

Comment parer les menaces dans les PME-PMI

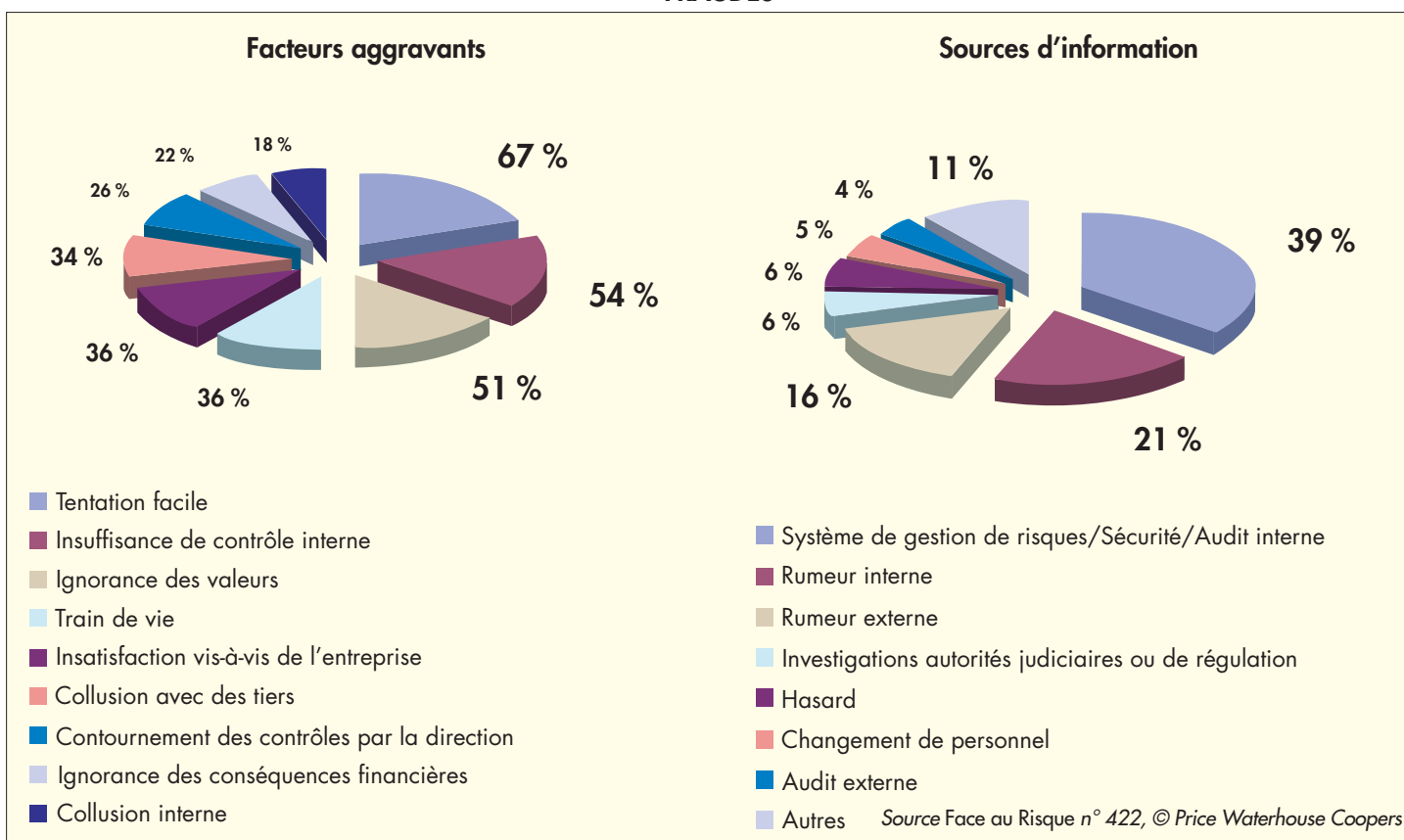
Face aux fraudes, négligences et autres malveillances qui les mettent en danger, les PME-PMI doivent analyser leurs vulnérabilités et mettre en place une organisation permettant d'éviter le pire

La prévention des risques ne peut plus être ignorée aujourd'hui dans les entreprises, tant par les dirigeants que par les personnels. Mais, dans le domaine de la sûreté-malveillance, force est de constater que les négligences, les fraudes et autre vols qui menacent les entreprises, notamment les petites et moyennes entreprises et industries (PME-PMI), ne sont que peu ou pas pris en compte dans les analyses de risques. Pourtant, ces actes, qu'ils soient d'origine interne ou externe à l'entreprise, entraînent

de nombreux dommages. Le Comité de sécurité industrielle du CNISF (Conseil National des Ingénieurs et Scientifiques de France) a estimé nécessaire d'alerter les dirigeants de ces PME-PMI et de leur proposer une méthode d'analyse simple et adaptable, ainsi que des solutions de prévention et de protection.

Ces actes de malveillance peuvent survenir dans toutes les entreprises, quelle que soit leur taille. Mais les dirigeants de PME ne disposent pas des mêmes moyens

FRAUDES



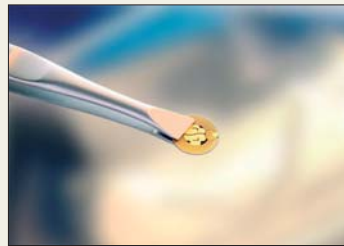
que les grandes entreprises. Ils choisissent alors d'autres priorités, pensant que la dimension de leur entreprise, la connaissance de leur personnel, la qualité des relations existantes les mettent à l'abri de ce type d'actions. Pourtant, aucune entreprise n'est à l'abri, même si les entreprises françaises se montrent discrètes sur le sujet et avouent rarement avoir subi des préjudices, signes d'un manque de vigilance ou d'un mélange de honte, de pudeur et de peur.

Le facteur humain dans le risque

Aux États-Unis, le coût annuel de cette criminalité dépasse les 200 milliards de dollars ; 30 % des faillites de PME résulteraient de la malhonnêteté des salariés. En Belgique, selon une étude statistique récente, la moitié des PME « se déclarent affectées par des problèmes de délinquance ». Dans l'Hexagone, il n'existe pas de telles statistiques, car le sujet reste tabou et les témoignages anonymes. Tout chef d'entreprise vit personnellement la fraude comme un traumatisme et redoute l'effet négatif que pourrait avoir l'ébruitement de l'affaire sur l'image de sa société.

Ces actes de malveillance peuvent revêtir différents aspects : incendies, vols, accidents, sabotages de machines, falsifications de documents, copies de brevets, contrefaçon, débauchage de personnel... Ils représentent des risques élevés pour l'entreprise, pouvant impliquer pertes d'explo-

Faiblesses des systèmes d'information



Technologie RFID

La dépendance vis-à-vis des systèmes d'information est très forte. Les savoirs sont plus largement diffusés sous forme numérique, les acteurs sont plus nombreux, avec des interconnexions de réseaux. L'informatique est partout : dans les badges, les étiquettes des produits de radio-identification (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, a été généralisé pour gérer les réseaux interne. 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, les télédéclarations... La concurrence est exacerbée dans certains secteurs de haute technologie, où les entreprises se dotent d'outils de veille et d'analyse très puissants. L'externalisation des services informatiques est de plus en plus souvent la règle, allant jusqu'à des sous-traitances offshore.

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. La large diffusion des failles techniques et des outils de piratage, d'une grande simplicité d'usage, contribue à développer la délinquance informatique.

tation et détérioration de l'image, voire des conséquences plus dramatiques. Par exemple, en cas d'incendie, les sinistres peuvent être déterminants sur le plan économique, mais aussi tragiques sur le plan humain. Autre exemple, les menaces sur les systèmes informatiques sont de plus en plus fréquentes. Selon une enquête menée en France dès 1998, les pertes, toutes catégories confondues, atteignaient 2,8 milliards d'euros. Et elles ne cessent d'augmenter.

Analyses de vulnérabilité et retour d'expérience

Les principales menaces viennent autant de l'intérieur que de l'extérieur. La plus fréquente est le détournement de matériel de son circuit habituel. Suit le détournement de 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. Par ailleurs, les personnes qui s'autorisent des écarts et mettent l'entreprise en danger ont sou-

vent, pour ceux qui les côtoient, un profil de « parfait collaborateur ». Si des grands groupes peuvent survivre, plus ou moins bien, à ces attaques, la situation peut être fatale pour les PME et PMI.

L'efficacité du dispositif de prévention et de protection de ces actes repose sur le degré de sensibilisation et d'implication du personnel. Tout d'abord, l'implication du dirigeant est une condition impérative de l'efficacité du dispositif. A lui de décider de mettre en place une démarche dans le but de protéger les biens dont il a la charge, parfois même la propriété. Il est le mieux placé, car il dispose de la connaissance la plus globale de l'entreprise et il est responsable des enjeux techniques, stratégiques et financiers. Son implication est d'autant plus nécessaire que nous assistons à des évolutions inéluctables pour les PME et PMI. De plus en plus de donneurs d'ordre, qui travaillent en flux tendu, veulent se garantir de la défaillance possible de leurs partenaires sous-traitants et fournisseurs. Les banquiers et actionnaires veulent des

Des facteurs, comme l'inadaptation des moyens ou encore l'éthique, entrent en jeu dans les causes des accidents.

L'approche cindynique

Elle propose un regard global sur les risques et peut s'appliquer à ceux liés à la malveillance. L'approche cindynique s'appuie sur une grille de lecture composée de déficits souvent à l'origine de sinistres :

- les déficits culturels : sentiment d'inafaillibilité, simplisme, non-communication, orgueil ;
- les déficits organisationnels : subordination des fonctions de gestion de risques aux fonctions de production, dilution des responsabilités ;
- les déficits managériaux : absence de retour d'expérience, d'approche globale, de culture de sécurité, de gestion de crise.

Des outils simples pour évaluer et réduire la vulnérabilité de l'entreprise

La brochure, réalisée par le Comité de sécurité industrielle du CNISF, présidé par Hubert Roux, propose un questionnaire permettant d'évaluer la sensibilité de l'entreprise, vis-à-vis des risques, en fonction des mesures techniques ou organisationnelles de réduction, existantes ou à mettre en place. Trois niveaux de mesures sont proposés, en fonction de la sensibilité de l'entreprise. La brochure recense également les menaces qui pèsent sur les systèmes d'information et propose une liste de mesures à mettre en œuvre. www.cnisf.org

Les accidents diffus, notamment les accidents de la route, les accidents du travail et les accidents domestiques, font de nombreuses victimes. Les statistiques sont malheureusement encore pauvres et la perception du risque n'est pas en adéquation avec la réalité.

garanties quant à leurs enjeux financiers. Les assureurs exigent une réduction des risques encourus avant d'accorder leurs garanties. Et la concurrence nationale et internationale est féroce.

C'est pourquoi il est impératif de mener une analyse de vulnérabilité de l'entreprise. Elle a pour objectif d'identifier les points névralgiques, cibles potentielles d'actes non souhaités et susceptibles de mettre l'entreprise en difficulté, voire en péril. A chaque point névralgique correspondent deux critères : la fréquence avec laquelle une menace peut le solliciter et la gravité, c'est-à-dire l'impact ou la conséquence de la réalisation de la menace sur ce point. Les évaluations recensées sont réunies sur un tableau à deux axes (fréquence et gravité) permettant une représentation graphique de tous les risques jugés possibles. 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 appel à un prestataire (consultant spécialisé, ingénieur prévention de compagnie d'assurance) qui a toutes les compétences, la formation et l'expérience nécessaires. Par ailleurs, le retour d'expérience est essentiel. Les incidents et accidents devront être analysés sous différents aspects (coûts, pertes de production, perte de clients, impact sur l'image de l'entreprise...), selon différents critères (nature de l'événement, origine de la menace, cibles supposées...).

Il sera ensuite possible de définir une politique de sécurité. Celle-ci permet de hiérarchiser les

actions à entreprendre pour ramener les niveaux de risques à des valeurs acceptables. Pour que les progrès soient durables, il faut mettre en place des moyens de contrôle périodiques. Les mesures dépendront de la vulnérabilité de l'entreprise, de sa taille et de ses activités. L'expérience montre que certaines mesures doivent dans tous les cas être envisagées : organisation de l'entreprise et définition des responsabilités, identification des dangers et des points sensibles, consignes et procédures mises à jour, exercices d'entraînement, 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, connaissance et respect des réglementations, prise en compte des remarques des assureurs, des donneurs d'ordres, des clients, des consultants.

Mobiliser l'entreprise

Pour motiver et mobiliser l'entreprise à la lutte contre le risque, il appartient à la direction générale de l'entreprise de donner et de maintenir l'impulsion nécessaire. Avec, tout d'abord, une organisation structurée. Il est souhaitable de confier cette mission de coordination à un responsable délégué par la direction, doté des pouvoirs et des moyens inhérents à sa mission. Ensuite, 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. C'est au stade de la mise en œuvre de la politique de sécurité que l'effort de concertation, d'explication et de formation doit être développé pour que les personnels qui vont subir les contraintes inhérentes à la mise en œuvre de ces mesures, aient bien conscience qu'ils en seront tous les principaux bénéficiaires. ■

Pascal Gavid

Conseil d'Administration de l'AGREPI
CNISF