutes les mesures pour réduire ces vulnérabilités ?
R : Très bien, le personnel a manifesté une bonne écoute.

3.9 – Avez-vous communiqué vers l'extérieur (clients, sous-traitants partenaires, administration, assureurs) ?
R : Très peu, uniquement vers l'administration et les assureurs

3.10 - Quels conseils donneriez-vous à une entreprise qui souhaite réduire ces vulnérabilités ?
R : Sans réponse

7.3. Troisième entreprise

1 - Présentation de l'entreprise

1.1 - Quel est le secteur d'activité de l'entreprise ?
R : Métallurgie.

1.2 - Quelle est la taille de l'entreprise (nombre de personnes et chiffre d'affaire) ?
R : 180 personnes

1.3 – L'entreprise possède-t-elle plusieurs sites d'exploitation ?
R : Oui.

1.4 - Le secteur d'activité est-il très concurrentiel ?
R : Le secteur d'activité est concurrentiel.

1.5 – L'entreprise a-t-elle des secrets de fabrication ou des informations stratégiques à protéger ?
R : Oui pour les deux domaines.

1.6 – L'entreprise fait-elle appel à des sous-traitants partenaires pour une partie de sa production ?
R : Oui, sous-traitance intervenant sur site.

1.7 – L'entreprise exporte-t-elle une partie de sa production ou de ses services et vers quels pays ?
R : Non communiqué.

1.8 – L'entreprise travaille t-elle avec des produits dangereux (inflammables, explosifs, corrosifs, toxiques,…) ?
R : Oui, les produits étant inflammables et corrosifs.

2 - Situation de l'entreprise vis-à-vis des actes de malveillance ou de négligences

2.1 – L'entreprise a-t-elle subi des actes de malveillance interne ou externe ?
R : Non

2.2 - Quelles en ont été les conséquences internes ou externes pour l'entreprise ?
R : -

2.3 – L'entreprise a-t-elle été victime d'incidents ou d'accidents dus à des négligences de votre personnel ?
R : Non

2.4 - Quelles en ont été les conséquences internes ou externes pour l'entreprise ?
R : -

3 - Actions de l'entreprise vis-à-vis des risques de malveillance ou de négligences

3.1 - Quelles raisons vous ont convaincu d'agir pour réduire vos vulnérabilités vis-à-vis de la malveillance interne ou externe ?
R : Risques d'attentats sur nos stockages de produits chimiques, risque de vol

3.2 – Quelles mesures avez-vous mises en place pour réduire ces vulnérabilités ?
R : Gardiennage 24h/24 et 365 jours/an
Surveillance vidéo

3.3 - Quelles raisons vous ont convaincu d'agir pour réduire vos vulnérabilités vis-à-vis des négligences ?
R : -

3.4 – Quelles mesures avez-vous mises en place pour réduire ces vulnérabilités ?
R : -

3.5 - Quels sont les principaux problèmes que vous avez rencontrés pour réduire ces vulnérabilités ?
R : -

3.6 - Quelles sont les aides ou les conseils dont vous avez bénéficié pour réduire ces vulnérabilités ?
R : Aide d'un cabinet extérieur spécialisé en sûreté

3.7 – Avez-vous impliqué votre personnel (formation, information) ?
R : Le personnel est impliqué par des actions de sensibilisation.

3.8 – Comment le personnel a-t-il accueilli toutes les mesures pour réduire ces vulnérabilités ?
R : Très bonnes réactions.

3.9 – Avez-vous communiqué vers l'extérieur (clients, sous-traitants partenaires, administration, assureurs) ?
R : Des communications avec les sous-traitants, l'administration et les assureurs, absolument pas vers les clients.

3.10 - Quels conseils donneriez-vous à une entreprise qui souhaite réduire ces vulnérabilités ?
R : Se faire aider de spécialistes en sûreté.

INGENIEURS ET SCIENTIFIQUES DE FRANCE

Cet ouvrage a été réalisé par le

Comité Sécurité Industrielle des Ingénieurs et Scientifiques de France (IESF),

Sous la direction de :

Hubert	**ROUX**	IESF

Avec la collaboration des membres actifs du groupe de travail :

Jean-Marie	BUSCAILHON	IESF
Toussaint	COPPOLANI	IESF/PRAXIS
Jean	DELAHAYE	IESF
Jean-Claude	FORESTIER	IESF/TOTAL
Pascal	GAVID	IESF/AGREPI
Gilles	GUITAUT	IESF/CGPME
Caroline	OLIVIER	IESF/UNIVERSITE DE ROUEN
Gérard	ORDIALI	IESF/CGPME
Guy	PLANCHETTE	IESF/IMdR
Patrick	RUBISE	IESF/IMdR
Bruno	WILTZ	IESF

Les membres du groupe déplorent la disparition prématurée de

Yvan	VEROT	qui a pris une part active aux travaux du groupe

Et remercient les dirigeants de PME qui ont participé à certaines séances et accepté de témoigner.

Réalisé en 2006/2007, cet ouvrage a été réactualisé en 2011, car le sujet reste malheureusement d'une grande actualité.