Laurent
COMBALBERT

Entreprises : halte aux prédateurs !

DUNOD

Laurent COMBALBERT

Entreprises : halte aux prédateurs !

DUNOD

Illustration de couverture :

Hervé Pinel

ISBN 978-2-10-053579-8

TABLE DES MATIÈRES

PARTIE III

LES MENACES D'ATTEINTE À L'IMAGE

PARTIE IV

LES MENACES D'ATTEINTES AUX BIENS

PARTIE V

LES MENACES D'ATTEINTES AUX PERSONNES

INTRODUCTION

« La stratégie d'une entreprise est l'ensemble des décisions destinées à adapter, dans le temps et l'espace, les ressources de la firme aux opportunités et aux risques d'un environnement et de marchés en mutation constante »

Octave Gélinier[1]

DU 11 SEPTEMBRE AU H5N1 : VERS UNE NOUVELLE CULTURE DU RISQUE

Confiance et risque sont les deux piliers d'une économie florissante et prospère. Confiance car les investisseurs, les collaborateurs, les pouvoirs publics, les clients ont besoin de savoir à qui ils ont à faire et de s'engager dans la durée. Risque car « qui ne risque rien n'a rien », a fortiori dans le monde des affaires. Ces deux notions ne sont pas antagonistes, bien au contraire : combinées de façon stratégique, elles s'avèrent redoutables et permettent aux sociétés qui savent les utiliser de gagner le haut du pavé et d'y rester. Mais l'entrepreneur se trouve parfois pris dans une vision quasi schizophrène de son environnement : il lui faut prendre des risques et se montrer audacieux pour pénétrer des marchés nouveaux, tout en faisant preuve d'une prudence sans cesse rappelée par tous les acteurs économiques cherchant vainement à garantir le risque-zéro.

Beaucoup de managers et de chefs d'entreprise aiment à penser que leurs prises de risque sont calculées. Ils font

1. *Le secret des structures compétitives*, 1966.

souvent reposer l'analyse des risques qu'ils prennent sur les méthodes analytiques et les calculs de probabilités. Cette importance accordée aux mathématiques n'est pas nouvelle en économie, mais elle pousse parfois à l'enfermement dans des modèles statistiques déconnectés de la réalité. Le risque est souvent défini comme une adéquation entre la probabilité d'occurrence d'une menace et sa gravité potentielle. Il est pourtant bien difficile de mettre le risque en équation et de l'affecter d'un ratio présumant sa survenue et/ou sa criticité. Cette nécessité de relativiser les définitions classiques du risque s'explique d'autant plus que l'environnement économique évolue vers un système complexe. Complexe mais non compliqué, et la différence est de taille pour appréhender les nouvelles menaces qui pèsent sur les entreprises. Bon nombre d'acteurs du monde des affaires pensent que le contexte dans lequel ils évoluent est compliqué, ce qui tend à expliquer pour eux les difficultés qu'ils peuvent avoir à anticiper leurs risques. Or, leur environnement est juste complexe, ce qui est une grande chance et sources d'opportunités.

DE LA COMPLICATION À LA COMPLEXITÉ

Une situation compliquée est une situation dans laquelle tous les paramètres qui la composent ne sont pas perçus, ce qui accentue d'autant l'impression de complication. Ce manque de perception peut être dû au fait que les paramètres ne sont pas observables, ou qu'ils sont liés à des éléments qui ne sont pas sous le contrôle de celui qui fait l'analyse. Il arrive parfois que ce manque de perception soit lié à des mécanismes de défense psychologiques : le déni, la

dénégation, la rationalisation sont autant de voies de secours inconscientes servant à ne pas voir l'ensemble des facteurs qui agissent sur un environnement et qui le rendent incertain.

Au contraire, une situation complexe est une situation dans laquelle tous les paramètres sont perçus, y compris ceux qui s'avèrent perturber le bon fonctionnement de l'organisation. En refusant de simplifier et en acceptant l'ensemble des contraintes qui agissent sur l'environnement économique, y compris les contraintes non conventionnelles, il est possible d'opérer une analyse objective et fiable des risques potentiels et de s'y préparer dans les meilleures conditions. L'acceptation de la complexité d'un environnement incertain est un gage de bonne perception des risques, et notamment des menaces nouvelles planant au-dessus des projets de demain : plus il y a de paramètres dans un contexte ou une situation, plus il y a d'opportunités à saisir et de leviers sur lesquels jouer.

L'ÉMERGENCE DE NOUVELLES MENACES

Une étude réalisée par la société de conseil Accenture, intitulée *Business in a fragile world*[1], montre à quel point l'environnement du monde des affaires évolue. Depuis le début des années 2000, de nouveaux paramètres sont apparus et ont bouleversé l'appréhension du risque par les entreprises : accroissement de l'insécurité internationale, augmentation du nombre de pays en proie à l'instabilité politique, changement dans les modes opératoires des

1. www.accenture.com

groupes terroristes et contestataires, immiscion de groupes criminels et mafieux dans les relations commerciales, guerre concurrentielle à couteaux tirés, hyperréactivité des medias et des vecteurs d'échanges d'information, autant de facteurs générant des risques inédits et non conventionnels.

Ces menaces nouvelles ne relèvent pas du périmètre traditionnel de la gestion des risques. Leur dimension systémique et leur caractère idiosyncrasique n'arrangent rien : mondialisation des échanges et des relations commerciales, accroissement des financements internationaux et des mouvements de capitaux, économies interconnectées avec de forts risques de contagion, volatilité de l'image et de la réputation des entreprises, actions malveillantes dans un but concurrentiel, criminel ou politique sont le nouveau terreau des menaces non conventionnelles.

Les nouvelles menaces					
	Atteintes économiques	**Atteintes à l'image**	**Atteintes aux biens**	**Atteintes aux personnes**	**Atteintes à l'information**
Origine interne	Fraudes OPA	Communication de crise Corruption	Vols Contamination	Harcèlement	Débauchage Espionnage
Origine externe	OPA Partenaires malveillants	Rumeurs Risque sectaire	Contrefaçon Vols Contamination	Terrorisme Kidnapping Racket Pandémie	Espionnage Attaques informatiques Cyberextorsion

Ces nouveaux prédateurs prennent plusieurs formes et agissent selon des modes opératoires extrêmement adaptables et particulièrement efficaces. On retrouve parmi eux plusieurs grandes familles de menaces :

• ***Les menaces nouvelles :*** elles sont rarement survenues, ou sont nées d'un nouveau contexte ou d'une situation émergente. C'est notamment le cas des atteintes à l'image et des risques de réputation, nés de la valorisation croissante du capital d'image des grandes marques, qui ont vu leurs noms salis par des rumeurs ou des campagnes de déstabilisation ciblées. C'est également le cas pour les agressions financières, issues de la libéralisation des échanges de capitaux.

• ***Les nouvelles formes de menaces anciennes :*** celles-ci ne sont pas à proprement parler nouvelles, mais leurs modes opératoires évoluent et en modifient la perception et l'impact. C'est le cas du kidnapping, pratiqué depuis des siècles, mais encouragé par la multiplication des déplacements de cadres expatriés dans des zones peu sécurisées. Le racket et l'extorsion suivent la même tendance : pratiques très anciennes, elles sont remises au goût du jour par des groupes mafieux et criminels saisissant toutes les opportunités, comme la contamination malveillante de produits alimentaires dans le but de soutirer de l'argent aux marques distributrices. Le terrorisme enfin, par ses nouvelles formes et ses cibles, change de visage et de mode de perception dans le monde de l'entreprise.

• ***Les menaces polymorphes :*** une seule menace peut prendre des formes extrêmement variées, obligeant ceux qui la combattent à réadapter sans cesse leurs dispositifs de protection et de prévention. C'est le cas de l'espionnage

économique, dont les acteurs ne cessent de changer de façon d'agir en fonction des contre-mesures utilisées par leurs cibles.

• ***Les nouveaux vecteurs de menaces :*** en utilisant les nouvelles technologies et les nouveaux moyens de communication, les prédateurs créent des menaces vectorielles, comme les attaques informatiques et les cyber-extorsions. Les vecteurs peuvent aussi être animaux ou humains, comme dans les situations de pandémies grippales (virus H5N1 ou maladie de la vache folle).

L'origine de ces risques est généralement malveillante, résultant de la volonté d'un ou plusieurs agresseurs. Ce qui a des conséquences sur la manière de les aborder : anticiper et gérer un risque opérationnel ou accidentel n'a jamais été une chose facile, même lorsque les organisations se dotent de structures dédiées et de risk managers spécialisés. Alors, que dire de menaces générées par des esprits mal attentionnés, malveillants, voire en proie à une psychopathologie ou une volonté perverse ? Comment agir ou réagir face à un risque qui s'adapte aux réponses anticipées ou appliquées par la cible, qui esquive les moyens de prévention au fur et à mesure de leur mise en œuvre, qui attaque sur les flancs quand on l'attend en face, qui utilise la technologie pour prendre la victime à son propre piège ?

Sans se vouloir alarmiste, cet ouvrage cherche à mettre en exergue un certain nombre de situations non conventionnelles que connaissent les entreprises aujourd'hui et qui ne manqueront pas de se multiplier dans les années qui viennent. En étant conscients du risque, et se montrant prêts à adapter leurs réponses aux situations nouvelles, les dirigeants

et les chefs d'entreprises pourront continuer à développer leurs activités en toute sérénité.

Note de l'auteur :

Un certain nombre d'affaires évoquées dans cet ouvrage sont volontairement blanchies pour ne pas nuire aux personnes ou aux entreprises qui en ont été les victimes. Les prénoms des responsables et les secteurs professionnels ont parfois été modifiés pour préserver leur anonymat.

PARTIE 1

LES MENACES FINANCIÈRES ET ÉCONOMIQUES

1

OPA ET AGRESSIONS FINANCIÈRES

« 421 entreprises françaises ont été rachetées en 2005, pour un montant de 37 milliards d'euros »

Rapport de l'AFII[1]

DES MOUVEMENTS DE CAPITAUX PARFOIS HOSTILES

La fin du XX^e^ siècle et le début du XXI^e^ sont indubitablement marqués par une accélération fabuleuse de la croissance des transactions financières et des mouvements de capitaux. Les études démontrent l'accroissement des entrées de capitaux dans les pays en développement, et la part des capitaux privés ne cesse d'augmenter dans l'économie mondiale. La mondialisation et la libéralisation des échanges, l'émergence de grandes puissances économiques comme l'Inde ou la Chine ont encore attisé ce phénomène au cours des cinq dernières années. Ce mouvement n'est d'ailleurs pas nouveau : le traité de la Communauté européenne impose, depuis 1957, la libéralisation des mouvements de capitaux entre pays membres et pose même ce principe comme une liberté fondamentale de l'Union.

Dans ce grand carrousel financier, la France est un pays qui attire les capitaux. Un rapport publié par l'Agence fran-

1. Rapport 2006 de l'Agence Française des Investissements Internationaux.

çaise pour les investissements internationaux établit que la France est la quatrième destination privilégiée des capitaux dans le monde, juste derrière le Royaume-Uni, la Chine et les États-Unis. Ce même document montre la proactivité des entreprises françaises dans des pays étrangers, puisqu'elles réalisent un grand nombre d'investissements ou d'acquisitions. Il n'est pas rare que les acquisitions soient faites au moyen d'une Offre Publique d'Achat : il s'agit d'une proposition faite par une entreprise à tous les actionnaires d'une autre entreprise de lui vendre leurs actions à un prix donné. Ces OPA peuvent être dites « amicales », c'est-à-dire qu'elles sont « négociées » par l'entreprise cible, voir même parfois sollicitées par elle. Pourtant, dans de nombreux cas, l'OPA est dite « hostile », car non sollicité par les dirigeants de la société qui en fait l'objet.

L'objectif d'une OPA peut être multiple : acheter une entreprise dans un but de croissance externe ou pour compléter une offre globale, acquérir un savoir-faire ou une clientèle, faire un coup financier et réaliser une plus-value conséquente, ou déstabiliser un concurrent en l'acquérant tout bonnement ou en acquérant ses partenaires stratégiques.

L'OPA de Mittal sur Arcelor a attiré l'attention du grand public sur ce phénomène, quand chacun s'est aperçu qu'un pan industriel de l'économie d'un pays pouvait être acquis par un concurrent étranger, au risque de pertes d'emplois et de restructuration draconiennes. Économiquement, cette opération se justifie car les deux entreprises se complètent dans leurs offres et leurs positionnements géographiques. Stratégiquement, l'opération est risquée car

elle menace l'Europe d'une perte de contrôle sur un secteur sensible de son économie, ainsi que d'un transfert de technologie et de main-d'œuvre.

Les investissements « agressifs » ne sont pas le seul apanage des capitalistes privés. Depuis quelques années, les fonds souverains ont fait leur entrée dans le jeu économique.

Les principaux fonds souverains		
Abu Dhabi Investment Authority	Émirats Arabes Unis	625 milliards $
Government Pension Fund-Global	Norvège	322 milliards $
Government of Singapore Investment Corp.	Singapour	215 milliards $
Reserve Fund for Future Generation	Koweït	213 milliards $
China Investment Corporation	Chine	200 milliards $
Stabilisation fund	Russie	127 milliards $
Temasek Holdings	Singapour	108 milliards $
Qatar Investment Authority	Qatar	60 milliards $

Les fonds souverains sont des acteurs puissants et incontournables de la finance mondiale. Créés et gérés par des gouvernements, ils permettent d'investir un surplus de richesse et générer des plus values importantes. C'est le cas notamment de la Norvège, qui investit les fonds tirés de sa ressource pétrolière dans l'économie mondiale. Beaucoup d'autres pays producteurs de pétrole en font de même. Abu

Dhabi possède un des plus importants fonds souverains, avec un capital évalué à environ 625 milliards de dollars. La crainte des pays qui attirent ces fonds est de voir leurs gouvernements d'origine utiliser ces investissements pour des raisons géopolitiques et non pour des raisons purement économiques. Les pays du G7 ont d'ailleurs appelé les États investisseurs à respecter un code de bonne conduite, en sollicitant notamment un peu plus de transparence de la part des fonds souverains.

Face à ce phénomène et au risque qu'il fait courir aux entreprises françaises, le gouvernement a fait adopter plusieurs mesures pour stabiliser l'actionnariat des entreprises et pour lutter contre les OPA non sollicités ou les entrées « agressives » de capitaux. Le décret du 31 décembre 2005, qui applique la loi du 9 décembre 2004, permet au gouvernement français de s'opposer à un investissement étranger dans une entreprise relevant de la défense nationale ou dont l'activité se révèle stratégique pour le pays, 11 secteurs d'activité ayant été énumérés dans le texte.

Des mesures visant à réduire le risque d'OPA agressives ont également été adoptées, transposant en ce sens les directives de l'Union européenne en la matière.

MITTAL SAUTE SUR ARCELOR, DANONE ÉCHAPPE À PEPSI

Il est intéressant de comparer l'OPA menée par Mittal contre Arcelor et la tentative avortée de Pepsi contre Danone. Deux acquisitions potentielles, deux traitements différents, deux issues opposées.

Le groupe indien Mittal lançait en 2006 une Offre Publique d'Achat contre le groupe métallurgique européen Arcelor. Arcelor, dirigé un temps par Francis Mer, devenu ensuite Ministre de l'Économie et des Finances, est un des fleurons de la métallurgie européenne. L'opération organisée par Mittal n'a pas soulevé la vague d'indignation qui aurait pu se produire. Pourtant, elle touchait un domaine vital pour le développement économique européen : l'acier est une des bases de ce développement, et la prise de contrôle d'un des leaders de ce secteur par un groupe indien aurait pu susciter une mobilisation plus importante et plus organisée.

Au même moment, une rumeur tenace annonce que le groupe américain Pepsi prépare une action identique sur le groupe Danone. Alors que l'affaire n'en reste qu'au stade du bruit qui court, tout le monde se mobilise pour défendre ce fleuron de l'industrie agroalimentaire européenne. Le patriotisme économique était avancé, et chacun des acteurs du monde économique annonçait ses arguments : Premier Ministre, Ministre de l'Économie, syndicats, consommateurs… L'opération avortait et Danone restait sous son contrôle initial.

Une telle différence de traitement peut paraître surprenante. Pourtant, elle peut s'expliquer par l'importance attribuée par l'opinion publique à chacune de ces sociétés agressées. À l'instar de la thèse développée par Jean-Yves Léger et Thierry Libaert [1], on peut s'apercevoir que l'image d'une entreprise peut être son meilleur bouclier face à une OPA hostile. Si on compare l'image de chacune des deux sociétés, il ressort :

• ***Danone :*** le groupe agroalimentaire a construit son image et sa réputation autour de sa proximité avec le consommateur. Il a une forte image nationale, bien que la France ne représente que 20 % de son chiffre d'affaires et

1. www.communication-sensible.com

14 % de ses effectifs. De plus, Danone fabrique et distribue des produits à destination notamment d'enfants et de bébés, ce qui contribue à lui donner une image d'une grande proximité, quasi familiale.

• ***Arcelor :*** sans image nationale particulière (le groupe Arcelor est basé à Luxembourg), doté d'un management très discret et quasiment inconnu du grand public, Arcelor n'a pas soulevé les passions dans sa confrontation avec Mittal. Peu d'actionnaires se sont mobilisés pour défendre l'entreprise, et la faible représentativité de l'actionnariat salarié (0,9 %) n'a rien arrangé. Les pouvoirs publics n'ont pas manifesté beaucoup plus de volonté de protéger le groupe.

Au-delà du marketing et du développement commercial, l'image d'une entreprise peut aussi s'avérer primordiale dans sa défense contre une OPA ou un agresseur financier. En démontrant son attachement à un pays, à ses consommateurs, à ses actionnaires, à ses collaborateurs, une entreprise peut ériger autour d'elle un mur intangible mais pourtant solide pour susciter l'intérêt des foules et des pouvoirs publics face à une situation difficile.

SE PRÉSERVER D'UNE OPA OU D'UNE AGRESSION FINANCIÈRE

La préservation des entreprises face aux risques d'agressions financières est prise très au sérieux par les gouvernements successifs : l'acquisition d'Arcelor, les rumeurs sur des OPA lancées contre Danone ou Suez, les prises de participation de fond souverains dans des entreprises nationales ont poussé le législateur à encourager les mesures de préservation et de stabilisation du capital des sociétés françaises.

Les dispositifs d'alerte

Il n'est pas toujours facile pour une entreprise cotée en bourse de connaître exactement la composition de son actionnariat. La loi prévoit des dispositifs d'alerte en imposant des seuils au-delà desquels il existe des obligations de déclaration. Ainsi, une entreprise peut avoir connaissance d'une tentative de prise de contrôle : tout rachat de titres permettant de passer au-dessus des 5 %, 10 %, 15 %, 20 %, 25 %, 33 %, 50 %, 66 %, 90 % ou des 95 % du capital ou des droits de vote doit en effet être déclaré, en vertu de l'article L. 233-7 du Code de commerce.

Pour compléter ce système, il existe une obligation pour les actionnaires qui franchissent les seuils de 10 et 20 % de déclarer leurs objectifs pour l'année à venir : souhaitent-ils poursuivre leur stratégie d'achat ? Avec qui agissent-ils ? Souhaitent-ils demander une nomination au conseil d'administration ?

Le contrôle de l'AMF

L'Autorité des Marchés Financiers exerce également un contrôle des OPA potentielles. Inspirée du principe britannique « put up or shut up[1] », cette surveillance permet à l'AMF d'exiger de toute personne ou société dont il y a des motifs raisonnables de penser qu'elle prépare une offre qu'elle déclare ses intentions. L'information qui déclenche l'action de l'AMF peut être une simple rumeur sur les marchés.

1. « Déclare tes intentions ou tais-toi ».

Pactes d'associés et actionnariat salarié

La fidélisation des actionnaires, notamment grâce au développement de l'actionnariat salarié, est un rempart aux OPA et entrées capitalistiques non désirées. Le gouvernement encourage cette fidélisation, notamment par la majoration du dividende des collaborateurs à l'ancienneté. Une étude récente estime que l'actionnariat salarié des sociétés du Cac 40 ne représente que 6 % du capital total, avec quelques exceptions comme c'est le cas pour Air France KLM dont l'actionnariat salarié représente 16 %.

Les pactes d'associés pour contrer des agressions financières sont aussi des outils efficaces : tout ou partie des actionnaires peuvent conclure des ententes confidentielles établissant un certain nombre de règles régissant leurs relations au sein de l'entreprise. Ces pactes d'associés peuvent notamment prévoir des actions concertées pour contrer une OPA ou pour s'engager entre eux dans une logique de non-agression.

Ces pactes peuvent aussi prévoir des actions à retardement, par le biais d'une promesse de cession d'actifs à un associé allié en cas de changement de contrôle de l'entreprise.

Le statut de la société

Opter pour un statut de société séparant le pouvoir de direction du capital est un bon moyen de se prémunir des attaques financières : il est rare qu'un investisseur souhaite prendre le contrôle d'une entreprise sans pouvoir en orienter la stratégie et les décisions. Le statut de société en

commandite répond parfaitement à cette stratégie : la prise de contrôle par un associé commanditaire ne remet pas en cause la direction de l'entreprise commanditée.

Les Bons de Souscription en Action

Cette pratique, inspirée des *Poison Pills*, permet à une société visée par une OPA d'émettre rapidement des bons de souscription en actions (BSA), renforçant ainsi son capital et augmentant de la sorte son prix pour un acquéreur. La société peut ainsi attribuer gratuitement à tous ses actionnaires des bons permettant de souscrire ses actions à des conditions préférentielles. Si l'acquéreur souhaite poursuivre son action, il va devoir revoir son offre à la hausse. Conformément à l'article L.233-32 du Code de commerce, l'émission de BSA est décidée par l'assemblée générale extraordinaire.

Le principe de réciprocité

Deux des trois articles optionnels de la récente directive européenne sur les OPA ont été transposés par la France dans sa législation nationale. L'article 9 encadre les mesures de défense des entreprises : hormis la recherche d'autres offres, elles doivent toutes être confirmées par une assemblée extraordinaire tenue durant la période de l'OPA. L'adoption de l'article 12 de cette même directive européenne a néanmoins assoupli cette obligation. Elle peut en effet être levée si l'initiateur de l'offre n'est pas lui-même soumis aux principes de l'article 9 ou à des « mesures équivalentes » (clause de réciprocité). Cela concerne au final un nombre important de sociétés, allant de l'entre-

prise américaine usant de *poison pills* au fonds de *private equity* en passant par les sociétés de pays européens n'appliquant pas l'article 9, comme c'est la cas pour l'Allemagne.

POUR EN SAVOIR PLUS

de Beaufort V., *Les OPA en Europe,* Economica, 2006.

Viandier A., « *OPA-OPE et autres offres publiques* », Francis Lefebvre, 2006.

2

LES PARTENAIRES MALVEILLANTS

« Près de 50 % des opérations de fusions acquisition capotent du fait d'un manque de fiabilité des cibles »

Un consultant en fusion acquisition

LA LOYAUTÉ N'EST PLUS DE MISE

Les entreprises dont les affaires sont prospères et qui font des profits, envisagent toutes à un moment donné de s'agrandir par une croissance externe : acquérir un partenaire ou monter une joint venture sont des éléments incontournables d'une stratégie de développement, a fortiori pour une entreprise qui souhaite se développer sur des marchés internationaux.

Les motivations qui poussent les entrepreneurs à acheter un partenaire ou à entrer dans son capital sont diverses :

• ***La croissance pure :*** il s'agit là d'accroître la taille et l'activité de l'entreprise. C'est le cas quand une entreprise acquiert une autre entreprise qui exerce exactement les mêmes activités, pour pouvoir tirer profit de son positionnement, de son capital humain, technique et de sa clientèle.

• ***L'acquisition de savoir faire :*** ce type d'acquisition ou de partenariat cible des entreprises qui possèdent un savoir faire spécifique ou qui exploitent un processus de fabrication qui fait défaut à la société à l'origine de l'opération.

• ***L'acquisition de clientèle :*** dans ce cadre, le partenariat vise à capter la clientèle acquise par la société cible. Ce type d'association permet d'acquérir rapidement un volume d'affaire captif car déjà habitué à travailler avec la société cible. Généralement, ces fusions acquisitions sont accompagnées d'une campagne de communication expliquant aux clients tout l'avantage qu'ils vont pouvoir tirer de l'opération.

• ***Le positionnement stratégique :*** la fusion acquisition de positionnement stratégique cherche à installer une entreprise sur un marché sur lequel elle aurait du mal à se positionner seule. C'est notamment le cas d'entreprises qui souhaitent se développer à l'international et qui, pour y parvenir plus efficacement, s'associent ou acquièrent une société locale et tenue par des ressortissants du pays où elles s'installent.

Les opérations de fusions acquisitions ne sont pas simples : elles mettent en relation un certain nombre d'acteurs, dont les objectifs et les attentes ne sont pas forcément complémentaires. Ces discordances entraînent parfois des problèmes d'appréciations mutuelles : les entreprises cibles se méprennent sur les objectifs finaux de celles qui les acquièrent, et celles qui les acquièrent évaluent mal la plus-value qu'elles vont tirer de l'opération. Contrairement à la plupart des pays anglo-saxons, l'audit pré-acquisition n'est pas obligatoire en France. Généralement, une société qui envisage d'en acheter une autre fait réaliser un audit financier pour vérifier la solidité et la fiabilité des comptes de la cible. Mais il est plus rare de faire réaliser un audit stratégique allant au-delà des chiffres qui mette en lumière des aspects moins techniques : la probité des dirigeants, la loyauté vis-à-vis des acquéreurs, l'origine des fonds, la structure exacte du chiffre d'affaire…

Les aspects non-financiers des fusions acquisitions sont de plus en plus complexes dans ce type d'opération, et la problématique de la fiabilité des partenaires se pose de façon parfois dramatique aux acquéreurs. Il existe plusieurs défauts de fiabilité dans le cadre d'une fusion acquisition. Parmi ceux-là, on peut citer :

• ***Le partenaire « incompétent » :*** la cible est au premier abord séduisante, sait mettre en avant ses atouts dans la négociation et parvient à faire réaliser l'opération. Par la suite, l'acquéreur s'aperçoit que les capacités humaines, techniques ou les potentialités de marchés ont été surévaluées.

• ***Le partenaire dispendieux :*** dès lors qu'elle est entrée dans le partenariat, la société cible néglige ses standards de rentabilité au motif que son partenaire pourra assumer les écarts réalisés. Certaines associations se terminent après que la société cible soit entrée dans une certaine euphorie faisant suite à la fusion acquisition.

• ***La coquille vide :*** c'est ce qui arrive aux acquéreurs qui ont affaires à des partenaires malhonnêtes. Dès que l'acquisition est signée, les tenants de l'entreprise cible remontent une autre structure en parallèle qui devient concurrente de la société conjointe. Ils aspirent les meilleures compétences, les savoirs faire et reprennent l'essentiel de la clientèle. Dans certains pays, la notion de concurrence déloyale est très flexible.

• ***Le partenaire « mafieux » :*** c'est ce qui se passe dans le cadre de l'acquisition d'une entreprise dont les dirigeants sont impliqués dans des activités illégales : transport de marchandises illicites, blanchiment de fond, corruption, etc.

• ***Le faux partenaire :*** c'est une pratique qui tend à se développer. Des entreprises peu scrupuleuses attirent leurs concurrents dans des partenariats alléchants au premier abord, dans le seul dessein de leur faire perdre du temps dans leur développement ou de les pousser à des associations contre-productives. Quand l'entreprise piégée s'aperçoit que le partenariat n'est pas viable, elle a déjà perdu une bonne part de son avance sur le marché ciblé.

Une nouvelle notion a fait son entrée dans l'environnement des acquisitions d'entreprises à l'international : le patriotisme économique. Sous couvert de vouloir défendre les intérêts économiques nationaux, des gouvernements s'opposent à des rapprochements de leurs entreprises avec des sociétés étrangères cherchant à se développer sur leur marché. Cependant, certains « veto » ont plutôt pour objectif de modifier la négociation d'acquisition et de tronquer les règles de l'économie. Ainsi, le fonds d'investissement américain Carlyle a revu à la baisse ses prétentions pour l'acquisition du constructeur chinois d'engins de chantier Xugong Group Construction Machinery. Même chose pour le groupe Seb dans sa volonté d'acquérir le fabricant chinois d'articles de cuisine Supor. Dans ces cas, ce sont les partenaires étatiques qui manquent de la fiabilité nécessaire au bon fonctionnement des règles économiques.

MALVEILLANTS & CO

> Une société européenne largement engagée dans l'industrie agroalimentaire décide d'élargir son activité de distribution de boisson dans un pays de l'est de l'Europe. Soucieuse de trouver

le partenaire idéal pour réaliser son implantation, elle procède à l'évaluation de quelques sociétés locales agissant dans la distribution de boissons. Ayant jeté son dévolu sur l'entreprise lui semblant la plus appropriée pour être une cible d'acquisition, la société européenne commence à engager des contacts et à mener une évaluation financière de la cible.

L'entreprise ciblée est une entreprise familiale, qui a réussi à développer son business en créant un solide réseau de distributeurs et de débitants de boissons. Tous les dirigeants sont issus de la même famille, et tous trouvent que l'acquisition par la société européenne est une bonne chose. Seule exigence : tous les dirigeants actuels gardent leurs fonctions, mais un Directeur général issu du staff de l'acquéreur est accepté pour superviser la synchronisation des activités. Dès les premiers mois de l'activité commune, les deux entreprises collaborent avec succès. La société acquéreuse parvient à écouler l'ensemble des stocks prévus dans le business plan, et la société issue de l'acquisition continu à fournir son réseau de distributeurs avec les nouveaux produits. Tout semble fonctionner comme prévu, jusqu'au jour où la police locale vient prendre contact avec le Directeur général. Ce qu'il va entendre va le sidérer : la famille gérant la société est en fait liée à la Mafia locale depuis des années. Les gérants de bars et de débit de boisson clients de la nouvelle entité commune ne sont en fait pas libres de leurs choix : soit ils achètent leurs produits auprès de l'entreprise familiale, soit leur bar devient le lieu de bagarres incessantes et de départs de feux intempestifs. En utilisant la menace et l'intimidation, la famille entretient son business en maintenant la pression sur les clients ainsi soumis. Pourtant, profitant de l'arrivée d'un nouveau management, certaines victimes ont décidé de se plaindre aux forces de l'ordre et de dénoncer ces pratiques. Et le Directeur général n'est pas au bout de ses surprises : sa fonction, et les statuts négociés lors de la transaction, font de lui le responsable légal de la société, et en font donc la personne pénalement responsable des menaces proférées par ses « associés ». Il est amené par la police au commissariat de police, et longuement

> interrogé. Après plusieurs heures, il est libéré mais son passeport lui est confisqué et il se voit interdire de quitter le territoire.

Bien que cette opération ait eu l'air d'être une bonne affaire, elle s'est en fait soldée par un fiasco pour la société acquéreur. Cette dernière a payé un gros montant pour acheter une société criminelle basant son business sur des pratiques mafieuses. D'un point de vue financier, l'acquisition était très rentable, et pour cause : des clients captifs tenus par la force, des prix au-dessus des cours du marché, aucune perte de clientèle, trop craintive des conséquences d'une fin de contrat… Par contre, une investigation de fiabilité aurait assez facilement démontré la malhonnêteté des gérants et évité de tels désagréments à l'acquéreur. Pour éviter qu'il ne passe en jugement, le Directeur général a été discrètement « exfiltré ». Aux dernières nouvelles, la société locale continue son activité criminelle, et a gardé malgré tout les fonds versés par l'acquéreur. L'affaire est toujours en justice…

GARANTIR LA FIABILITÉ DES PARTENAIRES

Savoir identifier le partenaire le plus efficace dans le cadre d'une stratégie de développement est une capacité primordiale pour un entrepreneur. Garantir ensuite sa loyauté et sa fiabilité nécessite d'avoir su encadrer son opération de fusion acquisition d'un certain nombre de mesures préventives.

Le conseil en fusions acquisitions

Le conseil en fusions acquisitions vise à accompagner les dirigeants des entreprises dans des opérations de partena-

riats ou de rachat d'entreprises. Dans ce cadre, les cabinets de conseil peuvent prendre en charge l'étude de marché, l'audit financier voire stratégique, la phase de négociation et la finalisation des documents liés à la transaction.

Il existe plusieurs sortes de cabinets de conseil :

• ***Les banques d'affaires spécialisées :*** Lazard, Goldman Sachs, Rothschild & Cie, Merrill Lynch, JP Morgan, qui accompagnent les opérations majeures de fusions acquisitions.

• ***Les banques généralistes*** ont parfois des services dédiés à la banque d'affaire, intervenant sur des opérations de moyenne importance.

• ***Des cabinets indépendants*** de groupes bancaires et des cabinets d'audit accompagnent aussi les opérations de fusions acquisitions.

• ***Des cabinets d'audits :*** PricewaterhouseCoopers, Deloitte, KPMG.

Ces cabinets de conseil permettent aux entreprises d'éviter les pièges classiques que l'on rencontre dans ce type d'opération, en apportant leurs capacités d'audit et d'anticipation : en posant les bonnes questions et en trouvant les réponses les plus appropriées, le conseil en fusions acquisitions sécurise les opérations de rapprochement.

Le due diligence

Le due diligence est une procédure d'audit spécifique qui doit permettre une juste valorisation de la cible. Il a pour finalité d'apporter une connaissance approfondie de son objectif à l'acquéreur tout en envisageant les risques financiers inhérents à la fusion acquisition. Le due diligence

permet d'envisager les potentiels de création de valeur ajoutée générés par l'opération.

Intervenant en aval de la lettre d'intention dans le processus d'achat ou de partenariat, le due diligence permet à l'acquéreur de vérifier que les différents aspects de l'acquisition ont été correctement négociés, et que leur valeur estimée correspond à la réalité des faits.

Contrairement à ce qui se passe dans les pays anglo-saxons, le due diligence ne répond pas en France à des normes précises. Dès lors, son champ d'application et l'ampleur des investigations réalisées sont établis entre l'acquéreur et le cabinet d'audit chargé de la mission.

L'audit stratégique

L'audit stratégique, plus rarement pratiqué que le due diligence car parfois considéré comme coûteux et inutile, est pourtant une phase importante d'une procédure de fusion acquisition. L'audit stratégique permet à l'acquéreur d'identifier les synergies résultant de l'acquisition et d'examiner les potentialités et les risques qui y sont liées. Il a pour objectif d'envisager le potentiel de développement et de rentabilité de la cible en étudiant entre autre :

– la compétence de l'équipe dirigeante ;
– l'efficacité de la stratégie mise en œuvre ;
– le positionnement stratégique de la société ;
– l'étendue des savoir-faire et des compétences ;
– le potentiel du secteur.

L'audit stratégique vise aussi à anticiper la fongibilité des cultures d'entreprises des deux sociétés qui vont fusionner

ou s'associer. Il peut également sonder des aspects moins pragmatiques, comme l'impact sur les clients et/ou sur les collaborateurs de l'opération et les réactions affectives et émotionnelles qui en résultent.

L'investigation de fiabilité

Au-delà du due diligence, il est possible de mettre en œuvre une investigation de fiabilité. Ce type d'enquête, réalisé par des cabinets spécialisés en intelligence économique, permet de rechercher des informations qui ne sont pas prises en compte par le due diligence. Parmi ces informations, il est possible de travailler sur :

– l'intégrité des dirigeants de la cible ;

– leur réputation dans leur secteur d'activité ;

– leur réelle volonté de collaborer par la suite avec l'acquéreur ;

– leur implication dans l'opération de fusion acquisition.

L'investigation de fiabilité peut se faire au moment de la lettre d'intention et se poursuivre pendant la phase d'acquisition voire même dans les mois qui suivent pour s'assurer du respect des modalités négociées dans l'accord de fusion acquisition.

POUR EN SAVOIR PLUS

Ceddaha F., *Fusions Acquisitions : évaluation, négociation, ingénierie*, Economica, 2007

Lawrence G.M., « *Due Diligence in Business Transactions* », Law Journal, 2007.

3

LES FRAUDES INTERNES

« 40 % des entreprises françaises ont été victimes de fraudes au cours des deux dernières années »[1]

PricewaterhouseCoopers

LES PRÉDATEURS DE L'INTÉRIEUR

Les agresseurs et aigrefins qui s'attaquent aux intérêts des entreprises ne sont pas toujours extérieurs à la société qu'ils prennent pour cible. C'est en tout état de cause ce que révèlent plusieurs enquêtes réalisées par de grands cabinets de conseil : sur les deux dernières années, plus de 3 milliards d'euros auraient disparu du fait de fraudes ou de malversations. Une enquête de PricewaterhouseCoopers, réalisée sur plus de 5000 entreprises, réparties dans presque 40 pays, démontre qu'aucune activité n'est épargnée par le phénomène : assurance, banque, grande distribution, arrivent en tête du palmarès des secteurs touchés, mais tous sont impactés par les agissements de collaborateurs indélicats ou malveillants. Une autre étude, réalisée auprès d'administrateurs et de dirigeants de grandes sociétés par Ernst&Young, a montré que près 85 % des fraudes ont été

1. Étude sur la fraude dans les entreprises en France, en Europe et dans le monde en 2007, PricewaterhouseCoopers, octobre 2007.

perpétrées par des collaborateurs, dont plus de la moitié sont des dirigeants ou des cadres de haut niveau. En outre, 85 % de ces collaborateurs fraudeurs étaient en poste depuis moins d'un an.

Entreprises victimes de fraudes déclarées			
Secteur d'activité	**Entreprises déclarant des fraudes**	**Secteur d'activité**	**Entreprises déclarant des fraudes**
Distribution et consommation	57 %	Communication	40 %
Assurance	57 %	Transport et logistique	37 %
Service public	54 %	Technologie	35 %
Services financiers	46 %	Énergie et extraction minière	35 %
Automobile	44 %	Chimie	35 %
Industrie manufacturière	42 %	Santé	33 %
Divertissement et média	42 %	Aérospatial et défense	33 %
Ingénierie et construction	40 %	Industrie pharmaceutique	27 %
Autres secteurs	47 %		

L'étude de PricewaterhouseCoopers attire aussi l'attention des entreprises sur les pays qui ont été rassemblés sous

l'appellation E7 : bien que les fraudes soient perpétrées dans le monde entier, 7 pays concentrent à eux seuls la moitié des pertes financières liées à de telles actions : il s'agit du Brésil, de la Chine, de l'Inde, de l'Indonésie, du Mexique, de la Russie et la Turquie. Enfin, l'étude indique que les sommes ainsi détournées sont rarement récupérées par les entreprises victimes, précisément dans à peine 38 % des cas.

Il est difficile de définir la notion de fraude de manière globale tant les modes opératoires et motivation des fraudeurs sont variés. Les textes réglementaires, par exemple le règlement CRBF 97-02 sur le contrôle interne ou la réglementation Bâle II, n'ont défini que le risque opérationnel sans rentrer dans le détail. Parmi les actions qualifiées de fraudes, on retrouve notamment :

• ***Les détournements d'actifs de l'entreprise :*** détournements de fond, détournement de biens, abus de biens sociaux, engagements hors bilan.

• ***Les escroqueries :*** carrousel de TVA, cavaleries, fausses factures.

• ***Les ententes :*** avec un concurrent, un fournisseur ou un client, dans le but de détourner des fonds ou des biens.

Face à l'accroissement du phénomène et à l'impact financier grandissant sur les entreprises, celles-ci ont commencé de s'organiser, au travers notamment des réglementations dédiées : la Sarbanes-Oxley, ou SOX, la loi sur la Sécurité Financière, la loi Perben II ou le CRBF 97-02 relatif au contrôle interne et à la lutte anti-fraude en sont des exemples. Ces textes imposent un certain nombre de règles et de pratiques, mais dont l'efficacité dépend avant

tout de l'engagement des dirigeants à les mettre en œuvre. Les procédures de contrôle doivent servir de référentiel, mais seules la motivation de l'ensemble des collaborateurs et la volonté d'aller chercher jusque dans les détails les prémices des actions frauduleuses peuvent initier une véritable politique de prévention du risque. Les chiffres sont d'ailleurs là pour étayer cette affirmation : Malgré l'accroissement des réglementations, les fraudes ne cessent d'augmenter au grand dam des Risk Managers et Compliance Officers. Un certain nombre de dysfonctionnements et de défaillances dans les dispositifs de contrôle continuent de laisser des intervalles aux fraudeurs : le manque de séparation claire entre engagement des dépenses et actions de contrôle, les délais trop longs entre les opérations de contrôle interne, la connaissance des procédures d'investigation par les fraudeurs sont des failles encore trop fréquentes dans les entreprises.

UNE IMAGINATION À TOUTE ÉPREUVE

Les fraudeurs internes ne manquent pas d'imagination pour trouver des moyens de parvenir à leurs fins. Leurs actes visent parfois au détournement de quelques euros par semaine, avec des préjudices pouvant représenter parfois plusieurs millions d'euros après plusieurs années de pratique.

> La SNCF a mis à jour, il y a quelques mois, une fraude simple et bien organisée de la part d'un certain nombre d'agents commerciaux. La compagnie de chemins de fer utilise un logiciel, appelé Mosaïque, pour gérer les émissions de titres de transport. Chaque fois qu'un billet est émis, il est enregistré par le logiciel qui affecte en caisse le montant dudit billet. À la fin de la jour-

née, il est donc aisé de faire un point entre les billets émis et les sommes encaissées. Or, le système ne fonctionnait pas toujours bien, de sorte que certains billets émis n'étaient pas imputés sur Mosaïque. Ce dysfonctionnement technique n'était pas volontaire, mais plusieurs agents commerciaux ayant identifié la faille en ont profité pour vendre des titres de transport et empocher les sommes correspondantes pour leur propre compte. Dès que cette fraude a été éventée, des dispositions techniques ont mis fin à la situation, mais la SNCF est restée très discrète sur le nombre d'agents impliqués ; il semble cependant que les sommes en jeu aient été conséquentes. Certains des fraudeurs, selon leur implication, ont été avertis voire licenciés.

Dans une telle situation, on peut parler de fraude d'opportunité : les fraudeurs n'ont pas causé les conditions des détournements de fond, mais ont profité de failles et de dysfonctionnements pour en tirer un profit personnel.

Gérard a repris la société familiale après trois générations d'entrepreneurs : créée à la fin du siècle dernier, elle est aujourd'hui leader sur son marché sur toute l'Europe. Gérard est entouré de collaborateurs fidèles : pour la plupart dans la société depuis plus de dix ans, ils ont travaillé avec son père et parfois même avec son grand père. Autant dire que la confiance règne, et que les 1200 salariés de l'entreprise partagent les valeurs familiales qui ont présidé à son développement.

M. X, le comptable de la société, fait partie de la garde rapprochée de Gérard. Etant un des plus anciens collaborateurs de son père, il jouit de toute la confiance du management. M. X, qui est à quelques mois de la retraite, souhaite mettre tous ses dossiers en ordre pour passer la main à son remplaçant, Thierry, qui est rejoint la société depuis 6 mois. Le nouveau comptable a peu d'expérience, car diplômé depuis peu, mais il est très au fait des dernières normes comptables et va pouvoir rajeunir les process en cours dans l'entreprise.

Thierry, le nouveau comptable, ne perd pas de temps dans son travail et a déjà étudié les trois dernières années de comptabilité.

> Tout à l'air en ordre, mais un élément pose problème : plusieurs fournisseurs de la société, bien qu'agissant des secteurs différents, sont domiciliés à la même adresse. Les vérifications faites, il s'avère que ces fournisseurs ont le même numéro de compte bancaire. Pierre prévient Gérard, qui ne tarde pas de s'apercevoir que ces fournisseurs n'existent pas. Allant plus avant dans ses investigations, il s'aperçoit que le compte bancaire est en fait détenu par… M. X, qui fait régler, depuis des années, des factures de fournisseurs n'existant pas sur un compte lui appartenant. Gérard tombe des nues : comment ce collaborateur fidèle et attentif a pu voler la société à laquelle il appartient depuis tant d'années ? Convoqué sur le champ, M. X ne tarde pas à s'effondrer et à tout avouer : il détourne de l'argent depuis 15 ans pour payer des dettes de jeu et des maîtresses trop gourmandes. Tout compte fait, la fraude s'élève tout de même à 3 millions d'euros. M. X n'avait même pas conscience du montant global de ces détournements, et il ne lui reste rien du fruit de son escroquerie. Pris de pitié pour cet homme, Gérard ne préviendra pas la police et ne déposera pas plainte.

Abusé par un collaborateur qu'il pensait au-dessus de tout soupçon, Gérard, tout comme ces prédécesseurs, n'a rien vu du manège de M. X, qui était à la fois responsable du paiement des factures et en charge du contrôle. De petits détournements tous les mois, qui au final font une somme considérable. Une somme perdue définitivement pour l'entreprise.

ANTICIPER ET RÉDUIRE LE RISQUE DE FRAUDE INTERNE

Du fait de ses formes variées et de la diversité des motivations poussant les fraudeurs à agir, il n'est jamais simple d'anticiper voir d'éradiquer les fraudes internes des entre-

prises. Une bonne sensibilisation au phénomène et des programmes de détection sont de bons atouts pour une entreprise consciente du risque.

La sensibilisation des collaborateurs

Une phrase fréquemment entendue dans les entreprises victimes de fraudes est « *comment avons-nous fait pour ne pas nous en apercevoir ?* ». Les fraudeurs profitent parfois d'un manque de vigilance de leur entourage ou d'un manque d'implication des personnes en charge du contrôle. Une bonne sensibilisation des collaborateurs sur les fraudes recensées dans le secteur d'activité permet de détecter en amont les comportements à risque et de voir les signaux d'alerte généralement non perçus par des personnes non sensibilisées.

Il existe désormais des modules de formation efficaces qui sont dispensés à plusieurs types de collaborateurs, selon leur rôle dans les processus de contrôle et selon leur engagement de responsabilité : collaborateurs dans leur ensemble, service comptable, service d'audit, directions générales, mandataires sociaux…

La cartographie des risques

Recommandée par toutes les réglementations et les processus de lutte anti-fraudes, la cartographie des risques permet d'identifier les fraudes les plus probables et d'en déterminer les causes et les effets. En réalisant un tel travail, le chef d'entreprise peut se rendre compte des vulnérabilités de son organisation et mettre en place les dispositifs de veille les plus adaptés à sa société.

La cartographie est également un bon outil pour accentuer la sensibilisation des collaborateurs en démontrant l'ensemble des fraudes auxquelles l'entreprise est exposée.

Une politique interne de contrôle

La politique interne anti-fraude vise à réduire le risque au sein de l'entreprise. Publique et connue des collaborateurs, elle vise à dissuader les fraudeurs d'opportunité, profitant des failles du système, et à mettre à jours les pratiques des fraudeurs organisés. La politique interne peut s'appuyer sur les organes internes comme :

• *le service Conformité*, en charge de concevoir les normes à mettre en œuvre ;

• *les services opérationnels*, assurant le respect des normes établies et réalisant un contrôle de premier niveau ;

• *le contrôle interne* permanent, surveillant les outils de suivi, tableaux de bords, et réalisant un contrôle de second niveau ;

• *l'audit interne*, qui réalise des contrôles périodiques ou des actions d'investigation en cas de fraude présumée.

Les réglementations spécifiques

La SOX, édictée le 31 Juillet 2002, prévoit notamment l'obligation pour les présidents et les directeurs financiers de certifier personnellement les comptes de leur entreprise, l'obligation de nommer des administrateurs indépendants au comité d'audit et au conseil d'administration ainsi que l'encadrement des avantages particuliers des dirigeants : perte de l'intéressement en cas de diffusion d'informations inexactes, interdiction des emprunts auprès de l'entreprise,

possibilité donnée à la Securities & Exchanges Commission d'interdire tout mandat social pour les dirigeants soupçonnés de fraude).

La loi de sécurité financière, ou LSF, aussi appelée Loi Mer du nom du Ministre des Finances qui l'a fait rédiger, encadre aussi les actions de contrôle et d'audit interne des entreprises.

La réglementation Bâle II, appliquée depuis 2004, place désormais la lutte contre la fraude dans la gestion des risques : il ne s'agit plus seulement de les connaître ou de les maîtriser, mais aussi de les anticiper pour éviter leur survenue. Bâle II recommande notamment la publicité et la transparence des actions engagées dans ce but, avec mention des sommes investies.

Le règlement CRBF 97-02 encadre les dispositifs de contrôle interne et de conformité. Il prévoit la mise en œuvre de contrôles périodiques et permanents, impliquant les dirigeants dans l'évaluation de la politique interne de prévention mise en œuvre. Ce règlement insiste également sur le développement d'une culture de prévention des risques auprès de l'ensemble des collaborateurs de l'entreprise.

L'auto-détection

L'étude réalisée par PricewaterhouseCoopers a montré que près de 40 % des fraudes détectées l'ont été du fait d'une dénonciation ou d'un signalement d'un collaborateur. Ce chiffre n'était que de 16 % en 2005, ce qui démontre une implication croissante des collaborateurs dans la lutte anti-fraude et dans la protection des intérêts

de leur entreprise. Parmi ces moyens d'auto-détection, le « whistleblowing »a été mis en oeuvre dans de nombreuses entreprises. Permettant de faire un signalement de manière anonyme, grâce à un numéro de téléphone de type hotline ou une adresse électronique spécifique, le whistleblowing a permis d'identifier 8 % des fraudes détectées en 2006.

POUR EN SAVOIR PLUS

Fernandez E., Koessler L., Siruguet J.-L., *Le contrôle interne bancaire et la fraude*, Dunod, 2006.

Gallet O., *Halte aux fraudes : prévenir et détecter les fraudes en entreprise,* Dunod, 2004.

PARTIE 2

LES MENACES D'ATTEINTE AUX INFORMATIONS STRATÉGIQUES

4

L'ESPIONNAGE ÉCONOMIQUE

« Pour les grandes sociétés françaises, le préjudice de l'espionnage économique s'élève à 1,5 milliard d'euros par an »

Un commissaire de la DST[1]

L'ESPIONNAGE, UN OUTIL DE LA GUERRE ÉCONOMIQUE

Le monde des affaires et l'environnement économique actuels sont un contexte dans lequel la concurrence fait rage et où tous les moyens sont bons pour gagner des marchés et conquérir de nouveaux territoires. De ce fait, la protection des intérêts économiques de l'entreprise est un des enjeux majeurs des années qui viennent : maintien ou accroissement de la compétitivité, découverte et ouvertures de marchés nouveaux, attractivité de l'entreprise, élaboration de produits ou de concepts innovants sont les facteurs du développement économique et de la préservation des emplois. Plus aucun secteur n'est épargné : informatique, pharmacie, industrie, construction, agroalimentaire, toutes les entreprises quelle que soit leur taille ou leur activité, peuvent faire l'objet d'une opération d'espionnage économique.

1. Direction de la Surveillance du Territoire.

Il est d'usage de diviser les informations nécessaires à la compréhension d'un contexte économique en trois catégories :

• ***Les informations ouvertes, dites blanches***. Elles sont accessibles à tous, à condition de savoir où et comment les chercher.

• ***Les informations semi-fermées, dites grises***. Elles sont accessibles à condition de mettre en œuvre des actions spécifiques d'investigation et de recherche.

• ***Les informations fermées, dites noires***. À très forte valeur ajoutée, elles ne sont généralement accessibles que par des actions déloyales voire malveillantes ou illégales.

L'espionnage économique cherche à identifier les informations fermées relatives à un projet économique : procédés de fabrication, coûts ou prix de revient de produits, partenaires stratégiques, hommes clés…

Ces actions d'espionnage peuvent être le fait de gouvernements ou de services étatiques de renseignement. Certains dirigeants étrangers ont déclaré publiquement que dans plusieurs pays, une direction spécialisée des services secrets était chargée de mener des opérations d'espionnage économique contre le personnel des entreprises étrangères. L'implication de services étatiques pose le problème de leur capacité à mettre en œuvre des moyens « exorbitants » pour arriver à leurs fins : fouilles de chambres d'hôtel, vols d'ordinateur, infiltrations d'agents dans le personnel local de l'entreprise, rétentions des ordinateurs portables à la douane… Certaines réglementations ont même l'air d'avoir été mises en œuvre uniquement à des fins d'espionnage économique. Dans le transport aérien

par exemple, les États-Unis imposent aux compagnies aériennes de leur transmettre les données fournies par les passagers voyageant en direction de leur territoire. Sous le prétexte de la lutte contre le terrorisme, les services américains ont désormais accès à la grande majorité des données contenues dans le dossier du passager, le PNR (*Passenger Name Record*) : moyen de paiement, numéro du siège, nombre de personnes voyageant ensemble, passager voyageant côte à côte, contact sur place, état de santé du passager, réservation d'hôtel, régime alimentaire… Dans la même veine, la norme ISO TC204 est également très ambiguë : elle permet la traçabilité des marchandises, quel que soit le moyen de transport utilisé. Grâce aux nouvelles technologies de l'information et de la communication, c'est véritable système d'espionnage du transport international, capable de suivre à la trace et en direct n'importe quelle marchandise partout dans le monde.

Les actions d'espionnage peuvent aussi être le fait de sociétés privées de renseignement économique. Avec le développement de l'intelligence économique comme une spécialité à part entière, certaines sociétés dotées de peu d'éthique utilisent des moyens illégaux pour se procurer des renseignements économiques au profit de leurs clients. Ces actions peuvent être menées dans le cadre d'une opération concurrentielle ou d'une conquête de marché. Généralement composées d'ancien des services de renseignement, ces sociétés peu scrupuleuses utilisent tous les moyens à leur disposition : faux entretiens de débauchage, écoutes et poses de microphones, attaques informatiques pour pénétrer les systèmes d'information de concurrents, etc. La presse se fait de plus en plus souvent l'écho d'actions de ce

type découvertes par des entreprises victimes et reprises par la justice. D'ailleurs, le rachat du cabinet Kroll, longtemps leader mondial de l'investigation économique et impliqué dans plusieurs affaires de captation d'information, par le groupe Marsh & McLennan a d'ailleurs suscité la crainte de bon nombre d'entreprises européennes[1]. En effet, Marsh & McLennan possède également la société de courtage d'assurances Marsh, numéro un mondial de son secteur, la société Putman, important fonds d'investissement, et la société Mercer, un des leaders mondiaux du consulting. Comment être assuré, quand on est un client européen d'une des sociétés de Marsh & McLennan, que les informations confidentielles données dans le cadre d'un plan d'assurance ou d'une mission de consulting ne vont pas se retrouver chez les investigateurs de Kroll ?

Le niveau de sensibilisation des entreprises au risque d'espionnage économique est encore faible. Quand elles sont bien faites, les actions de captation d'informations sont totalement transparentes et restent non détectées. On estime à 90 % le nombre des entreprises qui, s'apercevant qu'elles ont fait l'objet d'une action d'espionnage économique, refusent de porter plainte pour préserver leur image.

LE CAMBRIOLAGE N'EN ÉTAIT PAS UN

> Michel dirige l'entreprise familiale que lui a transmise son père il y a quelques années. Installée dans la grande banlieue de Toulouse, la société est pionnière dans une niche technologique

1. *Inquiétude en France après le rachat de Kroll par Marsh*, Le Monde, 1er décembre 2004.

liée à l'aéronautique, et malgré sa taille modeste, elle est l'un des leaders mondiaux dans sa spécialité.

Depuis plusieurs mois, Michel et ses ingénieurs multiplient les dépôts de brevets et les annonces liées à l'activité fructueuse de leur service Recherche et Développement. Évoluant parmi des collaborateurs fidèles et employés par la société depuis très longtemps, Michel, tout comme son père, n'est pas un fervent adepte des mesures de sécurité. Depuis quelques temps, il est bien en contact avec des fonctionnaires de la Direction de la Surveillance du Territoire mais il reste persuadé que l'espionnage, c'est pour les autres, et que son entreprise n'intéresse personne du fait de sa discrétion et de sa taille réduite par rapport aux autres entreprises du secteur.

En arrivant un lundi matin à son bureau, Michel a la surprise de constater que la porte principale du siège de la société a été fracturée. Il rentre dans le bâtiment avec prudence, et s'aperçoit que c'est le matériel informatique qui a été l'objet du vol : la plupart des unités centrales des ordinateurs de bureau ont été emportées. La surprise passée, Michel appelle la brigade de gendarmerie locale qui vient procéder aux constatations d'usage. En début d'après-midi, Michel a rendez-vous avec Sergio, son directeur commercial, pour une réunion stratégique prévue de longue date. Mais Sergio est de mauvaise humeur : parti en week-end dans sa famille en Italie, il a eu la surprise de constater en rentrant que son appartement toulousain avait été cambriolé. Fort heureusement, les voleurs n'ont pas eu le temps d'emporter grand-chose : seuls son ordinateur portable et quelques babioles ont disparu. Mais c'est en recevant un appel de Jack, le correspondant de la société aux États Unis, que tout s'éclaire dans la tête de Michel. En effet, son appartement New-Yorkais a aussi fait l'objet d'une effraction. Par chance, les agresseurs ont été mis en fuite par un voisin avant de pouvoir rentrer dans les lieux. Très vite, Michel s'aperçoit que les matériels informatiques, volés au siège de la société ou chez son directeur commercial, contenaient tous des données sensibles, tant au niveau technique qu'au niveau commercial. Par ailleurs, aucune de ces données ne

> faisait l'objet d'un cryptage particulier. Quoi qu'il en soit, Il était malheureusement trop tard pour les protéger…

Michel a visiblement fait l'objet d'une action d'espionnage économique bien organisée. L'objectif était manifestement le vol de données stratégiques contenues sur les supports informatiques de la société. Le vol de données peut se faire de diverses manières :

• ***Le vol des supports :*** les supports-papier ou numériques sur lesquels se trouvent les informations sont subtilisés à leur propriétaire.

• ***La soustraction temporaire des supports :*** les supports sont « empruntés » pendant le temps nécessaire à la duplication des informations. On peut imaginer cette pratique dans le cadre de la fouille d'un bureau, d'une chambre d'hôtel, d'une rétention plus ou moins longue lors d'un passage en douane… Avec un équipement spécifique qu'il est aisé de se procurer aujourd'hui, quelques minutes suffisent pour dupliquer un disque dur ou copier la carte SIM d'un téléphone portable.

• ***L'élicitation :*** il s'agit de la captation d'information dans le cadre d'un entretien ou d'une discussion ouverte. En créant une relation empathique et en jouant la proximité avec sa cible, l'investigateur va faire parler son interlocuteur et lui faire livrer des renseignements sans que celui-ci ne s'aperçoive de la manœuvre en cours.

En l'occurrence, la société de Michel a fait l'objet de l'action de captation la plus efficace et la plus rapide : le vol des supports. L'action, bien coordonnée, a permis de subtiliser en même temps les unités centrales du siège, l'ordinateur portable du directeur commercial et sans un voisin

attentif, l'ordinateur du représentant américain aurait subi le même sort.

Cet évènement a eu le mérite de démontrer que toutes les entreprises, quelle que soit leur taille, peuvent faire l'objet d'un acte d'espionnage, et que les mesures de préservation des informations sensibles sont indispensables dès lors que l'on évolue dans un environnement concurrentiel où tous les coups sont permis.

RÉDUIRE LE RISQUE D'ESPIONNAGE ÉCONOMIQUE

La réduction du risque d'espionnage économique repose essentiellement sur la protection des informations et des données sensibles qui pourraient éveiller la convoitise des chasseurs de renseignement. Cette protection repose sur la mise en œuvre de moyens techniques et humains pour sanctuariser les informations.

La sanctuarisation

• ***La première étape*** de la sanctuarisation est la classification des données : toutes les informations ne nécessitent pas le même niveau de protection, et leur nature ainsi que leur importance dans le temps changent leur statut et les mesures de sécurité applicables. La classification, généralement réalisée en trois niveaux (public, confidentiel, secret), permet d'affecter à chaque document un niveau de confidentialité spécifique impliquant des mesures de protection appropriées : interdiction de photocopier ou de sortir d'un service, diffusion retreinte aux membres du Comité de Direction, interdiction d'enregistrer sur un support amovible,

broyer après lecture… Les documents peuvent ensuite être déclassifiés avec le temps ou au fil du développement du projet, nécessitant une diffusion de plus en plus large du document.

• ***La seconde phase*** de la sanctuarisation est l'identification des lieux de vulnérabilité : il s'agit notamment des bureaux de la société, des salles de réunion ou des services particuliers (R&D, département technique, service juridique…) au sein desquels les informations se trouvent ou circulent. Les déplacements constituent aussi des moments de vulnérabilité : en restant discret sur ses activités et sur ces projets en cours, l'entreprise va permettre à ses cadres se déplaçant de le faire en toute sérénité.

L'utilisation de moyens de protections techniques

Le stockage sécurisé des données devrait être un principe dans les entreprises aujourd'hui. Il existe de nombreux moyens techniques de sécuriser une information : le stockage sur des supports qui ne quittent jamais l'entreprise (serveurs, disques durs amovibles gardés dans un coffre), ou sur des supports encryptés pour éviter les vols ou la copie.

Certaines entreprises font travailler leur personnel sur des ordinateurs qui n'acceptent aucune prise USB, et qui ne dispose d'aucun système de copie ou de gravure.

Pour les cadres se déplaçant, il convient de leur confier des ordinateurs sans archives, et qui ne servent qu'à la mission en cours. En cas de perte ou de vol, un minimum d'informations sont compromises.

Il existe désormais des dispositifs techniques permettant de crypter à distance un ordinateur qui aurait été perdu ou volé.

La sensibilisation et l'information des collaborateurs

Ces actions permettent d'impliquer les détenteurs d'information dans la politique de protection des données tout en les informant des modes opératoires pratiqués par les chasseurs de renseignement pour en identifier les attaques. En faisant de chacun un protecteur des données sensibles, l'entreprise développe la culture de sécurité. Ainsi, en cas de comportement étrange ou de suspicion d'une action d'espionnage économique, un collaborateur peut signaler ce qu'il a constaté et interrompre l'action des chasseurs de renseignement.

La collaboration avec les services de contre-espionnage

Les services étatiques, comme la Direction de la Surveillance du Territoire, proposent aux entreprises une assistance à la prévention du risque d'espionnage économique. Par des actions de sensibilisation, de formation ou d'assistance en cas de présomption d'espionnage, la DST participe à la préservation du patrimoine informationnel des entreprises françaises.

POUR EN SAVOIR PLUS

« *Rapport d'information* », Assemblée nationale, 9 juin 2004.

Baud J., *Encyclopédie du renseignement et des services secrets*, Éditions Lavauzelle, 1995.

Alem J.-P., *L'espionnage et le contre-espionnage*, PUF, 1980.

Forcade O., Laurent S., *Secrets d'État*, A. Colin, 2005.

5

LES CYBER-EXTORSIONS

« Aujourd'hui, la plupart des virus et des troyens sont codés dans l'intention d'extorquer de l'argent »

Graham Cluley
Consultant en sécurité informatique

QUAND LES DONNÉES SONT PRISES EN OTAGE

On sait depuis longtemps que les escrocs et les hackers ne manquent pas d'imagination. Mais les cyber-extorsions, que doivent affronter depuis peu les entreprises, démontrent que nous ne sommes pas encore au bout de nos surprises. Véritables prises en otage des données informatiques, les cyber-extorsions, aussi appelées « ransonware », sont des actions malveillantes ayant pour objectifs d'obtenir une remise de fond plus ou moins importante.

Le CERTA, Centre d'Expertise, de Réponse et de Traitement des Attaques informatiques rattaché au Secrétariat Général de la Défense Nationale, définit les cyber-extorsions comme une « *forme d'extorsion imposée par un code malveillant sur un utilisateur du système. Si ce dernier refuse de payer ou d'effectuer une tâche imposée, le service auquel il veut accéder lui est refusé par le code malveillant* ». C'est l'utilisation de la *cryptovirologie* qui permet aux agresseurs de pénétrer le système de leur victime et de mettre en

œuvre leur action malveillante. Le virus utilisé, généralement un cheval de Troie ou Trojan, est déployé simplement quand la victime visite les pages piégées de certains sites Internet. Le programme-parasite s'installe alors sur l'ordinateur infesté et parcours les disques durs à la recherche de certains types de fichiers ou des documents les plus fréquemment utilisés ou consultés. Dès que ces fichiers sont identifiés, ils sont cryptés par un algorithme spécifique et deviennent inaccessibles pour leur utilisateur. Un message apparaît pour demander le virement d'une somme d'argent en échange du code permettant de décrypter les fichiers.

Les auteurs de cyber-extorsions agissent de diverses façons dès lors qu'ils ont accédé aux fichiers visés :

• ***Le cryptage des données :*** après avoir codé les fichiers, le pirate sollicite le paiement de ce qu'il convient d'appeler une rançon. Elle peut varier, selon les cas, de 10$ à plusieurs dizaines de milliers d'euros. Après son versement, la victime reçoit une clé qui lui permet d'accéder à ces informations.

• ***La captation de données sensibles :*** le pirate identifie les informations importantes présentes sur l'ordinateur de sa victime, puis les transfère sur un serveur ou un autre ordinateur. Ensuite, il détruit les documents originaux et réclame le paiement d'une rançon pour restituer les fichiers.

• ***La démonstration de vulnérabilité :*** l'introduction dans l'ordinateur de la victime sert de prétexte au pirate pour démontrer à son propriétaire que son système est vulnérable. Dès lors, il peut demander le versement d'une somme d'argent en échange de la non-divulgation de sa vulnérabilité. En 2004, Google a été victime d'une telle

action : un pirate a proposé aux administrateurs de ce moteur de recherche sur Internet de lui vendre un logiciel qui était sensé permettre d'abuser le système de rémunération de Google basé sur les clics sur les liens publicitaires sponsorisés. En échange de 100 000 $, l'auteur de l'extorsion s'engageait à ne pas offrir son logiciel à des éditeurs de spam capables de fausser, avec un tel outil, le système de rémunération de Google.

• ***La menace de divulgation des données :*** le pirate pénètre le système informatique de sa victime, duplique des informations sensibles ou confidentielles, et menace de les révéler à des concurrents ou au grand public pour nuire à l'image ou à la réputation de la société ainsi abusée. C'est ce qui est arrivé à la Softbank, une banque japonaise, en Février 2004. Après avoir accédé à la base de données des clients de la banque, les pirates ont réclamé la somme de 28 millions de dollars pour ne pas divulguer les données personnelles des clients. L'affaire ayant été rendue publique, les dirigeants du groupe Softbank ont dû présenter leurs excuses officiellement.

Il existe peu de statistiques sur la problématique de la cyber-extorsion et des attaques de cryptovirologie. Cette absence de données est due à plusieurs causes :

Les collaborateurs des entreprises qui sont victimes de ce type d'attaque ont souvent vu leur ordinateur infesté en naviguant sur des pages web « douteuses » pour ne pas dire carrément interdites dans leur organisation. Il leur est donc difficile de révéler l'attaque sans préciser la source de l'infestation.

Les entreprises victimes sont peu enclines à révéler que leur système informatique est vulnérable et qu'il a fait

l'objet d'une agression. Cela pourrait paniquer les utilisateurs ou les clients dont les données sensibles sont stockées dans les ordinateurs ou les serveurs attaqués.

Communiquer sur une vulnérabilité, c'est montrer aux autres hackers qu'il existe une opportunité d'action dolosive et montrer le mauvais exemple.

LA BOURSE… OU LA DESTRUCTION DES FICHIERS CRYPTÉS !

Patrick est un manager pressé : chef de département dans une entreprise de dessin industriel, il passe ses journées penché sur ses tables à dessin et sur son écran d'ordinateur. Les dossiers qu'il gère sont tous de grands projets pour de gros clients, et les délais imposés sont souvent restreints. Pendant les rares pauses qu'il s'accorde, Patrick cherche de la musique sur Internet : étant adepte de musiques électroniques, il préfère surfer les sites confidentiels et discrets plutôt que sur les sites des grandes majors, au détriment parfois de la sécurité informatique.

Alors qu'il arrive un matin à son bureau et qu'il connecte son ordinateur au réseau de l'entreprise, Patrick a la surprise de constater que son accès aux fichiers partagés lui est interdit par un message d'annonce lui demandant de rentrer un nom d'utilisateur et un mot de passe. Furieux de ne pas avoir été averti d'un changement des procédures applicables, il appelle le responsable du service informatique… qui lui indique qu'aucun changement n'a été mis en œuvre depuis les trois derniers mois. Invité a venir voir par lui-même, le responsable informatique ne tarde pas à comprendre : l'ordinateur de Patrick a servi de point d'accès pour un cheval de Troie qui a bloqué les accès au serveur et qui demande une clé pour autoriser les connexions. Alors qu'ils tentent d'éteindre et de rallumer plusieurs fois le système, les deux hommes voient arriver dans le bureau de Patrick tous les autres collaborateurs qui se heurtent au même problème : plus aucun ne peut accéder à ses fichiers de travail sans se voir

> demander un code d'accès. Aucune sauvegarde n'ayant été faite hors du serveur par la plupart des collaborateurs, aucun projet ne peut avancer.
>
> Alors qu'il n'en revient toujours pas, Patrick voit apparaître sur son écran un message provocateur écrit dans la langue de Shakespeare : « Écoute-moi bien ! Tu tiens à ton ordinateur ? » Il a à peine terminé de lire ce message qu'une photo à caractère pornographique apparaît en plein écran. Patrick se jette sur son clavier, et un nouveau message s'affiche, toujours en anglais : « Les touches CTRL+ALT+SUPPR ne servent à rien ! ». En plus d'être malhonnête, le hacker est visiblement moqueur. La suite des évènements est moins drôle et plus explicite : un nouveau message annonce à Patrick, stupéfait, que tous les fichiers contenus sur le serveur vont être détruits toutes les 30 minutes si un code de désactivation n'est pas entré dans les 6 heures. Et pour obtenir ce code, un simple virement de 10,99 $ suffira. Après quelques de tergiversations, devant l'incertitude et le risque de perdre ses données, Patrick a décidé… de procéder au virement ! Après quelques trop longues minutes pour Patrick, un code de désactivation lui parvenait ainsi qu'un mode d'emploi pour retrouver et détruire le virus initial.

Patrick a été victime d'un virus appelé Ransom-A. Déployé grâce à un cheval de Troie, certainement implanté à partir d'une page web visitée par Patrick, le virus a bloqué le système informatique de la société et obligé le paiement d'une rançon, heureusement modique, mais extrêmement désagréable. Cette mésaventure a permis de rappeler à tous les collaborateurs que la navigation sur internet via les ordinateurs connectés au serveur de l'entreprise n'est pas une chose anodine, et que sans un antivirus et un anti spyware efficaces, le risque d'infestation de cyber-extorsion est une réalité. Par ailleurs, cet évènement a aussi permis à l'entreprise de Patrick de faire procéder quotidiennement à la sauvegarde des données sensibles sur des disques durs amovibles.

> Michael Bloomberg, et sa société d'information financière, ont connu une cyber-extorsion étonnante. Deux informaticiens d'origine Kazakhe, Oleg Zezov et Igor Yarimaka, ont tout simplement réussi à pénétrer le système informatique de la société Bloomberg et à soutirer des informations sensibles. Pour prouver leur exploit, les deux hommes ont fait une copie du véritable badge d'accès de Michael Bloomberg et lui ont envoyé par email. Afin de révéler la faille dans le système qui leur a permis de pénétrer le réseau Bloomberg, les deux kazakhes demandent la somme de 200 000 $ au titre de leurs « frais de consultants ». On imagine aisément la réaction des marchés dans le cas de la révélation que le système informatique d'une des plus importantes sociétés d'information financières est faillible et facile à détourner.
>
> Censé retrouver ses extorqueurs à Londres, Mickael Bloomberg s'est rendu au rendez-vous… accompagné de deux policiers de Scotland Yard se faisant passer pour un des ses employés et pour un traducteur. Arrêtés par les policiers, Zerov et Yarimaka ont été mis en examen pour intrusion dans un système informatique et extorsion.

PRÉVENIR LE RISQUE DE CYBER-EXTORSION

La prévention du risque de cyber-extorsion passe en premier lieu par la sensibilisation des utilisateurs de systèmes informatiques, et à la mise en œuvre d'une politique spécifique de prévention « technique » au moyen d'antivirus et de firewall adaptés.

La prise en considération du risque

L'imagination et la capacité à nuire des pirates informatiques n'a pas de limite, la cyber-extorsion en est un exemple frappant. Cependant, ce phénomène particulier étant encore peu connu du grand public, bon nombre d'entre-

prises pensent que cela n'arrive qu'aux grands groupes, qui ont des informations stratégiques à très forte valeur ajoutée. Pourtant, si ces grandes sociétés peuvent effectivement intéresser les pirates chevronnés et ambitieux, l'ensemble des autres entreprises de taille plus réduites font des cibles faciles pour les pirates « de masse » qui s'attaquent à leurs cibles tout azimut. L'exemple de la société de Patrick, PME florissante, montre que pour ne demander qu'une somme de 10,99 $ à sa victime, le pirate auteur de cette attaque doit multiplier les cyber-extorsion pour rentabiliser son acte.

L'utilisation d'antivirus

La mise en œuvre d'antivirus est devenue une obligation dans les organisations : connexions sur Internet, implémentations de CD-Rom ou de clé USB, autant de vulnérabilités qu'un antivirus peut renforcer en vérifiant régulièrement les fichiers entrants et les fichiers de stockage. Encore faut-il que ces antivirus soient à jour, c'est-à-dire aptes à identifier les derniers virus circulant sur les réseaux.

Une politique de connexion efficace

Sensibiliser les collaborateurs, c'est aussi établir une politique de connexion stricte. Il est possible d'interdire tout simplement les connexions Internet au sein de l'entreprise : c'est encourager les connexions sauvages, réalisées en dehors de tout contrôle. Il est préférable d'expliquer à tous les utilisateurs les dangers des connexions non sécurisées et de restreindre l'utilisation du Web à l'utilisation de sites professionnels.

Cette politique de connexion peut s'étendre aux collaborateurs en déplacement : interdiction de se connecter par exemple dans des business center ou à partir d'ordinateurs publics. Ces ordinateurs, accessibles à tous, sont faciles à piéger avec des *keyloggers* qui permettent d'enregistrer les codes d'accès utilisés pour ensuite pénétrer un système.

Sauvegardes automatiques et régulières des données

Pour faire face aux possibles altérations (codages, destructions) des données, il est important de réaliser régulièrement des backups des données importantes des ordinateurs sur un support externe tel qu'un CD-ROM, un DVD-ROM ou un disque dur amovible. Ces copies doivent être conservées sur des supports isolés des réseaux ou d'internet.

En cas de survenue

La première chose à faire si une menace de cyber-extorsion survient, c'est d'évaluer la véracité de l'action. Il est arrivé que des pirates simulent le blocage du système alors qu'en fait les fichiers avaient juste été déplacés. S'il s'avère que les fichiers sont réellement encodés et inaccessibles, il faut essayer d'isoler très vite l'ordinateur infesté pour éviter que le virus ne se propage. Il faut ensuite protéger, c'est-à-dire dupliquer, toutes les données encore accessibles.

Quand le système attaqué est vaste et qu'il comprend de nombreux postes, identifier la faille demande du temps. Ce temps peut être gagné dans le cadre des négociations qui peuvent s'engager entre l'extorqueur et sa victime. Il est

préférable, dans ses conditions, de faire rapidement appel à un spécialiste de ce genre de négociation.

Le recours aux forces de l'ordre : Les services de police sont désormais dotés d'unités spécialisées pour contrer les attaques informatiques et identifier les auteurs. Une collaboration rapide avec les forces de police peut permettre de mettre fin à l'agression au plus tôt, en minimisant les dégâts.

POUR EN SAVOIR PLUS

Filiol E., Richard P., *Cybercriminalité : Les mafias envahissent le web*, Dunod, 2006.

Paget F., Rosé P., *Vers et virus : Classification, lutte anti-virale et perspectives*, Dunod, 2005.

Quemener M., Ferry J., *Cybercriminalité : Défi mondial et réponses,* Economica, 2007.

6

LES ATTAQUES INFORMATIQUES

« Un ordinateur qui se connecte sans antivirus ou fire wall est infesté par un virus en moins de 10 minutes »

Un consultant spécialisé

LES SYSTÈMES INFORMATIQUES, TERRAIN DE CHASSE DES HACKERS

Les systèmes et les réseaux informatiques sont devenus la clé des échanges d'information du XXI^e^ siècle. De plus en plus d'individus, d'entreprises, d'institutions publiques dépendent de communications et de réseaux informatisés, et la configuration de ces réseaux informatiques et de leurs systèmes d'exploitation devient chaque jour plus complexe, créant ainsi des vulnérabilités plus nombreuses, exploitables par les pirates informatiques. Cette dépendance croissante modifie radicalement la définition de la menace d'attaque informatique. L'interdépendance entre les systèmes génère de plus une nouvelle menace : les agresseurs n'ont plus besoin d'avoir un accès direct à un ordinateur pour subtiliser, détruire ou altérer les informations qu'il contient. Dès lors que le hacker parvient, à distance, à s'infiltrer dans un système, il est dans la place pour se livrer à toutes les exactions qu'il souhaite mettre en œuvre. La frénésie entraînée par le virus *« I love you »*, qui a traversé la

planète informatique il y a plusieurs années, a démontré la vulnérabilité d'un système à ce point interdépendant.

Une attaque informatique est l'exploitation d'une faille, identifiée dans un système informatique à des fins inconnues par l'exploitant des systèmes et généralement préjudiciables pour celui-ci. Ces failles peuvent toucher le système d'exploitation, les logiciels utilisés par ce système ou l'utilisateur lui-même quand il n'applique pas les règles élémentaires de prudence. Ce qui rend difficile la prévention des attaques informatiques, et la prise de conscience même de ce risque, c'est que la sécurisation d'un système informatique est forcément asymétrique : le hacker n'a qu'à trouver une seule vulnérabilité pour pénétrer et compromettre le système, alors que l'entreprise doit identifier l'ensemble des failles potentielles pour essayer de les combler toutes.

Les motivations des hackers sont multiples :

• Le jeu : certains pirates ne s'attaquent à des systèmes que par défi pour démontrer, souvent à eux-mêmes ou à leur entourage, qu'ils sont capables de prouesses techniques.

• Accéder à un système pour subtiliser des données : voler des informations dans un but criminel[1], ou dans le cadre d'un acte d'espionnage économique[2].

• Récupérer des données sur un utilisateur : informations bancaires, usurpation d'identité…

• Recenser les habitudes des utilisateurs du système pour en tirer des statistiques.

1. Voir chapitre « Les cyber-extorsions ».
2. Voir chapitre « L'espionnage économique ».

• Altérer le bon fonctionnement du système pour le rendre inopérant (*deny of service*) ou pour en modifier les caractéristiques (aspect d'un site internet).

Utiliser l'ordinateur attaqué comme un intermédiaire pour des attaques par rebond : ces attaques consistent à attaquer un système par l'intermédiaire d'un autre système. Ces intrusions cherchent à utiliser les ressources du système cible, notamment lorsque le réseau sur lequel il se trouve possède une bande passante élevée permettant une forte capacité de travail.

Le développement des réseaux mobiles va encore accroître la vulnérabilité des systèmes : réseaux sans fils, accroissement de la flotte d'ordinateurs mobiles, smart-phones, autant de vulnérabilités nouvelles que les entreprises vont devoir combler pour réduire les agressions.

Afin de faire face aux attaques informatiques, il est important de connaître les principaux modes opératoires permettant la mise en œuvre des mesures préventives adaptées. Les virus sont les principaux vecteurs des attaques : ces CPA, ou *Codes Auto-Propageables*, ont un champ d'application vaste. Cela peut aller de la perte de contrôle de la souris d'un ordinateur jusqu'à la destruction totale des données du système. Pour essayer d'y voir plus clair dans la faune extraordinairement prolixe des virus, les spécialistes classent ces derniers selon leur mode de propagation dans les systèmes :

• ***Les vers*** sont des virus capables de se propager à travers un réseau et de l'infester dans son intégralité.

• ***Les chevaux de Troie***, ou *trojan*, sont des virus qui permettent à leur concepteur de s'introduire dans un

système pour en prendre le contrôle. À l'instar de la fable antique, le virus pénètre dans le système en se cachant dans un programme d'apparence inoffensif pour tromper l'utilisateur du système qui va autoriser son installation.

• ***Les bombes logiques*** sont des virus qui s'introduisent dans un système pour s'y cacher en attendant qu'un *trigger* ne l'active. Ce trigger d'activation peut être un événement particulier, comme une date dans le système, ou une activation à distance. Il y a quelques années, les pirates utilisaient fréquemment la menace de bombe logique pour extorquer de l'argent à leurs victimes.

• ***Les hoax***, souvent reçus par emails, sont de faux virus. Mais en jouant sur la crainte des utilisateurs, ils permettent d'altérer un système. Aussi appelés *Do it yourself*, le hoax s'accompagne d'une note indiquant qu'un virus circule sur les réseaux et qu'il faut le détruire manuellement. Puis s'ensuit une liste de choses à faire, notamment rechercher des fichiers système pour les détruire. Or, ces fichiers systèmes ne sont pas infestés, et leur destruction par l'utilisateur non averti entraîne le blocage complet du système.

• ***Les virus mutants*** sont des virus déjà existants, mais réécrits par d'autres hackers afin d'en modifier la signature pour les rendre plus difficiles à détecter. La multitude de versions d'un même virus le rend plus difficile à décoder.

• ***Les virus polymorphes*** sont des virus qui ont la possibilité de modifier automatiquement leur apparence et leur signature pour se rendre plus difficiles à détecter.

• ***Les rétrovirus*** s'attaquent aux antivirus pour modifier leurs signatures afin de les rendre inopérants.

• ***Les boot virus***, ou virus de secteur d'amorçage, endommagent le secteur de démarrage d'un disque dur sensé amorcer le système d'exploitation. Ainsi, l'ordinateur ne se lance pas et est donc inutilisable.

Les hackers ne sont malheureusement limités que par leur imagination : plus les systèmes se développent et plus les failles nouvelles les rendent vulnérables aux attaques de pirates qui ont pour principal passe-temps la conception de nouveaux moyens d'agression.

ATTAQUES EN SÉRIE

Un laboratoire pharmaceutique a vécu il y a quelques semaines une crise liée à des attaques informatiques qu'il n'avait pas imaginée. Comme la plupart des entreprises de cette taille, l'ensemble de ses réseaux sont interconnectés pour permettre une plus grande fluidité des échanges d'information. Les données les plus sensibles, comme les travaux de recherche ou les brevets en cours, sont stockées dans des serveurs inaccessibles, mais l'ensemble des autres systèmes sont parfois protégés sans plus d'attention.

Le responsable du service informatique du groupe est alerté en pleine nuit par un de ces collègues de la région asiatique : leurs serveurs ont été victimes d'une série d'attaques simultanées, qui ont bloqué l'intégralité des serveurs. Aucune connexion n'est possible à l'heure actuelle, et les informaticiens locaux sont à la tâche pour essayer de trouver une solution. Sentant le piège, le responsable informatique se rend au siège du groupe et appelle son adjoint pour lui demander de le rejoindre. Bien lui en pris : quelques minutes plus tard, plusieurs tentatives d'intrusion étaient signalées sur les serveurs centraux, montrant une attaque massive. Au petit matin, tous les warnings sont au rouge, et aucun des collaborateurs situés entre Pékin et Paris ne peut plus se connecter.

> Rapidement, les informations accréditant la thèse d'une attaque ciblée et massive se confirment. Le site internet du groupe a été modifié : en lieu et place des informations classiquement diffusées par ce média, à savoir l'actualité du secteur et du groupe en particulier, des images de tests sur des animaux sont montrées à tous ceux qui se connectent. Il y est décrit dans le détail comment les laboratoires pharmaceutiques pratiquent des expériences sur des animaux vivants, et les commentaires mettent en cause directement le laboratoire concerné. L'action est revendiquée par un lien vers le site d'une association d'Ecowarriors, militant pour la cause des animaux et contre la vivisection.

Dans ce cas d'espèce, l'attaque contre le laboratoire avait une motivation politique : bloquer les systèmes de la société pour arrêter son activité, et en modifier le site internet pour faire passer un message politique de grande envergure. Il a fallu plusieurs heures aux informaticiens pour remettre le système en état, et plusieurs semaines pour en identifier les failles et trouver des moyens de les combler. La crise ayant été gardée secrète, hormis pour les quelques utilisateurs s'étant connectés sur le site pendant l'attaque, aucune données précises n'a pu être collectée. Il aurait été intéressant de connaître le coût d'une telle situation, et les coûts engendrés pour y remédier.

Un célèbre hacker, Kevin Mitnick, alias *el Condor*, a défrayé la chronique des États-Unis il y a quelques années. Champion toutes catégories des attaques informatiques, il a commis l'erreur de s'attaquer à l'ordinateur personnel de Tsutomu Shimomura, ancien pirate reconverti dans la sécurité informatique et de livrer ses secrets professionnels sur Internet. Ce dernier, en se mettant au service du FBI, a

permis l'interpellation de Mitnick qui a écrit un livre racontant ses exploits par la suite.

RÉDUIRE LE RISQUE D'ATTAQUES INFORMATIQUES

Face à la vulnérabilité et à l'interdépendance des systèmes, la réduction du risque d'attaque informatique passe par une sensibilisation des utilisateurs et la mise en œuvre de moyens techniques dédiés.

Le contrôle d'accès aux systèmes

70 % des entreprises utilisent des moyens de contrôle d'accès aux données ou des outils de cryptage. En restreignant les accès aux seuls personnels autorisés, on peut limiter le nombre de personnes ayant accès aux systèmes. Encore faut-il que les comportements de prudence soient efficaces pour que les codes d'accès ne soient pas corrompus.

Les comportements de prudence

Afin de ne pas faciliter la tâche des hackers, le respect de quelques règles s'impose :

• Utiliser systématiquement un password pour verrouiller et accéder au système. La technologie permet aujourd'hui d'utiliser des moyens biométriques, plus difficiles à intercepter.

• Changer régulièrement de mot de passe, en utilisant des formules complexes et une multitude de caractères spéciaux et des caractères non consécutifs. Cette pratique permet de dissuader les hackers utilisant des dictionnaires de mots de passe.

• Ne jamais écrire son password sur un bout de papier, un post-it et le laisser sous un clavier ou à proximité des postes.

• Éviter les connexions au réseau depuis des postes non sécurisés : business center, hôtels, aéroports, etc. Les ordinateurs mis à disposition du public peuvent être équipés de keyloggers physiques ou logiques enregistrant les frappes sur le clavier, et ainsi les password employés par les utilisateurs.

• Ne pas ouvrir de fichiers exécutables envoyés par internet et dont l'auteur est inconnu.

• Ne pas se connecter sur des sites internet douteux ou n'étant pas autorisés par l'administrateur du système.

L'utilisation systématique d'antivirus

La première mesure technique est la mise en œuvre d'un logiciel antivirus. C'est un programme capable de détecter la présence de virus sur un ordinateur ou dans un système et, dans la mesure du possible, de le détruire définitivement. Plus de 95 % des entreprises utilisent un antivirus, avec une efficacité importante quand les logiciels sont mis à jour régulièrement.

Les antivirus détectent les virus grâce à leur signature. Les virus se propagent en infectant des fichiers hôtes, c'est-à-dire en copiant un code exécutable dans un programme déjà installé sur le système. Or, pour que le virus puisse fonctionner, il ne doit pas modifier plusieurs fois un même fichier. Afin de s'assurer que le programme a préalablement été infecté, le virus laisse dans ce programme une suite d'octets bien spécifiques : c'est leur signature virale. Les antivirus recherchent ces signatures, propre à chaque virus, pour les détecter et les éradiquer.

Pour que cette méthode soit efficace, le programme antivirus doit posséder une base virale à jour, comportant les signatures virales de tous les virus connus. Cette méthode ne peut cependant pas identifier les virus nouvellement créés ou les virus polymorphes qui changent régulièrement leur signature[1]. Certains antivirus utilisent un système appelé contrôleur d'intégrité, pour vérifier si les fichiers ont été modifiés par un virus. Le contrôleur d'intégrité de l'antivirus construit une base de données contenant des informations sur les fichiers exécutables du système au sein duquel il se trouve : dates des dernières modifications, tailles des fichiers, etc.…Si le contrôleur d'intégrité s'aperçoit qu'un fichier exécutable a été modifié et que ces caractéristiques ont changé, l'antivirus signale la possibilité d'un risque.

Le dédoublement de réseaux

En divisant les réseaux informatiques, et en ne laissant pas sur les ordinateurs connectés des données sensibles pouvant intéresser les hackers, on peut éviter les attaques et les intrusions. Plus le cloisonnement est étanche, plus le système est fiable.

Le cryptage des données

Il existe sur le marché des logiciels de cryptage des données efficaces qui permettent de protéger les informations sensibles et de les soustraire à la convoitise des hackers. L'utilisation de tels systèmes permet à deux utilisateurs qui s'échangent des données de les protéger pour éviter toute compromission.

1. Voir supra.

POUR EN SAVOIR PLUS

Favre B., Goupille P.-A., *Guide pratique de la sécurité informatique*, Dunod, 2005.

Mansfield R., *Hacker attaque*, Eska, 2001.

Mitnick K., *L'art de l'intrusion*, New Ed., 2005.

7

LE DÉBAUCHAGE DÉLOYAL

« Sur les 200 000 cadres recrutés en France chaque année, 75 000 sont recrutés dans des entreprises concurrentes. »

Un « chasseur de tête »

LA CHASSE AUX MEILLEURS CADRES

Dans un environnement économique où la concurrence fait rage et où les sociétés, quelle que soit leur taille, rivalisent pour emporter de nouveaux marchés et développer de nouvelles activités, la recherche de talents et de compétences est une priorité. Avoir l'ingénieur, le manager ou le technicien le plus qualifié est devenu un enjeu capital pour la croissance et la pérennité des organisations.

Dans cette recherche de la perle rare, les règles sont parfois oubliées et certains n'hésitent pas à pratiquer le débauchage des meilleurs collaborateurs de leurs concurrents. Il y a encore quelques années, seuls certains secteurs étaient touchés par cette « chasse à l'homme » : la finance, la banque, l'informatique étaient des environnements réputés pour l'esprit « mercenaires » de certains de leurs meilleurs représentants, n'hésitant pas à quitter leur entreprise du jour au lendemain pour un salaire majoré ou des avantages plus importants. Aujourd'hui, toutes les entreprises sont susceptibles de se voir débaucher un cadre efficace.

Il est surprenant de voir que depuis peu, la plupart des organisations travaillant sur leur organisation de gestion de crise et sur leur cartographie des risques mettent le débauchage d'une personne clé parmi les cinq risques les plus craints et les plus déstabilisants.

La concurrence déloyale et le débauchage		
Fondement juridique	**Éléments constitutifs du fait**	**Risques pour le débaucheur**
Art. 1382 du Code civil	Action commise dans le but de : Détourner une clientèle acquise. Connaître des secrets de fabrication ou des procédés confidentiels. Utiliser des connaissances acquises par le collaborateur débauché dans le but de concurrencer son entreprise d'origine.	Engagement de sa responsabilité civile Condamnation au versement de dommages et intérêts

Le « débauchage », prévu par l'article L122-15 du Code du Travail, qualifie l'action d'un salarié qui a rompu abusivement le contrat le liant à son employeur pour accepter d'être engagé par une autre entreprise, généralement concurrente de sa société d'origine.

Le débauchage déloyal, c'est-à-dire le débauchage d'un employé réalisé dans le cadre d'une concurrence déloyale, n'est pas toujours facile à qualifier. Le principe de la liberté

du travail, notamment celle de pouvoir choisir sans contrainte son activité, tout comme celui de la liberté de l'industrie et du commerce, trouvent leur fondement dans l'article 7 du décret d'Allarde de mars 1791 : « il sera libre à toute personne de faire tel négoce, ou d'exercer telle profession art ou métier qu'elle trouvera bon ». Empêcher un collaborateur de rejoindre une autre société, même si elle est complètement concurrente de sa société d'origine, ne peut se faire sans un certain nombre de contraintes pas toujours faciles à appréhender. Un recrutement bien organisé peut cacher un débauchage déloyal.

Les objectifs d'un débauchage déloyal peuvent être multiples :

• ***Recruter des collaborateurs formés chez un concurrent***, et ainsi acquérir un savoir-faire éprouvé sans aucun coût de formation.

• ***Obtenir des informations techniques :*** procédés et méthodes de fabrication, brevets, activités de Recherche&Développement.

• ***Obtenir des informations commerciales :*** clients, prospects, tarifs.

• ***Attirer une clientèle*** acquise ou gérée par le collaborateur débauché.

• ***Désorganiser un concurrent*** en le privant d'une ressource humaine clé et des connaissances associées.

Le débauchage n'est pas en lui-même un acte de concurrence déloyale. En effet, il est tout à fait licite si le salarié quitte son ancien employeur en étant libéré de toutes obligations : fin de contrat à durée déterminée, préavis effectué ou dispensé dans le cadre d'un contrat à durée

indéterminé, absence de clause de non-concurrence. Pour être considéré comme de la concurrence déloyale, le débauchage doit s'accompagner de manœuvres dolosives factuelles de la part de la nouvelle société du collaborateur à l'encontre de son ancienne société :

Une promesse de rémunération anormalement excessive au salarié dans le but de l'inciter à quitter son précédent employeur. Cette rémunération excessive s'étend à la promesse d'un plan de carrière exceptionnel, disproportionné par rapport aux autres salariés de même niveau. Il n'y a pas débauchage déloyal si la rémunération est normalement plus élevée.

La recherche manifeste de secrets de fabrication et autres informations dont le collaborateur débauché a eu connaissance. Le principe est qu'il puisse utiliser le savoir-faire qu'il a acquis, mais uniquement ce savoir-faire, sans rien dévoiler d'autre sur son ancien employeur.

Le détournement de clientèle, en utilisant le fichier du précédent employeur ou en utilisant des informations privilégiées dont il a connaissance afin de démarcher de nouveaux clients. Le départ d'un collaborateur, suivi immédiatement du départ de gros clients pour rejoindre sa nouvelle structure caractérise la concurrence déloyale.

Une action de débauchage massif et sélectif : les débauchages ciblés et multiples de collaborateurs dans le but de désorganiser un concurrent, comme le débauchage d'un service entier par exemple.

Les cabinets de chasseurs de tête sont parfois accusés d'encourager le débauchage. Il est à noter que ces professionnels du recrutement ont généralement un code de

déontologie strict : cloisonnement des informations sur les collaborateurs, interdiction de recruter au sein de leurs propres clients, respect de la réglementation quant à la concurrence déloyale… Certaines personnes malveillantes n'hésitent cependant pas à se faire passer pour des chasseurs de tête dans le but unique de faire parler le « candidat » et lui soutirer des informations confidentielles. Il y a quelques années, un faux cabinet de recrutement s'est installé dans le sud de la France dans le seul but d'organiser de faux entretiens de recrutement et de collecter des informations confidentielles auprès des personnes reçues, qui n'ont bien sûr jamais été embauchées.

HÉMORRAGIE DE TALENTS

Jean-Marc peut être fier de sa réussite : ayant senti avant tout le monde l'engouement naissant pour l'informatique, il a créé dans les années quatre-vingt une société spécialisée dans la programmation et dans la création de logiciels professionnels. Après des débuts plutôt chaotiques du fait d'un manque de main-d'œuvre qualifiée, son entreprise a pris un essor important est se retrouve aujourd'hui numéro une dans son secteur.

Jean-Marc, en parvenant à toujours rester à la pointe de l'innovation, a donné à sa société une certaine force d'attraction. De plus, il collabore activement avec les écoles d'ingénieurs de sa région, ce qui lui permet d'avoir toujours les meilleures recrues qu'il embauche généralement dès leur sortie d'école après les avoir accueillis en stage. Ainsi, Jean-Marc s'assure une main-d'œuvre efficace et motivée pour le développement de sa société.

Depuis quelques mois, devant la bonne santé de l'entreprise, les ingénieurs les plus anciens et les plus engagés dans la société sollicitent un intéressement financier : ils souhaitent rentrer dans

le capital. Jean-Marc n'est pas contre cette idée, mais il hésite encore à partager sa réussite personnelle.

En ce début de semaine, Jean-Marc voit un de ses ingénieurs seniors frapper à sa porte : il souhaite un entretien. Surpris, Jean-Marc le fait asseoir, et a la surprise de l'entendre lui dire qu'il souhaite partir aux États-Unis pour accompagner son épouse qui vient de décrocher un très beau poste à Washington. Jean-Marc se montre déstabilisé, car cet ingénieur est en charge de l'innovation et il dirige une équipe de spécialistes tous plus talentueux les uns que les autres. Rassurant, le partant lui affirme que son adjoint est à même de remplir ce rôle, et lui remet en même temps sa démission. Un accord est pris pour qu'il ne fasse qu'un seul mois de préavis pour préparer au mieux son déménagement. Malheureusement, tout s'accélère pour Jean-Marc dans les semaines qui suivent : son ingénieur senior n'est en fait pas parti pour accompagner son épouse mais pour rejoindre une société américaine, directement concurrente de celle de Jean-Marc. Et il emmène avec lui son équipe, puisque peu après son départ, cinq des sept ingénieurs de l'équipe Innovation donnent leur démission sans plus d'explications. Abasourdi, Jean-Marc réalise qu'il vient de se faire débaucher tout un pan de son entreprise : des ingénieurs formés, une équipe soudée et efficace, les « têtes chercheuses » de l'entreprise. Malheureusement, sa prise de conscience a été trop tardive, et il y a fort à parier que la plainte pour concurrence déloyale déposée au Tribunal de Commerce ne donnera pas grand-chose, le siège de la société concurrente étant en Californie.

Jean-Marc a été victime d'un débauchage déloyal bien organisé. Son ingénieur senior a vraisemblablement été le premier approché par la société concurrente. Il est en effet une personne clé, expérimentée, et connaissant très bien le secteur. Il est de plus le leader d'une équipe, susceptible de pouvoir amener avec lui l'ensemble de ses talents. Il n'a certainement pas été difficile de convaincre les autres, a

fortiori si leur demande d'intéressement n'a pas été suivie d'effet par leur employeur. Cette situation a toutes les caractéristiques d'un débauchage massif et sélectif : tout un service, identifié comme étant l'élément moteur de l'innovation de la société visée, et dont le départ est de nature à déstabiliser toute l'activité et à la priver d'une ressource clé.

RÉDUIRE LE RISQUE DE DÉBAUCHAGE DÉLOYAL

Il est difficile de faire la différence entre un recrutement légal et un débauchage déloyal. Un certain nombre de bonnes pratiques sont susceptibles de réduire cette menace.

Identifier les fonctions clés

Si tous les collaborateurs de l'entreprise sont importants, certains ont des positions stratégiques primordiales pour la bonne marche de la société ou pour son développement futur. L'identification des fonctions clés d'une organisation est une première étape dans la protection du patrimoine humain. Lister les collaborateurs dont le départ pourrait déstabiliser l'activité, c'est savoir à qui il faut prêter une attention toute particulière pour veiller à ce qu'il reste dans l'entreprise.

Transmettre le savoir

Le savoir et les savoir-faire sont les clés de la compétitivité des entreprises. Or, personne ne devrait être indispensable : pour éviter le débauchage déstabilisant, la transmission du savoir est un atout non négligeable. Les

entreprises qui savent faire vivre leurs savoir-faire pour éviter qu'un seul collaborateur ne détienne l'essentiel de la connaissance technique sont plus sereines s'il est amené à prendre sa retraite ou à rejoindre la concurrence.

La clause de non-concurrence

Pour que le salarié qui quitte l'entreprise ne puisse pas exercer une concurrence déloyale à l'encontre de son ancien employeur, les contrats de travail des collaborateurs ayant une fonction particulière comportent une clause de non-concurrence. Cette mesure s'applique plus particulièrement aux personnels techniques, qui ont acquis un savoir-faire bien spécifique dans leur entreprise, ou aux personnels commerciaux qui ont à disposition le fichier client de l'entreprise.

La clause de non-concurrence doit trouver un juste équilibre entre la protection des intérêts de l'ancien employeur et la liberté de travailler dont doit jouir le collaborateur. Trois arrêts rendus par la Cour de Cassation le 10 juillet 2002 clarifient une situation qui est restée longtemps ambiguë : « Attendu qu'une clause de non-concurrence n'est licite que si elle est indispensable à la protection des intérêts légitimes de l'entreprise, limitée dans le temps et dans l'espace, qu'elle tient compte des spécificités de l'emploi du salarié et comporte l'obligation pour l'employeur de verser au salarié une contrepartie financière, ces conditions étant cumulatives ». Pour être licite, la clause de non-concurrence imposée à un salarié doit donc cumuler quatre conditions impératives :

• Être indispensable à la protection des intérêts légitimes de l'entreprise quittée.

• Être limitée dans le temps et dans l'espace.

• Tenir compte des spécificités de l'emploi du collaborateur.

• Prévoir le versement d'une contrepartie financière par l'ancien employeur.

Les obligations diverses

L'employeur peut s'appuyer sur un certain nombre d'obligations et d'engagements liant le collaborateur à sa société :

• ***L'obligation de loyauté :*** en vertu de l'article 1134 du code civil, les contrats doivent être exécutés de bonne foi, pendant toute leur durée d'exécution.

• ***L'engagement de fidélité et la clause de dédit-formation :*** cette clause peut prévoir un engagement de rester, pendant une durée déterminée, au service de l'employeur qui a financé une formation au-delà de ses obligations légales ou conventionnelles, sous peine de devoir en rembourser tout ou partie du coût. Cette clause doit cependant être justifiée par la fonction du collaborateur.

• ***Le secret professionnel :*** cette clause impose au collaborateur le secret en ce qui concerne les procédés techniques de fabrication, de vente, et tout ce qui touche l'activité économique de son employeur. Le secret professionnel interdit également au collaborateur toutes manœuvres dolosives et toutes actions de dénigrement auprès du personnel de son ancien employeur, de sa clientèle, de ses

prestataires qui serait de nature à causer un préjudice. La clause de non-démarchage : cette clause interdit au collaborateur de démarcher la clientèle de son ancien employeur à l'expiration de son contrat de travail.

POUR EN SAVOIR PLUS

Roy V., *Droit du travail 2007*, Dunod, 2007.
Vogel, L., *Droit de la concurrence déloyale*, Lawlex, 2007.

PARTIE 3

LES MENACES D'ATTEINTE À L'IMAGE

8

LES RUMEURS ET LES ATTEINTES À L'IMAGE

« Lorsque le mérite est supérieur à la réputation, il faut se réserver. Lorsque le mérite est inférieur à la réputation, il faut se produire »

Gratien

LA DÉSTABILISATION COMME UNE ARME

L'image que l'on se construit est un capital instable : réversible, il est d'autant plus fragile que l'image est importante. Il faut des années pour construire une réputation, alors qu'une simple rumeur peut la ruiner en quelques jours.

La rumeur est un média particulier, qu'il est difficile d'envisager dans sa globalité tant il est difficile à définir. On lui attache un vocabulaire le plus souvent « aquatique » : la rumeur circule, elle s'infiltre, elle peut sourdre. En bref, elle est aussi complexe à contrôler que l'eau, insaisissable : on ne sait pas toujours d'où elle vient et on ne peut pas toujours l'arrêter.

Il existe de multiples définitions de la rumeur. Mais on retrouve souvent comme une de ces caractéristiques le fait que sa source est non officielle : on pourrait donc définir une rumeur comme une information dont l'origine est indéfinie et dont la teneur n'a pas été validée ou infirmée par des sources habilitées à le faire. La rumeur n'est rien

d'autre que de l'information, qui n'est pas toujours fausse, mais dont le mode de genèse et de circulation reste obscur. Tout est donc une affaire de perception : ne dit-on pas « il n'y a pas de fumée sans feu » ?

Les nouvelles technologies de l'information ont largement modifié les mécanismes des rumeurs et leur vitesse de propagation dans le corps social. Aujourd'hui, avec quelques pages internet et une campagne de SMS bien ciblée, on peut faire courir un bruit à une vitesse impressionnante de façon exponentielle. Internet est d'ailleurs un vecteur redoutable pour les chasseurs de rumeurs : réseau mondial, facile à utiliser, visité au moyen de moteurs de recherche dont les processus d'indexation sont facilement décryptables, touchant chaque jour plus d'utilisateurs : un vrai bonheur pour ceux qui utilisent la rumeur comme une arme de guerre.

Les entreprises ont intégré le risque d'atteinte à l'image par une rumeur depuis quelques années : les rumeurs impliquant les eaux de Perrier concernant une contamination au benzène ou Mercedes quant à la fiabilité de son modèle Classe A ont montré les difficultés à contrer une information insidieuse et ses effets sur le grand public. Ces crises ont également démontré que l'image et la réputation font partie du capital des entreprises. Ce capital immatériel est à prendre en compte dans la politique de gestion des risques, en l'appréhendant comme une cible potentielle d'actions accidentelles ou malveillantes : une crise d'atteinte à l'image génère le plus souvent une baisse des actions en bourse pour les sociétés cotées, des pertes de chiffres d'affaires ou une défiance de la part des utilisateurs ou des consommateurs. Et dans certains secteurs, la réputation

est particulièrement difficile à bâtir et fragile à entretenir : assurances, finances, grande distribution, des activités pour lesquelles le public est prompt a accepter les informations négatives d'où qu'elles viennent.

Face à cette fragilité de l'image et de la réputation, certains n'ont pas de scrupules pour instrumentaliser les rumeurs et en faire un outil de la guerre de l'information. Désinformer pour déstabiliser est devenu un mode opératoire de la guerre économique, et de telles actions sont difficiles à démontrer pour aller au contentieux par la suite. Afin de s'en prendre à une marque connue dont ils voulaient salir l'image pour des raisons idéologiques, un groupe d'activistes a monté une opération de déstabilisation simple mais redoutable. En identifiant les requêtes les plus fréquemment faites par les internautes sur les moteurs de recherche pour parvenir au site de l'entreprise visée, les auteurs ont utilisé le paramétrage de ces moteurs pour indexer des pages afin qu'elles apparaissent systématiquement en haut de la liste dans les réponses. Sur ces pages, la société ciblée par l'action apparaissait de façon négative, avec des commentaires d'utilisateurs très mécontents ou des tests de produits très critiques. Des renvois vers des blogs, eux aussi montés de toutes pièces pour la circonstance, étaient proposés sur chacune des pages. En quelques heures, ces activistes ont orienté les réponses aux recherches des internautes pour atteindre l'image de leur cible. Ce type d'opération s'appelle un « caviadarge », qui laisse des traces jusqu'à ce que les pages décrivant la société de façon négative soient définitivement supprimées du web.

La déstabilisation est une arme dangereuse, car la rumeur a un caractère très volatil et difficilement maîtrisable. Il est

rare que les auteurs de telles actions puissent contrôler leurs conséquences, et les effets de « bouche à oreille » amplifient et modifient les informations lâchées sans plus de contrôle de la part des auteurs de l'atteinte à l'image. L'arme peut même se retourner contre son auteur : une atteinte à l'image, organisée par une entreprise contre le produit d'une de ses concurrents, peut se retourner contre le secteur dans son ensemble au-delà de la société visée initialement, impactant du même coup l'initiateur de la déstabilisation.

UN MÉDICAMENT DANGEREUX

Il y a quelques années, un laboratoire pharmaceutique élabore un nouveau produit destiné à améliorer la vie des patients atteints d'une maladie chronique répandue. Ce produit à vocation à être un block buster, c'est-à-dire à booster les ventes du département à l'origine de cette innovation. Il fait l'objet de toute l'attention des services marketing et communication du groupe.

Alors que le produit doit obtenir son autorisation de mise sur le marché dans plusieurs pays européens, une information commence à circuler dans le milieu médical : le produit aurait des effets secondaires désastreux sur les patients ayant des problèmes de tension artérielle, effets potentiellement mortels. Ces effets auraient été cachés par le laboratoire pour ne pas nuire à son produit et pour ne pas perdre les fonds investis depuis plusieurs années sur la molécule. La rumeur enfle rapidement, et des compléments d'informations sont demandés par les autorités sanitaires de plusieurs pays concernant l'autorisation de mise sur le marché. Des blogs commencent à évoquer le sujet, et sont peu favorables au produit.

Le laboratoire n'est pas pris au dépourvu, car tous les tests ont été faits en amont de la commercialisation, et il lui est facile de

démontrer que l'information est fausse. Echaudé par cette affaire, le laboratoire sollicite une société d'investigation pour faire la lumière sur la rumeur. Après plusieurs jours d'enquête, l'implication d'une société spécialisée dans la guerre économique est démontrée. Au travers de plusieurs sites internet créés pour l'occasion, et de blogs animés par des complices, elle à divulgué de faux rapports de tests qui auraient été faits aux États-Unis. Informations prises, les professeurs de médecine signataires des rapports sont complètement inconnus, et les cas d'effets secondaires évoqués n'ont jamais existé. Des procédures judiciaires ont été engagées par le laboratoire victime contre la société en question. Il n'a pas pu être démontré qu'elle agissait pour le compte d'un laboratoire concurrent, même si les soupçons ont été très forts en ce sens.

Dans cette affaire, l'information a circulé très rapidement grâce à Internet et a été entretenue par des blogs spécifiquement constitués par les agresseurs. Fort heureusement, la rumeur se basait sur une donnée dont le caractère erroné était facile à démontrer. De plus, le fait que l'action de déstabilisation ait été faite organisée de toute pièce dans l'intention de nuire aurait pu avoir des effets désastreux si elle n'avait pas été aussi grossière. Il est à souligner que bien que les faux rapports aient été démentis, il y a encore des médecins qui questionnent les visiteurs médicaux du laboratoire producteur pour savoir ce qu'il en est des effets secondaires sur les patients atteints de problèmes de tension artérielle. Calomniez, il en reste toujours quelque chose.

Apple a subi en Mai 2007 une crise d'atteinte à l'image liée à une rumeur, faisant chuter le cours de bourse du groupe de presque 5 % en quelques heures.

Un site internet spécialisé dans les nouvelles technologies et les innovations techniques sort une information très embarrassante

> pour Apple : les mises sur le marché du nouveau système d'exploitation Leopard, et du téléphone révolutionnaire Iphone seraient retardées du fait de problèmes techniques inattendus. L'information est d'importance, et elle émane d'un email qui circule au sein du groupe Apple lui-même. Ce sont d'ailleurs des collaborateurs d'Apple qui ont transmis l'information au site internet. Pour vérifier que ce qui est dit est vrai, les éditeurs du site appellent plusieurs de leurs contacts chez Apple qui confirme que cet email s'échange entre collaborateurs.
>
> L'information se propage très rapidement sur le web, au point que l'action perd presque 5 % en quelques heures.
>
> Apple réagit rapidement pour démentir l'information, mais le mal est fait : beaucoup pensent que le démenti n'est là que pour différer l'annonce de retards dans la sortie des produits.

Apple a les reins assez solides pour se sortir sans trop de dommages de ce type d'atteinte à l'image. Mais cette déstabilisation, dont le mobile reste flou, a montré la fragilité des cours de bourse, liés aux rumeurs qui circulent souvent sans fondement. Il s'avère que si l'information contenue dans l'email était fausse, les échanges ont bien eu lieu entre personnels d'Apple. Celui ou ceux qui ont organisé ce qui semble être un canular ont réussi à faire entrer leur message dans les flux d'informations Apple. Dès lors, quand ceux qui, involontairement, diffusent la rumeur pensent qu'elle est véridique, il est difficile de savoir par qui et comment elle a commencé. En trompant des collaborateurs d'Apple, les créateurs de la rumeur ont donné du crédit à leur information, et lui ont donné une authenticité. C'est l'exemple type d'une rumeur qui peut se montrer très dévastatrice : basée sur une information plausible, relayée et crédibilisée par des collaborateurs internes de bonne foi, elle s'est

propagée à grande vitesse et le démenti n'a eu que des effets limité.

ANTICIPER ET GÉRER LES RUMEURS ET LES ATTEINTES À L'IMAGE

Bien qu'elles soient difficiles à saisir, les rumeurs obéissent à des règles spécifiques dont il est possible de démonter le processus. Ceci les rend détectables, et permet au cas par cas d'établir des stratégies appropriées pour en réduire les effets.

Organiser une veille

La détection d'une rumeur est complexe et relève de la veille. La veille informationnelle est un véritable métier de spécialiste : il faut être à l'écoute de l'ensemble des médias formels et informels, et ce dans toutes les secteurs pouvant impacter l'entreprise : partenaires, utilisateurs, consommateurs, autorités de tutelles, pouvoirs publics, ordres professionnels.

Si Internet est un outil qui permet de véhiculer rapidement les rumeurs, il permet aussi de les détecter très en amont pour les contrer au plus tôt. Des sociétés spécialisées proposent des veilles informationnelles dédiées à la recherche de rumeurs susceptibles d'atteindre l'image d'une entreprise. Ces veilles peuvent porter sur le nom de l'entreprise, le nom des dirigeants, des produits vendus ou de tout autre vecteur lié à la société. Une fois détectées, les rumeurs sont analysées pour en connaître l'origine, la motivation des auteurs et pour proposer les stratégies de contre-influence les stratégies les plus adaptées.

Contrer les rumeurs avant qu'elles ne sortent

Dès qu'une rumeur est anticipée ou détectée, il existe plusieurs possibilités :

• ***Attendre sans rien faire***

Attirer l'attention sur une rumeur naissante en communiquant trop tôt, alors qu'elle n'est pas encore sortie dans les média, est une erreur grave car c'est l'entreprise elle-même qui génère l'attention négative. Par contre, attendre peut aussi laisser libre cours à la rumeur qu'on ne pourra plus rattraper par la suite.

• ***Lancer des contre-feux***

Quand une rumeur se prépare à sortir, lancer deux ou trois autres rumeurs contradictoires peut invalider la première en la tuant dans l'œuf. Dans ce cas, il faut doser les contre-feux pour utiliser les mêmes médias que la rumeur initiale et ne pas en faire plus que ce qui est nécessaire. En diffusant des informations contradictoires sur le même thème, on invalide toutes les informations qui s'annulent les unes les autres.

• ***Dissuader les auteurs de la déstabilisation***

Si la veille permet d'identifier les auteurs de la tentative d'atteinte malveillante, il peut être judicieux de leur faire savoir que leur action a été détectée. La poursuivre ne pourrait que générer un contentieux médiatique et judiciaire.

Conduire une stratégie anti-rumeur quand elle se produit

Un plan anti-rumeur peut envisager plusieurs scénarios, ayant des implications et des effets très différents.

• ***Garder le silence :*** en situation difficile, garder le silence et attendre que cela passe n'a jamais été une stratégie. Se taire alors que l'on est agressé par une rumeur, c'est donner du crédit à l'information car « *qui ne dit mot consent* ». Certaines sociétés préfèrent faire le dos rond en attendant que la rumeur soit oubliée. Cela peut fonctionner si l'entreprise jouit d'une vraie crédibilité dans son secteur, et si les informations propagées sont suffisamment peu crédibles en elles-mêmes.

• ***Démentir :*** c'est déjà un premier pas dans une stratégie anti-rumeur, mais ce n'est pas suffisant en soi. Le démenti suite à une rumeur provoque systématiquement de la suspicion. Ensuite, il est rare que les médias qui ont propagé la rumeur acceptent de bonne grâce d'annoncer qu'ils se sont trompés : les démentis, hormis quand ils sont flagrants, ont rarement la même exposition médiatique que la rumeur elle-même. Enfin, en démentant, l'entreprise ajoute une nouvelle information à celle fournie par la rumeur, jetant le doute sur ces deux informations, la fausse et la vraie.

• ***Faire diversion :*** il s'agit de donner une information qui ne dément pas la rumeur mais qui attire l'attention sur un autre sujet, sur lequel l'entreprise peut se valoriser, montrer une image positive et susciter l'intérêt des médias qui vont mettre la rumeur au second plan.

• ***Démontrer l'origine malveillante de la rumeur le cas échéant :*** quand l'origine de l'atteinte à l'image est manifestement malveillante, la société victime peut lancer une investigation spécifique pour identifier les auteurs, les modes opératoires et engager une procédure au contentieux.

Dans la gestion d'une rumeur, il faut cependant savoir raison garder dans la communication. Une multinationale qui consacre des millions d'euros dans sa communication peut se permettre une forte présence médiatique. Par contre, une entreprise discrète qui communique peu ne doit pas en rajouter ni trop s'exposer car une rupture dans les habitudes des médias peut développer un climat de suspicion.

POUR EN SAVOIR PLUS

Kapferrer J.-N., *Rumeurs*, Seuil, 1998.
Laurier P., *Déstabilisation d'entreprises*, Maxima, 2004.
Froissart P., *La rumeur, histoires et fantasmes*, Belin, 2002.

9

LA CORRUPTION

« La corruption à laquelle participent les entreprises est un piège dont on ne sort pas et qui fini par coûter des fortunes considérables »

Un chef d'entreprise travaillant en Afrique.

LA CORRUPTION, OMNIPRÉSENTE DANS LE MONDE DES AFFAIRES

Estimée à près 1 000 milliards de dollars par la Banque Mondiale, la corruption est omniprésente dans le monde des affaires. Les différents rapports de Transparency International, ONG travaillant à la lutte contre ce phénomène, montre que tous les pays du monde sont touchés à des degrés divers. Depuis quelques années, la corruption est incriminée dans plusieurs conventions internationales : l'OCDE a adopté le 21 novembre 1997 une convention sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales, l'ONU a fait de même en adoptant l'UNCAC[1] le 31 Octobre 2003, démontrant le sérieux avec lequel le phénomène et ses impacts sur l'économie mondiale sont traités. Depuis, de nombreuses entreprises de toutes les tailles ont été condamnées par leurs juridictions nationales pour avoir corrompus ou tenté de corrompre. La commission indé-

1. United Nations Convention Against Corruption.

pendante d'enquête sur le programme des Nations Unies *Pétrole contre nourriture* a identifié 2 412 entreprises impliquées dans des affaires de corruption, dont près de 200 françaises.

Classement mondial de la corruption en 2006 Source : Transparency International			
Rang	**Pays les moins corrompus**	**Rang**	**Pays les plus corrompus**
1	Finlande	**168**	Guinée
--	Islande	**168**	Laos
--	Nouvelle-Zélande	**172**	Afghanistan
4	Danemark	**172**	Tchad
5	Singapour	**172**	Soudan
6	Suède	**175**	Tonga
7	Suisse	**175**	Uzbekistan
8	Norvège	**177**	Haïti
9	Australie	**178**	Irak
10	Pays-Bas	**179**	Somalie

Dans bon nombre de pays, l'achat des faveurs d'un fonctionnaire, d'un douanier ou d'un politique est monnaie courante : certaines entreprises qui travaillent à l'international sont habituées à payer des dessous de tables en échange de l'attribution d'un contrat ou pour voir leur dossier placé bien en évidence sur le bureau d'un décideur politique.

Le Code pénal prévoit et réprime la corruption dans son article 435-4, modifié par la loi du 13 novembre 2007 : « Est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende le fait, par quiconque, de proposer, sans droit, à tout moment, directement ou indirectement, des offres, des promesses, des dons, des présents ou des avantages quelconques à une personne, pour elle-même ou pour autrui, afin qu'elle abuse de son influence réelle ou supposée en vue de faire obtenir des distinctions, des emplois, des marchés ou toute autre décision favorable d'une personne dépositaire de l'autorité publique, chargée d'une mission de service public ou investie d'un mandat électif public au sein d'une organisation internationale publique.

Est puni des mêmes peines le fait, par quiconque, de céder à toute personne qui sollicite, à tout moment, directement ou indirectement, des offres, des promesses, des dons, des présents ou des avantages quelconques, pour elle-même ou pour autrui, afin d'abuser de son influence réelle ou supposée en vue de faire obtenir des distinctions, des emplois, des marchés ou toute autre décision favorable d'une personne visée au premier alinéa. »

Cette définition du Code pénal distingue la corruption active de la corruption passive, mais prévoit de condamner le corrupteur aux mêmes peines que le corrompu.

L'enjeu de la corruption pour les entreprises n'est pas simplement pénal. En utilisant ce moyen illégal, les entreprises engagent leur responsabilité sociale : un cas de corruption révélé au grand public dégrade considérablement l'image de la société et engendre le plus souvent une forte sanction des marchés financiers : en 2003, la société

américaine Titan se voit mise en cause dans une affaire de corruption au Bénin. Lors de cette révélation, Titan est en voie d'être rachetée par la société Lockheed : l'annonce de cette mise en cause a conduit au gel de la transaction, et à l'effondrement de l'action de la société Titan.

Des dispositifs étatiques se mettent en place pour inciter les entreprises à ne plus avoir recours à la corruption. Un des dispositifs les plus anciens est le « Foreign Corrupt Practices Ac », adoptée par les États-Unis en 1977. Ce texte s'applique aux entreprises américaines, mais également aux multinationales dont les sièges se trouvent sur le territoire américain. Les enquêtes se multiplient sur le thème : la Banque Mondiale a récemment enquêté sur le temps passé par les chefs d'entreprise à gérer leurs contacts avec les fonctionnaires dans certains pays. Certains passent l'essentiel de leur temps à débrouiller leurs pratiques de corruption, avec tous les risques que cela comporte. Car la corruption est un outil de court terme : quand une société entre dans ces pratiques, les conséquences qui s'ensuivent sont souvent graves, sans compter le fait qu'une fois entré dans ce jeu, il est difficile d'en sortir et de cesser de corrompre.

Il n'est pas rare d'entendre un chef d'entreprise dire qu'il souhaiterait bien ne pas céder à la corruption, mais que sans cela, impossible d'obtenir les marchés souhaités dans certains pays ou sur certaines zones. Car deux stratégies s'offrent aux sociétés face à une sollicitation :

• accepter de payer pour obtenir un avantage, mais en rentrant dans un cercle infernal ;

• refuser de payer, et courir le risque de perte de chiffre d'affaire.

Il n'existe pas encore de solution miracle pour faire face à ce fléau, mais les choses s'organisent pour fournir aux entrepreneurs les outils pour travailler de manière éthique et efficace.

Les cas de corruption ne cessent de défrayer la chronique. L'affaire qui a touché le groupe allemand Siemens en est un exemple. Plusieurs des plus hauts dirigeants ont été mis en cause dans une affaire de caisse noire : Heinrich von Pierer, président du conseil de surveillance à la tête du groupe jusqu'en janvier 2005, et Klaus Kleinfeld, PDG du groupe, ont dû quitter leurs fonctions après de multiples révélations. Cette affaire a créé une tourmente dans laquelle l'ensemble de la société a laissé des plumes. Dans un communiqué de presse, le groupe Siemens a annoncé avoir déboursé plusieurs millions d'euros pour mener une enquête interne, laissant entendre que la société en tant que personne morale ou d'autres dirigeants feraient vraisemblablement l'objet de procédures au civil et au pénal. Malgré des résultats en hausse de plus de 49 %, le PDG de Siemens Klaus Kleinfeld a quitté ses fonctions à cause de cette affaire.

UN PIÈGE INEXTRICABLE

> Samir est le directeur d'une filiale africaine d'un grand groupe industriel européen. Il supervise la direction de plusieurs usines de montage au Maghreb et en Afrique francophone et doit assurer la livraison de pièces industrielles aux autres sites du groupe dispersés dans toute l'Europe. Samir sait qu'une rupture dans la production de ces sites impactera très rapidement l'ensemble de l'activité de son groupe.

> Dans le cadre de l'audit interne, Samir est interrogé par des consultants envoyés par la direction générale du groupe. Ceux-ci ont identifié dans les comptes des anomalies, et notamment des remboursements de notes de frais étrangement élevées. En guise de réponse, Samir leur demande s'ils sont déjà venus travailler en Afrique du Nord. Devant la réponse négative des jeunes consultants, Samir leur explique comment il peut assurer l'efficacité de ses chaînes de production : pour aller plus vite, il « graisse la patte » de plusieurs fonctionnaires locaux. « Nous n'avons pas le choix ici. Quand certaines autorités locales s'aperçoivent que vous appartenez à un grand groupe, ils viennent vous expliquer que pour que le système devienne plus fluide, il faut mettre de « l'huile » dans les rouages. Si vous ne payez pas, votre marchandise sera bloquée au port pendant plusieurs jours, ou sera renvoyée à l'expéditeur pour défaut de procédure. Si je ne paye pas, on peut arrêter les chaînes de production tout de suite ». Ce que n'avait pas prévu Samir, c'est qu'en quelques années, le système organisé pour « fluidifier » les approvisionnements s'est transformé en piège inextricable. Avec le temps, les sommes demandées n'ont cessé de croître, tout comme le nombre de personnes les réclamant en échange de leur silence ou de leur appui. Au final, Sami s'est enfermé dans un système duquel il ne peut plus sortir et dont il est complètement dépendant.

Au cours de multiples discussions menées avec Samir au sujet de cette corruption dans laquelle il s'est laissé prendre, il est apparu plusieurs facteurs :

• Une fois commencée, la corruption ne s'arrête que par un acte ferme et brutal qui aura, quoi qu'il en soit, des répercussions sur l'activité.

• Samir ne sait pas comment « passer la main » : quelle sera la réaction de son groupe s'il exprime clairement une situation dont personne n'est dupe, et comment passer la

main à un remplaçant sans lui expliquer le mode de fonctionnement mis en place ?

• Le risque pénal encouru à la fois par Samir et par ceux qu'il paye est de plus en plus important, sans parler du risque social et d'image encouru par le groupe.

• Lors d'une de ces discussions, Samir a eu cette phrase terrible : « Cela coûtera beaucoup plus cher de lutter contre ce phénomène que de céder au chantage […]. Nous n'avons pas toujours les moyens d'être transparents ». Proche de l'extorsion et du racket, ces pratiques de corruption sont difficiles à éradiquer sans la mise en œuvre de politiques publiques et privées coordonnées[1].

PRÉVENIR ET RÉDUIRE LE RISQUE DE CORRUPTION

Les entreprises, confrontées à ce fléau du développement, et notamment à l'international, sont conscientes des risques qu'elles courent. Elles cherchent régulièrement à développer des initiatives dans le sens d'une réduction de la corruption, et intègrent les dimensions éthiques et sociales dans leurs stratégies de développement. Elles relayent en cela les initiatives déjà lancées par les principales institutions internationales.

Les standards internationaux

Les divers textes et conventions édictés par les institutions internationales (ONU, OCDE) constituent une base pour la création de standards basés sur la mise en œuvre de bonnes pratiques. Repris et développés par les institutions

1. Voir chapitre « Rackets et extorsions ».

nationales, ces standards commencent à instaurer une norme éthique au travers de laquelle les entreprises de toutes tailles et de tous secteurs peuvent se retrouver pour harmoniser leurs dispositifs internes de gestion du risque de corruption. Plusieurs CCI[1] ont repris ses textes pour inciter leurs ressortissants à adhérer au principe de leurs déclarations.

L'application de ces standards est aussi un facteur de qualité et de plus-value : les investisseurs commencent à les exiger dans leur notation extra-financière pour apprécier les entreprises et leurs actions. L'application de ces standards est aussi un moyen de démontrer, de la part de la société qui le promeut, sa volonté de s'inscrire dans le cadre d'un développement durable et socialement responsable.

L'indice FTSE4Good[2] qualifie les entreprises engagées dans des politiques de développement éthique, notamment par la prévention et la lutte contre les actes de corruption.

Les bonnes pratiques des entreprises

De nombreuses sociétés ont pris d'initiative la décision de constituer en interne une charte anti-corruption, incitant l'ensemble des filiales et des collaborateurs à respecter un certain nombre de critères ou de pratiques dans l'exercice de leurs fonctions.

• ***La publication des comptes :*** c'est le premier pas d'un dispositif interne. Il s'agit de rendre publics les investissements mis en œuvre sur les projets, notamment internationaux, pour permettre une meilleure transparence. Cette

1. Chambres de Commerce et d'Industrie.
2. www.ftse.com.

publication exige un contrôle interne sur la véracité des chiffres annoncés, et la mise en œuvre de sanctions internes en cas de non respect des règles. Certaines ONG ont d'ailleurs lancé des campagnes dans le sens de la publication des comptes, la plus connue étant la campagne « *Publish what you pay* ».

• ***Les dispositifs d'alerte éthique :*** la loi du 13 novembre 2007, relative à la lutte contre la corruption, crée un régime de protection pour les collaborateurs qui dénoncent les faits de corruption dont ils auraient eu connaissance dans l'exercice de leurs fonctions ou dans le cadre de projets qu'ils gèrent. Ces dispositifs ressemblent à une pratique déjà mise en œuvre dans un cadre plus large, appelée *whistleblowing*, et qui incitent les salariés à dénoncer de façon anonyme les actes répréhensibles dont ils pourraient être témoins.

• ***L'établissement d'une grille de rémunération type*** pour les agents, correspondant à une rémunération raisonnablement pratiquée en fonction des missions accomplies. La problématique des agents est un élément important de la prévention de la corruption : quand commence la corruption, quand s'arrête le lobbying ? il existe de nombreux pays dans lesquels faire du business sans agent est quasiment impossible. Instaurer des règles de fonctionnement « normales » pour gérer les agents semble être un facteur de transparence efficace, qu'il faut avant tout faire accepter aux collaborateurs habitués à utiliser ce genre d'intermédiaire, et également aux intermédiaires eux-mêmes.

• ***Le recours à des agences privées de notation :*** certaines agences se sont spécialisées dans l'accompagnement des

entreprises dans leurs processus de lutte contre la corruption. Elles délivrent des certificats aux sociétés qui jouent le jeu, certificats permettant de démontrer la bonne foi de l'entreprise en cas de mise en cause.

Les alliances sectorielles

Des démarches anti-corruption peuvent être organisées au niveau des fédérations professionnelles. En jouant sur l'aspect sectoriel de tels dispositifs, les entreprises peuvent donner plus d'impact et plus d'envergure à leurs actions. En regroupant toutes les sociétés d'une même activité, les dispositifs sectoriels permettent d'apurer un marché et de dissuader ceux qui sollicitent les entreprises en uniformisant les réponses négatives données par tous.

Les dispositifs étatiques

Difficile de réduire la corruption si les responsables politiques ne peuvent pas contrôler leurs propres collaborateurs. Comment empêcher un douanier local de demander un bakchich pour apposer des tampons plus rapidement sur un document de transit ? Comment faire cesser le racket de forces de polices locales peu scrupuleuses ? C'est un enjeu important pour les pays dans lesquels la corruption sévit, mais c'est un enjeu sur lequel les entreprises n'ont pas de prise, hormis celle d'imposer ces dispositifs étatiques en refusant d'entrer dans le cercle vicieux de la corruption.

Ces dispositifs étatiques commencent à porter leurs fruits : le président du Nigéria a annoncé la mise en œuvre de dispositifs anti-corruption et la publication des recettes

pétrolières du pays, sans aucune clause de confidentialité comme c'était le cas jusqu'à présent.

POUR EN SAVOIR PLUS

Dommel D., *Face à la corruption*, Karthala, 2003.
Boulanger H., *La criminalité économique en Europe*, PUF, 2002.
Gazette trimestrielle de *Transparency International*.

10

LA COMMUNICATION DE CRISE

« Nous sommes dans un siècle de l'image. Pour le bien comme pour le mal, nous subissons plus que jamais l'action de l'image »

Gaston Bachelard

LA VAGUE MÉDIATIQUE : ENTRE SURF ET NOYADE

La gestion de crise est une pratique de plus en plus souvent prise en compte par les entreprises, soit qu'elles aient été directement impactées par un évènement grave, soit qu'elles aient pris conscience du risque de crise en observant leur environnement et les déstabilisations qui s'y produisent. Les situations de crise peuvent toucher tous les types d'entreprises, quelle que soit leur taille, leur activité ou leur nationalité.

10 communications de crise Source : « Crises, de 10 à 100 » par Thierry Libaert		
30/ 06/04	**Mc Donald's**	Sortie en France du film de Morgan Spurlock *"Super size me"* dirigé contre le groupe américain.
23/ 05/04	**ADP**	Effondrement du terminal aéroportuaire le plus récent de Roissy, quatre morts. La conception du bâtiment est mise en cause.

13/ 01/04	**Adecco**	Le titre du groupe d'intérim perd 47,8 % de sa valeur à la suite de soupçons d'irrégularités comptables.
05/ 08/03	**Santé publique**	La canicule provoque 12.000 décès. Le gouvernement et les institutions sont mis en cause sur la gestion de l'événement.
01/ 03/03	**Le Monde**	Publication du livre de Pierre Péan et Philippe Cohen : *La face cachée du Monde.* Le quotidien décide d'attaquer les deux auteurs.
04/ 01/03	**Cofiroute**	15 000 véhicules sont bloqués sur le réseau autoroutier de l'Ouest de la France en raison d'importantes chutes de neige.
18/ 12/02	**Buffalo Grill**	Suspicion (affaire en cours) d'importation de viande britannique malgré l'embargo lié à la vache folle.
18/ 11/02	**Prestige**	Naufrage du pétrolier au large des côtes portugaises. Marées noires sur la côte Atlantique.
02/ 12/01	**Enron**	Le courtier en énergie américain est mis en faillite. Il entraîne dans sa chute le cabinet Andersen.
21/ 09/01	**Total - AZF**	Explosion à l'usine Grande-Paroisse de Toulouse. 29 morts. Les scénarios évoqués sur la cause de cette explosion sont multiples.

Les crises sont de plus en plus souvent médiatisées, avec une rapidité et une efficacité qui surprend les entreprises les mieux préparées. Parfois même, une crise résulte moins de l'événement déclencheur qui se produit que du contexte qui l'entoure et du tourbillon médiatique qu'il génère. C'est tout l'aspect ambigu de la communication de crise : une crise mal gérée mais entourée d'une communication efficace sera moins mal perçue par l'opinion qu'une crise bien conduite mais dont la communication aura été négligée.

Pour faire face à de tels évènements, les entreprises s'organisent en interne et mettent en place des dispositifs et des procédures spécifiques : une cartographie des risques recensant les principales menaces, une ou plusieurs cellules de crise pour conduire l'incident et prendre les meilleures décisions, et des dispositifs de continuité de l'activité en cas de graves menaces sur la poursuite de la production ou du service. Mais un des aspects de la gestion de la crise reste encore trop négligé par les entreprises : la communication avec les medias et les conséquences qu'elle peut avoir sur l'image de la société. Il est donc important de prévoir une organisation de gestion des crises globale, incluant bien entendu des dispositifs de conduite, mais également des correspondants « communication de crise » capables de répondre aux questions des journalistes et autres parties prenantes qui ne manqueront pas de se manifester dès le début de l'incident.

Pourquoi considérer la communication de crise comme une menace potentielle planant au-dessus des entreprises ? Tout d'abord, parce que la négligence de son importance et de ses impacts potentiels génère des dégâts en termes d'image et de confiance des clients ou des collaborateurs souvent très longs à réparer. Ensuite, parce que les acteurs qui pourraient être amenés à s'intéresser à l'entreprise en crise ne sont pas toujours de bonne foi ni toujours très objectifs. Enfin, parce que l'excès de confiance dans ses capacités à faire face va faire trébucher le dirigeant devant les caméras de télévision et les micros de la presse.

L'effet accélérateur des parties prenantes qui peuvent, à quelque titre que ce soit, être impliquées dans une action de communication de crise est non négligeable ; leur

arrivée au cœur de la crise peut s'avérer plus déstabilisatrice encore que la crise elle-même. Parmi ces parties prenantes, citons notamment :

• ***Les médias :*** en quête d'informations, et si possible d'informations de « première main », les médias se caractérisent par une réactivité impressionnante et une capacité à poser les questions délicates pouvant mettre un dirigeant dans l'embarras. Souvent perçus comme des agresseurs, les journalistes font leur travail d'investigation avec eux-mêmes des contraintes particulières : la nécessité de fournir des articles dans des délais très courts, restreignant d'autant le temps de vérification, et l'obligation de présenter un sujet susceptible d'attirer la plus grande audience. Les entreprises de presse sont avant tout des entreprises, qui doivent vendre des journaux ou attirer des téléspectateurs.

• ***Les autorités judiciaires :*** l'implication des autorités judiciaires, magistrats ou autres services officiels d'investigation laisse planer sur l'affaire une suspicion terrible, même quand l'entreprise est innocente des faits dont on l'accuse. Et l'annonce de l'ouverture d'une enquête ne fait que rajouter au sentiment que des choses louches se trament certainement.

• ***Les instances professionnelles :*** à l'instar des autorités judiciaires, l'entrée en lice des instances professionnelles suggère que des entorses aux règlements ou aux règles de déontologie ont été commises, même si à la fin de l'affaire, tout prouve que ce ne fut pas le cas.

Les effets d'une communication de crise difficile ne sont pas toujours directs, et peuvent impacter une entreprise, une profession voir même tout un secteur d'activité

alors même que seule une entité de ce secteur a raté sa communication. C'est ce que l'on appelle un impact par rebond, comme cela a été le cas lors de la crise de l'Association pour la Recherche contre le Cancer. Des accusations de malversations ont été lancées contre son président, et une procédure judiciaire engagée. Très rapidement, l'ensemble des envois de dons ont sensiblement diminué pour tous les organismes caritatifs, bien que n'ayant pas directement été visés par la crise. Même mésaventure pour un pâtissier belge il y a quelques années : alors que les premiers éléments de l'affaire Dutroux commencent à être portés à la connaissance du public, la police interpelle un dénommé Nihoul, dont le nom est également cité dans la presse. Pour son malheur, un des meilleurs pâtissiers bruxellois porte le même nom. Bien qu'il n'ait rien à voir, ni de prêt ni de loin, avec l'affaire Dutroux, le pâtissier Edouard Nihoul voit sa clientèle diminuer sans ne pouvoir rien y faire. Malgré de multiples démentis, il aura été indirectement impacté par une crise avec laquelle il n'avait aucun rapport.

UN RESTAURATEUR SUR LE GRILL

Le groupe Buffalo Grill a traversé une tempête médiatique qui a marqué le début des années 2000. Suite des dénonciations faites aux forces de police, la chaîne de restauration est soupçonnée d'avoir importé de la viande britannique, en pleine crise de la vache folle, et après l'embargo établi en 1996. La juge d'instruction Marie-Odile Bertella-Geffroy est saisie d'une enquête relative au décès de plusieurs personnes atteintes de la maladie de Creutzfeldt-Jakob. Au vu des éléments en sa possession, elle met en examen le fondateur du groupe Buffalo Grill, Christian Picart, et son directeur des achats, Daniel Batailler, générant

ainsi une vaste crise de communication entraînant une chute de près de 40 % de la fréquentation des restaurants de la chaîne.

Mis en examen, Christian Picart ne peut plus s'exprimer. Son avocat se présente alors comme un des interlocuteurs pour les médias. Mais la chaîne garde le silence pendant de nombreuses heures, avant que plusieurs communications contradictoires ne soient faites, jetant le trouble sur une situation qui n'avait pas besoin de cela. Contacté pour aider à la mise en place de la communication, le philosophe Alain Etchegoyen quitte l'équipe de crise pour des raisons de discordes internes, ajoutant au flou ambiant. L'intervention des pouvoirs publics dans le débat, en l'occurrence Renaud Dutreil, secrétaire d'État au commerce et aux PME, alimente les rumeurs et les contradictions.

Face à autant de désorganisation, François Picart, frère du fondateur et membre du conseil de surveillance, prend les commandes de la communication et fait entrer une agence spécialisée dans le jeu. Une manifestation de soutien des salariés de Buffalo Grill est appuyée par la direction, un site internet est mis en ligne, et les rumeurs circulant autour de l'affaire sont systématiquement attaquées. Une campagne de presse est ensuite lancée pour reprendre l'initiative, adressée à la fois aux consommateurs mais également aux franchisés.

L'affaire du Buffalo Grill démontre le danger que fait planer une communication de crise non maîtrisée. Par manque de préparation, par l'émergence de discordes au sein de l'équipe de crise, par des discours désordonnés ou contradictoires, Buffalo Grill est passé très près d'une catastrophe économique dont il aurait été difficile de se relever. En prenant le leadership sur la conduite de cette affaire, et en organisant une action proactive de communication, François Picart a certainement permis à la marque de se relever et de passer la tempête dans les conditions les moins défavorables possible.

ANTICIPER LE RISQUE D'UNE MAUVAISE COMMUNICATION DE CRISE

Face au risque d'une atteinte à l'image liée, non pas à une action de déstabilisation malveillante, mais réellement à une communication inadaptée ou maladroite, les entreprises doivent se préparer à réagir dans l'urgence aux situations de crises qu'elles pourraient connaître. Et chaque entreprise, chaque situation implique une stratégie différente qu'il faudra adapter au contexte et aux parties prenantes engagées dans l'affaire.

La préparation d'un plan de communication de crise

C'est la base de la communication de crise efficace : comment être bon au match si on ne se prépare pas à jouer ? Cette préparation repose sur plusieurs étapes :

• L'identification de l'ensemble des scénarios de crise que l'entreprise pourrait connaître : cause, émergence, signaux précurseurs, évolution, point de paroxysme, durée et conditions d'un retour à la normale.

• La cartographie des parties prenantes pouvant être impliquées, à quelque titre que ce soit, dans l'affaire : type de partie prenante, attentes, modes opératoires, moyens d'en faire des alliés.

• L'identification des portes-paroles de l'entreprise susceptibles d'intervenir devant les medias.

• La constitution d'un stock argumentaire adapté à chacune des crises potentielles.

• L'annuaire de la presse locale et nationale pour avoir le bon contact au bon moment.

Le media training

Face à la presse, rares sont les chefs d'entreprises qui peuvent garder leurs moyens au milieu d'une situation dégradée et de questions qui fusent. Un seul moyen de s'y préparer : le media training. Devant un ou plusieurs journalistes jouant leurs propres rôles, les participants peuvent affronter des rafales de questions ou de remarques plus acerbes les unes que les autres et y répondre au mieux. Ces exercices, généralement filmés, sont ensuite débriefés pour en tirer les meilleurs enseignements et identifier les erreurs commises. Chaque dirigeant qui a eu à affronter la presse en situation de crise, et qui s'y était préparé par un media training, a loué l'intérêt d'une telle mise en situation préalable.

Les principes de la communication de crise

Les principes de base de la communication en situation de crise sont :

• ***La réactivité :*** il faut agir vite, répondre rapidement aux attentes des médias avant même qu'elles ne soient manifestées. Attendre, c'est prendre le risque que la presse interprète des faits ou invente des informations qu'on ne lui donne pas.

• ***L'occupation de l'espace médiatique :*** communiquer, c'est occuper l'espace médiatique le plus largement possible. Presse écrite, radio, télévision, Internet, aucun media ne doit être négligé pour passer les messages que l'on souhaite transmettre.

• ***La cohérence des propos :*** tous les aspects de la communication doivent être cohérents. Un seul discours

discordant, et c'est l'ensemble de la communication de crise qui s'effondre.

• ***L'honnêteté :*** le mensonge finit toujours par ressurgir, et il est inutile de mentir en croisant les doigts et en espérant que personne ne s'en aperçoive. De plus, soutenir un mensonge, même par omission, face à des journalistes qui ne manqueront pas de vérifier l'information est un risque qu'il vaut mieux éviter de courir.

Les stratégies de communication de crise

L'objectif de la communication de crise est de fournir au public des grilles de lecture de la situation. Cela permet d'éviter les interprétations, les incompréhensions et les rumeurs. Encore faut-il que la stratégie adoptée soit efficace. On peut identifier un certain nombre de stratégies face à une situation dégradée :

• ***Le refus de s'exprimer :*** c'est la pire des stratégies, généralement exprimée par « tout est sous contrôle ». Refuser de parler, c'est laisser les autres parler à sa place et ne plus rien contrôler de ce qui se dit.

• ***La reconnaissance responsable du problème :*** c'est une course de vitesse, il faut révéler les informations plus vite que ne le fait la presse pour rester maître de la communication. En annonçant ce qui se passe en son sein et en assumant ses responsabilités, l'entreprise peut couper l'herbe sous le pied de ses potentiels détracteurs.

• ***Le « block and bridge » :*** il s'agit de déplacer le débat sur un autre sujet pour attirer l'attention des médias sur un thème connexe mais décorrélé de l'entreprise en cause.

POUR EN SAVOIR PLUS

Libaert T., *Crises, de 10 à 150*, Observatoire International des crises, 2007.

Libaert T., *La communication de crise*, Dunod, 2005.

11

LE RISQUE SECTAIRE

« Les mouvements sectaires n'ont plus besoin d'adeptes pour faire de l'argent, le marché de la formation professionnelle peut suffire »

Un responsable d'une association anti-secte.

UN FLÉAU INSIDIEUX

Le marché de la formation est un marché en pleine expansion depuis de nombreuses années : séminaires de management, conférences sur la comptabilité (normes IFRS, négociation, techniques de vente…) autant de sujets qui alimentent les catalogues des organismes de formation ayant pignon sur rue. Et cette prolifération de l'offre correspond à une demande sans cesse croissante des collaborateurs : stages de développement personnel et de construction de soi se multiplient, avec l'assentiment des dirigeants d'entreprises qui y voient un moyen d'accroître l'efficacité et donc le rendement de leurs équipes.

Le marché de la formation est colossal : on estime à 22 milliards d'euros le montant des budgets consacrés à ce poste chaque année selon les statistiques du Ministère du Travail. Plus de 45 000 organismes prestataires ont été recensés, même si seuls quelques milliers sont connus du grand public. Dans cette offre pléthorique, les dérapages ne sont pas rares : certains escrocs profitent du faible nombre

de contrôles pour abuser le système, d'autres n'hésitent pas à mettre en œuvre des méthodes de formations douteuses voire carrément excentriques sous prétexte de développement personnel et de « rencontre de son moi intérieur ». Face à cette manne financière, les groupes et organisations sectaires ont vite compris l'intérêt qu'il y avait à tirer en pénétrant le monde des entreprises.

Dans ces actions d'infiltrations de sociétés par le biais de la formation professionnelle, les groupes sectaires voient de multiples avantages :

• ***Accaparer l'argent*** affecté aux budgets formation des entreprises. Chaque société ayant l'obligation d'affecter un pourcentage de sa masse salariale à la formation de ses collaborateurs, ces budgets captifs sont disponibles tous les ans, et les entreprises n'hésitent pas à les solder avant la fin de l'année, parfois en ayant recours des prestataires dont ils n'ont pas forcément vérifié ou contrôlé les références.

• ***Infiltrer*** de manière insidieuse les entreprises, soit pour recruter des « adeptes », soit pour infiltrer le réseau au sein duquel l'entreprise évolue. En étant référencé par une société, il est plus facile de proposer ses prestations aux autres entreprises du même secteur.

• ***Avoir accès*** aux informations détenues par l'entreprise : données personnelles sur les collaborateurs, informations liées à l'activité professionnelle, ou toutes autres données susceptibles d'intéresser la secte.

Les modes opératoires mis en œuvre par les groupes sectaires sont pour la plupart bien pensés : ils commencent par approcher leur cible en proposant des prestations de formation, le plus souvent axées sur le développement

personnel. Les modules ainsi proposés sont accompagnés de sommaires alléchants, bien pensés, et proposant de démultiplier le potentiel personnel des participants. Ces organismes sont bien sûr tous dotés d'un numéro d'agrément auprès du Ministère du Travail et proposent, dès la première rencontre, d'établir une convention de formation pour faire prendre en charge leurs prestations par les fonds spécialisés. Après plusieurs réalisations de modules tout à fait classiques et anodins, les méthodes utilisées par les formateurs commencent à évoluer vers des pratiques parfois étranges : ainsi, cet organisme dont les formateurs demandaient aux participants de s'imaginer dans la peau d'un animal et de mimer les actes de reproduction pour extérioriser leurs frustrations interpersonnelles (sic !). Les méthodes de formations utilisées par les groupes sectaires ont pour objectif d'isoler le collaborateur en le coupant de son environnement : cela peut se faire en dénonçant le système dans lequel il évolue ou en stigmatisant ceux des collaborateurs qui adhèrent à l'organisation mise en place dans l'entreprise. Dès que la victime semble déstabilisée, le « formateur » peut le formater à sa guise et selon le modèle qui lui permettra de l'attirer dans son organisation.

De tels agissements sont très déstabilisants, aussi bien pour les collaborateurs que pour l'entreprise elle-même. Au-delà de la captation des budgets de formation, les groupes sectaires ébranlent les entreprises en diffusant leurs doctrines.

Le phénomène n'est pourtant pas nouveau : l'infiltration du monde de l'entreprise par de soi-disant coachs, plus apparenté aux gourous et aux farfelus, intéresse depuis plusieurs années les associations de lutte contre les sectes.

Dès 2000, une circulaire du Ministère du Travail en abordait la problématique en évoquant « un moyen privilégié de pénétration du milieu de la formation par les organismes sectaires ».

En 2007, La Miviludes[1] publie un guide à destination des acteurs de la vie économique. Ce vade-mecum, intitulé « Les entreprises face au risque sectaire », cherche à donner aux responsables économiques et aux chefs d'entreprises les outils efficaces pour détecter et mesurer les risques d'intrusion de mouvements sectaires dans l'entreprise. Et cette prise de conscience touche aussi les chefs d'entreprise et les collaborateurs les plus avertis : de plus en plus de responsables formation, RH ou de délégués du personnel s'interrogent ou sollicitent la Miviludes au sujet d'organismes de formations aux méthodes étranges ou inquiétantes. C'est le début d'une prise de conscience d'une menace insidieuse et sournoise qui, patiente, s'en prend aux collaborateurs et aux personnels cherchant leur épanouissement personnel et professionnel.

UNE MÉTHODE BIEN ÉTRANGE

> Responsable de la Direction des Achats d'un grand groupe, Alain souhaite proposer à ses collaborateurs une formation au développement personnel. Depuis plusieurs mois, il ressent ce besoin de la part de ces collaborateurs et sa proposition soulève l'enthousiasme de sa responsable des ressources humaines. Sans tarder, elle établit un cahier des charges et contacte plusieurs organismes de formation. Quelques semaines plus tard, une société est choisie et une convention de formation signée pour commencer les formations à la rentrée.

1. Mission interministérielle de vigilance et de lutte contre les dérives sectaires.

Les premiers modules sont dispensés, et les retours des sessions sont plutôt bons, mêmes si peu de participants sont capables d'expliquer les méthodes pédagogiques utilisées. D'ailleurs, les formateurs demandent à ceux qui ont fait les premiers modules de ne pas révéler aux autres ce qui se passe durant la journée.

Les modules s'enchaînent, et Alain a du mal à voir les effets des séminaires : au lieu de constater un épanouissement de ses collaborateurs, il s'aperçoit que des clans se créent entre les services, et que certains membres du personnel n'hésitent pas à remettre ouvertement en cause le système d'avancement en œuvre dans l'entreprise. Plusieurs accrochages, à deux doigts de l'affrontement physique, lui ont été rapportés. Mettant ce phénomène sur le compte de la pression des objectifs et les difficultés du métier, Alain ne fait pas le rapprochement avec les modules de formation. Mais lors d'un entretien avec un membre de son comité de direction, tout va devenir plus clair : une partie des collaborateurs ayant participé aux séances de développement personnel se met à avoir une attitude agressive à l'encontre de l'entreprise, et leur comportement général change au point d'impacter l'efficacité de leur travail.

Alain décide faire le point avec sa DRH : celle-ci n'a rien remarqué de particulier, et défend au contraire le prestataire qu'elle a choisi en indiquant que les méthodes de développement personnel impliquent forcément une remise en cause des acquis des participants. Surpris de cette réponse, Alain sollicite un autre collaborateur pour avoir son avis. Celui-ci est édifiant : pour lui, les formateurs sont complètement « excentriques », il a du mal à faire le lien avec l'activité de l'entreprise ou un quelconque développement personnel, d'autant plus qu'ils n'hésitent pas à parler de « vie extraterrestre » devant guider la vie des managers. Au fil de ses discussions, Alain s'aperçoit que les modules de formation sont en fait un mélange de psychanalyse de bas étage et de management mal maîtrisé. De plus, les échanges suscités par les formateurs sont souvent orientés sur la sexualité des participants et sont organisées des séances de remises en cause publiques et d'autoflagellation. Ceux qui n'adhèrent pas au principe sont mis

> à l'écart. Les formateurs proposent même aux participants de continuer leur introspection en participant à des séances organisées en dehors des heures de bureau.
>
> Au vu des effets dévastateurs de la formation, Alain interrompt les sessions et convoque une réunion avec le responsable de l'organisme de formation et sa DRH. Au cours de cette rencontre, Alain s'aperçoit que sa DRH connait en fait très bien le formateur et qu'elle partage sans réserve les méthodes pratiquées. L'entretien tourne court, devant l'opposition conjointe des deux autres participants. Le contrat est dénoncé, et la DRH quittera l'entreprise quelques semaines plus tard d'un commun accord.

L'entreprise d'Alain a été abusée par une organisation sectaire. Sa DRH, embrigadée dans un groupe revendiquant une appartenance à une vie extraterrestre, a pris l'occasion de l'organisation de sessions de formation au développement personnel pour faire entrer la secte dans l'entreprise. Fort heureusement, l'action de déstabilisation a pu être arrêtée, mais les effets se sont fait sentir encore pendant de longs mois. Alain n'avait rien perçu de cette double vie chez sa collaboratrice.

ANTICIPER ET RÉDUIRE LE RISQUE SECTAIRE EN ENTREPRISE

La réduction du risque sectaire dans les entreprises passe avant tout par une bonne capacité à se renseigner en amont sur les organismes prestataires et par un contrôle continu des prestations réalisées.

La sensibilisation au phénomène

Il y a un déficit important de prise de conscience du risque sectaire dans les entreprises. La Miviludes a réalisé

une étude auprès de 200 chambres consulaires et entreprises de toutes tailles, qui montre que seuls quelques grands groupes avaient détecté les tentatives d'intrusion de groupes sectaires par le biais de la formation. Pour accélérer la prise en compte de cette menace nouvelle, l'ensemble des acteurs de l'entreprise devrait être impliqué dans la surveillance de ce phénomène : les dirigeants, les responsables de la fonction RH, les responsables de formation, les délégués du personnel, les représentants syndicaux, jusqu'aux collaborateurs participants directement aux actions de formation.

Poser les bonnes questions

Il est primordial, avant de choisir un organisme de formation, de poser les bonnes questions sur les méthodes pédagogiques appliquées. En matière de développement personnel, beaucoup de formateurs vous diront que « tout est possible ». Encore faut-il que cela se fasse dans les limites du raisonnable, et que les méthodes n'aient pas pour objectif de déstructurer les participants. Avant de signer une convention de formation, les donneurs d'ordre devraient demander des réponses écrites et explicites sur les points suivants :

- Quels sont les thèmes abordés par le prestataire de la formation ?
- Ses modules s'adressent-ils à tous les collaborateurs ou sont-ils réservés à une « élite » ?
- Les formateurs utilisent-ils un « jargon » qui leur est propre ?
- Entendent-ils imposer ce jargon aux participants ?

• La formation impacte-t-elle le temps de sommeil des participants ?

• La formation impacte-t-elle le mode alimentaire des participants ?

• Les réponses à ces quelques demandes peuvent générer d'autres interrogations permettant de démonter une entreprise sectaire par les méthodes pédagogiques qu'elle envisage.

Des organismes de formation référencés

Sur les 45 000 organismes de formation officiellement référencés auprès du Ministère du Travail, il n'est pas simple de faire le tri entre ceux qui sont de vrais professionnels du métier et ceux qui profitent de la formation pour pénétrer le monde des entreprises. Hormis ceux qui ont pignon sur rue, certains organismes sont complètement inconnus, voire même créés de toutes pièces du jour au lendemain pour répondre à un appel d'offres. La Miviludes, suite aux plaintes de sociétés abusées, a recensé un certain nombre de charlatans, d'escrocs ou de sectaires. Cependant, en vertu du respect des libertés fondamentales, la Miviludes ne peut à ce jour en publier la liste. Elle peut cependant être saisie par une entreprise qui s'interroge sur un organisme lui proposant ses services.

Les groupes sectaires ne se contentent pas de monter un seul organisme : bon nombre de sociétés de formation, qui n'ont officiellement aucun lien entre elles, sont en fait des sociétés gigognes ne servant parfois que de boîtes aux lettres. Dans le cadre de propositions de services, il est important d'exiger une liste de références ainsi que les

noms des responsables formations qui ont organisé les évènements afin de les contacter et de les interroger sur les méthodes pédagogiques appliquées et sur les résultats obtenus.

L'évaluation des actions de formation

Les groupes sectaires utilisent fréquemment des méthodes poussant à la déstabilisation mentale, qu'il est possible de détecter par les changements de comportement de la part des participants. Ces méthodes poussent également au prosélytisme, au rejet du système installé dans l'entreprise et à « l'agression » de ceux qui s'opposent à cette remise en cause. Des dispositifs de contrôle et d'évaluation des actions de formation peuvent permettre de mettre à jour des pratiques dangereuses pour l'intégrité physique et psychologique des participants.

Le signalement

En cas de pratiques douteuses ou manifestement dangereuses, les sociétés victimes ou abusées devraient signaler leur mésaventure à la Miviludes afin que les organismes en cause soient recensés et qu'il soit mis fin à leurs pratiques.

POUR EN SAVOIR PLUS

Miviludes, *L'entreprise face au risque sectaire*, Documentation Française, 2007.

« *Prévention du risque de prosélytisme sectaire* », CNDP, 2007.

PARTIE 4

LES MENACES D'ATTEINTES AUX BIENS

12

LA CONTREFAÇON

« Toute atteinte aux droits du breveté constitue une contrefaçon qui engage la responsabilité de son auteur »
Art. L615-1 du Code de la Propriété Intellectuelle.

LA CONTREFAÇON, FLÉAU DE L'ÉCONOMIE MONDIALE

Plus aucun produit n'est aujourd'hui à l'abri des contrefacteurs et des pilleurs d'idées. Longtemps réservée au monde du luxe, la contrefaçon s'attaque depuis quelques années à tout ce qui peut rapporter de l'argent à ces auteurs : cigarettes, stylos à bille, parfum, habillement, montres, jouets, pièces automobiles et aéronautiques… Mais si porter un faux foulard de marque ne peut blesser que l'ego, consommer un alcool contrefait ou une copie de médicament sans principe actif peut se révéler dangereux voire mortel. En 2004, au moins 13 bébés sont décédés en Chine après avoir été nourris avec du faux lait en poudre, ne contenant aucune protéine de lait.

Les 8 premiers pays d'origine des produits contrefaits saisis par les douanes européennes en 2006							
Chine	EAU	Inde	Algérie	Hong Kong	Égypte	Turquie	Iran
79 %	5 %	1 %	1 %	1 %	1 %	1 %	1 %

Part des biens contrefaits par secteur en pourcentage du chiffre d'affaire Source : OCDE							
Montre	Médicaments	Parfum	Pièces d'avion	Jouets	Musique	Vidéos	Logiciels
5 %	6 %	5 %	10 %	12 %	33 %	50 %	43 %

Définition

La contrefaçon consiste en la fabrication d'un produit, qui imite l'apparence du produit original, dans le but de faire croire au consommateur qu'il s'agit du produit d'origine. Les contrefaçons sont parfois de pales copies identifiables au premier coup d'œil, et ceux qui les achètent ne doutent en rien qu'il s'agit d'une fabrication copiée. Mais les contrefacteurs se montrent de plus en plus efficaces et de plus en plus rapides : on estime à 10 jours le délai nécessaire pour contrefaire un foulard de luxe, en réalisant une copie d'excellente qualité difficilement décelable pour un acheteur non averti.

Si les consommateurs sont les premiers abusés, la contrefaçon a également un impact de plus en plus important sur la vie économique et sur l'activité des entreprises. En faisant perdre des parts de marché aux producteurs, elle

entraîne la baisse de leurs chiffres d'affaires avec toutes les conséquences que cela implique : perte d'emploi, perte de compétitivité, perte de confiance des consommateurs.

Pour les seules entreprises françaises, une étude de l'OCDE[1] estime que la contrefaçon représente un manque à gagner annuel de 6 milliards d'euros, et la perte de 30 000 emplois tous les ans.

Des conséquences parfois très lourdes

• ***Pour les entreprises***

Au-delà des pertes de parts de marché, elle affecte l'image des produits originaux et du secteur au sens large. Les consommateurs sont par exemple très méfiants quant aux pièces automobiles qu'ils achètent pour leurs voitures, du fait de la présence d'une grande quantité de pièces contrefaites impactant directement la sécurité du conducteur et des occupants.

Les entreprises voient également leurs efforts de recherche et de développement menacés : tout le temps et l'argent consacrés à l'innovation et au perfectionnement de ses produits sert en fait aux contrefacteurs qui, en copiant le produit, bénéficient de recherches qu'ils n'ont pas financées.

Enfin, les mesures de lutte contre la contrefaçon coûtent chaque année plus cher aux entreprises qui tentent de s'en protéger.

• ***Pour les États***

Les pertes de parts de marché des entreprises nationales engendrent des pertes de revenu, et donc des pertes fiscales

1. Organisation de Coopération et de Développement Économiques.

pour l'État dont elles sont ressortissantes. De plus, les pertes d'emplois liées à la contrefaçon font grossir le nombre des chômeurs, indemnisés par les services sociaux.

• ***Pour les consommateurs***

Les produits contrefaits sont une tromperie grave sur la qualité. Ils peuvent être dangereux, comme dans le cas de jouets de mauvaise qualité ou de produits cosmétiques contenant des substances irritantes. Ils peuvent aussi être mortels quand il s'agit de pièces automobiles ou aéronautiques réalisées dans des alliages déficients et s'usant prématurément. De plus, en cas de réclamation ou de demande d'indemnisation, la société dont le produit a été contrefait ne peut procéder à la maintenance ou à la réparation.

La lutte contre ce nouveau fléau de l'économie repose sur des actions concertées impliquant à la fois les entreprises, les autorités étatiques et les associations de consommateurs pour démonter les filières de fabrication, d'importation et de distribution des contrefaçons.

COPIES PRESQUE CONFORMES

> La société X appartient à un groupe industriel international travaillant dans le secteur des automatismes complexes. Ayant emporté de gros appel d'offres en Asie et étant devenue une référence dans son secteur d'activité, la société X décide d'installer en Chine le site de production d'un automatisme bien spécifique, rentrant dans la construction d'un ensemble automatisé complexe de plus en plus demandé dans les pays d'Asie.
>
> Après plusieurs mois de préparation de l'implantation du site, les premiers coups de pioche sont donnés et l'usine de construction est livrée en temps et en heure. Les premiers expatriés commencent à arriver, amenant avec eux un certain nombre

d'informations confidentielles relatives aux processus de fabrication et aux alliages utilisés dans l'exécution de certaines pièces.

Les premiers ingénieurs expatriés arrivés sur place, outre la construction des chaînes de fabrication de l'automatisme, ont aussi la charge d'identifier des prestataires locaux pour leur confier des tâches non stratégiques du processus de fabrication. Alors qu'ils sont installés depuis près de trois semaines, ces ingénieurs ont la visite du dirigeant d'une entreprise locale qui souhaite leur proposer une collaboration. Quelle n'est pas la surprise des ingénieurs de voir le type de collaboration proposée : le chinois a en effet sorti de son cartable une pièce très complexe, élément fondamental de l'automatisme, et propose de les fournir à la société X pour la moitié du prix de revient habituel. Le problème, c'est que cette pièce est la copie exacte de celle produite par la société X, et pourtant aucun plan ni aucun exemplaire original n'est censé être à la disposition du public.

Remis de leur surprise, les ingénieurs demandent au chinois où il a pu trouver un exemplaire de cette pièce pour pouvoir la produire : celui-ci leur répond par un sourire, et propose de laisser sa pièce pour expertise. Après trois jours d'examen minutieux, la copie de la pièce originale est qualifiée de dangereuse car ne répondant pas aux normes de solidité et de résistance à l'usure pour ce type de mécanisme.

La mésaventure de la société X démontre que les contrefacteurs ont une vraie capacité à identifier très rapidement les produits à forte valeur ajoutée et à les copier dans les délais les plus brefs pour les mettre sur le marché. Dans les quelques mois qui ont suivi l'implantation de la société X en Chine, des centaines de pièces contrefaites ont inondé le marché et se sont retrouvées sur les chantiers ou dans les sociétés de maintenances travaillant dans le secteur.

Il est difficile d'identifier par quel moyen le contrefacteur chinois s'est procuré la pièce qu'il a proposée à la société X.

Mais au vu de la qualité et de la rapidité de réalisation, il ne peut s'agir que d'une copie faite par rapport à la pièce originale ou en suivant les plans techniques de fabrication. À ce jour, cette affaire n'a toujours pas été élucidée, et il y a fort à penser qu'elle ne le sera jamais. La société X a décidé depuis de protéger ces informations sensibles et s'est rapprochée des autorités chinoises en arguant des problèmes de sécurité liés à l'utilisation des pièces copiées au détriment des pièces originales.

Dans le secteur pharmaceutique, la société Johnson & Johnson Vision Care, une division du groupe Ethicon, a été victime dans récemment d'une contrefaçon de l'un de ces produits phare, les lentilles Surevue®. Bien qu'aucun problème de santé grave n'ait été rapporté suite à cette contrefaçon, la société Johnson & Johnson a été obligée de mettre en œuvre un plan de rappel impactant inévitablement son image auprès des consommateurs. Par chance, l'absence de deux pictogrammes sur les boîtes de copies a permis aux consommateurs et aux professionnels de les identifier assez rapidement pour les retirer du marché ou les ramener chez leur opticien.

Bien organisés, les contrefacteurs ont packagé leurs copies de lentilles dans des boîtes ressemblant à s'y méprendre aux boîtes originales de Surevue®, et ont réussi à les introduire dans le circuit de distribution. L'introduction de ces contrefactions a pu être identifiée à la suite de plusieurs signalements d'inconfort et de corrections inadaptées par des utilisateurs. Au-delà de ce désagrément, une mauvaise stérilisation de ces lentilles aurait pu entraîner des infections oculaires sérieuses chez les porteurs.

Pour faire face à cette crise de contrefaçon, Johnson&Johnson a réagi avec responsabilité et efficacité : en alertant l'Agence Française de Sécurité Sanitaire des Produits de Santé et en s'associant aux services publics, toutes les mesures ont été prises pour faire cesser la distribution des copies dangereuses.

LUTTER CONTRE LA CONTREFAÇON

La lutte contre la contrefaçon met en œuvre des moyens de prévention du risque de copie et de captation d'informations sensibles, et des moyens de lutte contre les contrefacteurs.

La prévention

La prévention consiste essentiellement à la protection intellectuelle et physique des produits potentiellement copiables.

• ***La protection de l'information stratégique :*** données liées à la recherche et développement, plans techniques, processus de fabrication, modèles originaux.

• ***La protection juridique de la marque :*** brevets, dépôt légal…

• ***La protection technique :*** apposition sur les produits de sceaux de sécurité, utilisation de l'holographie, d'encres spéciales, de papiers sécurisés, de marqueurs biométriques.

La lutte contre les contrefacteurs

Elle passe par l'identification des filières, que ce soit en utilisant les moyens internes pour les entreprises qui en ont

la capacité, et/ou avec les moyens étatiques dédiés à la lutte contre la contrefaçon.

• ***Les filières de fabrication :*** souvent implantées dans des pays en voie de développement, elles sont difficiles à remonter notamment quand elles recrutent dans les populations locales qui participent à leur protection.

• ***Les filières d'importation :*** les services douaniers peuvent apporter leur soutien dans l'identification des filières d'approvisionnement et dans la saisie des produits contrefaits.

• ***Les filières de distribution :*** développées grâce à des complicités au sein de la chaîne de distribution finale, elles peuvent être démontées grâce notamment aux associations de professionnels et à l'utilisation de moyens techniques.

Les initiatives privées

Les pays où sein desquels les détenteurs de marques contrefaites sont nombreux ont créé des associations de lutte contre la contrefaçon, dont les activités essentielles sont la protection de la propriété intellectuelle et des brevets, la collecte d'informations et la conduite de relations efficaces avec les instances officielles de répression.

Créé en France en avril 1995, le CNAC[1], qui fédère des entités publiques et des acteurs privés de la lutte contre la contrefaçon, est une « instance d'échange et de concertation entre acteurs concernés ». Sa présidence est toujours confiée à un député, et son secrétariat général assuré par l'INPI[2]. Sa création a été préconisée lors de la préparation

1. Comité National Anti Contrefaçon.
2. Institut National de la Propriété Industrielle.

de la loi du 5 février 1994, dite loi Longuet, contre la contrefaçon.

Les moyens étatiques

L'Organisation Mondiale des Douanes et Interpol ont adopté une stratégie préventive : elles utilisent désormais des bases de données recensant les produits de contrefaçon pour échanger rapidement des informations. Elles organisent également des formations à l'intention des entreprises pour les sensibiliser au risque.

La contrefaçon de marque constituant un délit douanier, les douanes sont le fer de lance de l'appareil d'état pour endiguer le phénomène. La législation française repose sur le code de la propriété intellectuelle, modifié de façon substantielle par la loi du 5 février 1994. Cette législation est mise en œuvre de façon complémentaire à la réglementation communautaire. Il est à noter que la loi du 5 février 1994 a étendu aux dessins et modèles, aux droits d'auteur et droits voisins, le dispositif de protection qui ne concernait auparavant que la marque.

Deux types de procédures peuvent être mis en œuvre par les douanes.

• ***La retenue***, lorsque les marchandises sont soupçonnées d'être une contrefaçon, et à la condition qu'une demande d'intervention spécifique ait été préalablement déposée auprès du service des douanes compétent.

• ***La saisie douanière***, lorsque la marchandise en cause est manifestement et objectivement un produit contrefait.

POUR EN SAVOIR PLUS

Baudart A., de Bouchony A., *La contrefaçon*, PUF, 2006.
Defer A., Lecou C., Schmitt J.-M., *Contrefaçon*, Economica, 1998.

13

LES VOLS ET DÉTOURNEMENTS DE PRODUITS

« 2 000 plaintes ont été enregistrées en 2005 pour vols de marchandises sur les routes, avec un préjudice de 360 millions d'euros »

Source : OCLCDI[1]

UN PILLAGE DE PLUS EN PLUS SOPHISTIQUÉ ET ORGANISÉ

Le vol et le détournement de marchandises ne sont pas de nouveautés : les voleurs de grands chemins n'ont pas attendu l'ère du numérique pour s'attaquer aux transports de fret et piller les cargaisons. Pourtant, depuis quelques années, le phénomène prend une telle ampleur que l'impact ressenti par les entreprises et les coûts générés incitent les pouvoirs publics à agir de façon plus organisée et plus radicale face à ce fléau.

Délaissant les braquages de banques, trop risqués pour des butins rarement supérieurs à 10 000 euros, les tenants du grand banditisme et du crime organisé se reconvertissent en pirates des aires d'autoroutes et des entrepôts. Des produits en grandes quantités, souvent à très forte valeur ajoutée, des mesures de sécurité sans communes mesures avec celles mises en œuvre dans le secteur bancaire, des

1. Office central de lutte contre la délinquance itinérante.

butins se comptant en centaines de milliers d'euros : tous les ingrédients pour faire du vol et du détournement de marchandises un business lucratif pour des acteurs malveillants.

Les vols de marchandises lors de transport terrestre restent la part la plus importante de ce pillage. À la fin de l'année 2007, un gang particulièrement bien organisé à fait main basse sur tout un stock de jeu vidéos pour consoles. Déguisés en policiers, ils ont intercepté un poids lourd peu après sa sortie d'un entrepôt de l'Essonne. Le conducteur, se pliant aux injonctions de ces faux fonctionnaires de police, descend de son véhicule et est aussitôt ligoté et séquestré dans son camion. Il est relâché près de cinq heures plus tard, son véhicule ayant été complètement vidé. Montant du butin : près d'un million d'euros.

Les pirates des routes ne se contentent pas des produits finis : les composants électroniques, les pièces détachées, les semi-conducteurs font maintenant partie des produits recherchés. Leur disparition impacte de plein fouet les entreprises qui les produisent mais également celles qui les attendent pour assurer leur production. Derniers butins en vogue : les matières premières. Cuivre, acier, zinc, aluminium deviennent des produits de choix depuis l'envolée des cours sur les marchés internationaux.

Les vols de stocks sont également en pleine expansion : attaquer un entrepôt au petit matin, en prenant en otage un à un les employés au fur et à mesure de leur arrivée sur leur lieu de travail est devenu un mode opératoire en vogue. Et les agresseurs sont de plus en plus organisés et de mieux en mieux informés, parfois par des complices en interne : ils connaissent les dates d'arrivée en stock,

l'importance des flux, la qualité des produits. Et les périodes de fêtes sont des moments privilégiés : beaucoup de marchandises sur place, généralement des produits de luxe, facile à écouler sur les marchés parallèles. Des stocks de foies gras, de spiritueux, de parfums, de téléviseurs à écran plat et de téléphones mobiles s'évaporent à l'approche des fêtes, générant des millions d'euros de perte.

Le vol de fret maritime se développe également : les détournements de containers et parfois même de cargaisons complètes se multiplient. Les vols se passent le plus souvent dans les ports, lors des phases de débarquement. Ils se déroulent aussi parfois en pleine mer, à l'occasion d'abordages dignes des meilleurs films de pirates. Des navires entiers sont détournés puis revendus, leurs cargaisons alimentant des marchés parallèles de plus en plus organisés. La Chine, la Malaisie, Les Philippines sont les principales zones d'écoulement de ces marchandises volées : de nombreux ports non surveillés, une corruption endémique, des circuits de distributions tenus par les mafias locales sont autant d'atouts pour ce commerce en pleine expansion.

Les pouvoirs publics se sont mobilisés depuis quelques années, mobilisation matérialisée par un rapport intitulé « *Fraude et délinquance dans les transports routiers de marchandises* ». Ce document, élaboré dans le cadre de la Conférence Européenne des Ministres des Transports, a été publié le 13 juin 2002. Ce document, et toute la politique qui en découle, incitent l'ensemble des acteurs à se concerter pour endiguer le phénomène :

Les transporteurs : Ils sont les mieux placés pour décider du niveau de protection approprié à mettre en œuvre sur

leurs véhicules. Ils peuvent adopter les outils techniques de réduction des vols, et sensibiliser leurs conducteurs aux risques encourus, que ce soit pour la prévention ou pour la gestion d'une agression.

• ***Les utilisateurs :*** les progrès dans les méthodes de conditionnement et dans la discrétion des colis sont de la responsabilité des donneurs d'ordre.

• ***Les assureurs :*** les compagnies d'assurance remplissent un rôle de conseil envers leurs assurés. Elles donnent des consignes de prévention et de précautions pour éviter la survenance des vols.

• ***Les pouvoirs publics :*** en assurant une meilleure disponibilité des moyens et une adéquation aux nouveaux modes opératoires, ils peuvent contribuer grandement à la répression du vol et du détournement de produits.

SOUSTRACTIONS FRAUDULEUSES

> Le journal Economic Daily News a révélé en 2006 un vol surprenant. La société Hynix, fabricant de semi-conducteur, a été victime d'un gros détournement de marchandises dans la région taïwanaise de Taoyuan. Une de ces cargaisons de puce DDR 400 MHz, acheminée à Taiwan par voie routière, a été détournée par un groupe d'agresseurs. Après avoir neutralisé le conducteur au moyen d'un pistolet électrique, les voleurs ont tout simplement disparu avec le véhicule. Montant du préjudice : 306 000 $, soit 20 colis contenant plusieurs milliers de puces, subtilisés en quelques minutes et revendus vraisemblablement sur le marché chinois.

Cette mésaventure survenue au groupe Hynix montre que la vulnérabilité des acheminements de produits se situe

au niveau du transport entre le producteur et le consommateur. En quelques minutes, plusieurs centaines de milliers de dollars ont disparus, et plusieurs constructeurs d'ordinateurs ont vu leur production impactée par le vol de ces composants indispensables à leur activité. D'après des sources proches de l'enquête, les malfaiteurs ont vraisemblablement bénéficié d'une complicité interne pour réaliser leur forfait.

Patrick travaille depuis plusieurs années pour un grand groupe de cosmétique européen. Il est installé sur la zone Europe de l'Est, et supervise la logistique et les approvisionnements. Les produits vendus sur ces marchés, généralement des produits en bouteille ou en boites de petites tailles, sont acheminés par voie terrestre ou par ferroutage.

Depuis plusieurs semaines, Patrick a un problème : une partie du fret acheminé disparaît entre l'entrepôt et le pays de destination. Plus de la moitié des cartons sont ouverts durant le transport, et une bonne partie des produits disparaît lors de presque toutes les expéditions. La police locale s'avère incapable d'enquêter sur les faits. Patrick essaie d'analyser le processus d'acheminement : les colis sont emballés dans un des sites de production de la société, puis placés en conteneurs et transportés par voie routière jusqu'au site de transbordement pour être placés sur des wagons. Ils arrivent ensuite en zone douanière dans leur pays de destination, puis les containers sont une nouvelles fois placés sur des camions pour être acheminés jusqu'au site de stockage avant l'envoi dans les points de vente. C'est à ce moment-là que la disparition régulière de cartons est constatée. Les montants des vols commencent à se montrer exorbitants, et le groupe souhaite mettre un coup d'arrêt à ces pratiques.

Sur les conseils du directeur de la sûreté corporate, Patrick a recours à une société d'investigation pour savoir où se trouve la vulnérabilité dans son dispositif. Chaque étape est étudiée, il

> s'avère que les ouvertures de cartons ne peuvent pas se produire durant le premier transport routier, qui est assuré par un transporteur consciencieux et mettant en œuvre des mesures de sûreté efficace. Le ferroutage est lui aussi sécurisé : les colis sont placés en container scellé, et descellé uniquement lors du second transbordement. Reste le dernier acheminement à partir de la zone douanière, qui semble être le moment le plus favorable au vol des produits. Mais après plusieurs filatures des véhicules, il s'avère que les conducteurs ne s'arrêtent pas dans des zones non prévues à l'avance, et que les remorques ne sont pas ouvertes. Pourtant, les produits continuent à disparaître. Il est donc décidé le recours à la technique : des balises GPS sont placées dans les plusieurs boîtes les plus grandes, et le chargement est suivi étape par étape. À la grande surprise de Patrick, certaines balises commencent à s'éloigner du reste des produits quand les cartons se trouvent… en zone douanière ! Alors que les produits sont placés sous douanes le temps des formalités administratives, soit plusieurs heures, des cartons sont ouverts et les cosmétiques dérobés par des criminels, certainement complices de douaniers malveillants. En suivant les produits dérobés, Patrick et les investigateurs ont pu alerter les forces de police, ce qui a permis une interpellation en flagrant délit. Plusieurs centaines de produits volés depuis plusieurs semaines ont été saisies, le cerveau de l'affaire étant le beau-frère d'un douanier local.

Les vols ou les détournements ne sont pas toujours le fait de criminels purs et durs. Devant le prix de certains produits, des représentants de l'autorité peuvent se laisser aller à ces pratiques pour arrondir leurs fins de mois. C'est monnaie courante dans certains ports ou dans certaines zones de fret à travers le monde. Quand cette « distribution » de produit est faite en connaissance de cause par le transporteur ou le fabricant, il s'agit de corruption. Quand cela se passe à leur insu, c'est du vol, réprimé par la loi qu'elle que soit la zone du monde où il se produise.

RÉDUIRE LE RISQUE DE VOL DE MARCHANDISES

La prévention du risque de vol et de détournement de marchandises nécessite l'implication de tous les acteurs et la mise en œuvre de mesures à la fois humaines et techniques.

La discrétion des emballages

Pour endiguer la menace et dissuader les voleurs, la discrétion quant aux colis et aux cargaisons est indispensable. Depuis peu, les fabricants de produits à forte valeur ajoutée masquent la nature de leurs produits en les transportant dans des emballages neutres ou en filmant le contenu de leurs palettes avec un revêtement plastique opaque. De nombreux voleurs agissant sur les aires d'autoroute commencent par découper les bâches des camions pour voir ce qu'ils contiennent : des emballages opaques rendent les produits à forte valeur ajoutée plus difficilement identifiables.

La discrétion s'entend aussi pour les programmes d'expédition : les pirates et autres détourneurs de marchandises sont souvent renseignés de l'intérieur. Des complices, manutentionnaires ou employés de zones de fret, identifient les cargaisons les plus intéressantes et les signalent aux agresseurs qui vont pouvoir s'en emparer dans les entrepôts ou lors des transports. Expédier sous un nom d'emprunt ou du moins en indiquant le moins possible la marque des produits transportés est un gage de sécurité.

Un cahier des charges pour les transporteurs

Les transporteurs sont les acteurs principaux de la protection des cargaisons. Depuis quelques années, ils

mettent en œuvre certaines mesures de prévention qu'il est possible, pour les donneurs d'ordre, d'exiger dans le cadre d'un cahier des charges sur la sûreté des marchandises. Parmi ces mesures, il est possible de recenser les suivantes :

• ***La formation des conducteurs***

Une bonne sensibilisation au problème du vol de fret et aux modes opératoires utilisés par les agresseurs permet d'adopter les bons comportements et d'éviter les erreurs les plus fréquentes.

• ***La sécurisation des véhicules***

Bâches plus épaisses ou anti-déchirure, alarme d'effraction, système de détection des changements brusques de température indiquant l'ouverture des portes du container, sont autant de mesures de prévention qui peuvent garantir l'intégrité du véhicule et dissuader les voleurs.

• ***Le stationnement en zone sécurisée***

Il existe désormais un réseau de parcs de stationnement sécurisés pour les poids lourds. Chaque site est évalué en fonction des mesures de sûreté appliquées : vidéo-surveillance, gardiennage, dispositifs d'alarme, proximité des services de police. Une brochure « Zones de stationnement pour camions en Europe » est mise à disposition des transporteurs par le CEMT pour permettre de préparer des itinéraires en anticipant les points de stationnement.

• ***Le géo-tracking***

Des balises GPS, à peine plus grosses qu'un paquet de cigarette, sont mises à disposition des sociétés de transport pour assurer un suivi des véhicules. Ces dispositifs peuvent aussi être placés dans des colis pour suivre leur déplacement et éventuellement leur détournement s'ils sont volés.

• ***La centralisation des informations***

Il est encore difficile de quantifier exactement l'ampleur des vols et détournement de biens. Les statistiques, selon les pays, ne se basent pas sur les mêmes critères, ce qui contribue à brouiller les pistes. Des réseaux d'échange d'information sont mis en œuvre, par des services comme Europol entre autres, pour partager les données et anticiper les évolutions du phénomène. Le croisement des bases de données permettra de démanteler des réseaux transnationaux qui passent facilement les frontières pour écouler le produit de leurs vols à travers l'Europe.

La coordination avec les pouvoirs publics

Particulièrement conscientes du problème des vols de fret, les autorités publiques travaillent à un cadre cohérent de sécurisation des transports maritimes et routiers. Les directives régulièrement adressées aux constructeurs ainsi qu'à l'ensemble des acteurs du secteur poussent chacun à collaborer dans le sens de la réduction du risque.

En mai 1997, une cellule interministérielle de lutte contre la délinquance itinérante a été créée pour travailler notamment sur les vols de fret. Transverse, elle regroupe des gendarmes, policiers, magistrats, fonctionnaires de l'administration fiscale et travaille à la fois à la répression des détournements de marchandises et également à la coordination des actions de prévention.

POUR EN SAVOIR PLUS

La sûreté dans le transport routier de marchandises, Ministère des Transports, 2002.

Fraude et délinquance dans les transports routiers de marchandises, OCDE, 2002.

Bertin-Mourot E., Lelieur F., Terroir E., *Terrorisme et piraterie : des menaces contemporaines à la sûreté des transports maritimes de marchandises*, L'Harmattan, 2005.

14

CONTAMINATION ET ALTÉRATION DE PRODUITS

« Aujourd'hui, une contamination de produit sur trois est d'origine malveillante ou criminelle »

Un consultant spécialisé

UNE NOUVELLE FORME DE MALVEILLANCE

La sécurité alimentaire et la sécurité des produits ont fait des progrès impressionnants depuis ces dernières années : contrôles des chaînes de fabrication, audits des sites d'approvisionnement, traçabilité des produits, visites des services vétérinaires, pression des associations de consommateurs, organismes de contrôles indépendants… Pourtant, le nombre de contaminations de produit n'a pas cessé de croître, générant une méfiance grandissante de la part des consommateurs et des utilisateurs finaux.

La contamination accidentelle a toujours existé et a toujours été intégrée dans le processus de prévention des risques des fabricants et des distributeurs. Mais un phénomène nouveau est apparu depuis ces dernières années, suscitant incompréhensions et inquiétudes chez les professionnels : la contamination malveillante, également appelée MPT (*Malicious Product Tampering*). Ces actions, généralement réalisées dans l'objectif d'obtenir une contrepartie, touchent principalement les produits alimentaires et

les produits de grande distribution touchant potentiellement des publics « sensibles » : enfants, malades, personnes âgées…

Cas de contaminations malveillantes de produits (cas relatés dans la presse)			
Année	**Produits concernés**	**Type de contaminant**	**Motivation**
1977	Agrumes en provenance d'Israël	Mercure injecté avec une seringue	Politique
1984	Salades d'une chaîne de restaurant américaine	Salmonella Typhimurium	Politique
1989	Raisins d'origine chilienne	Cyanure	Politique
1996	Pâtisserie d'un restaurant d'entreprise américain	Shigella Dysenteriae	Malveillance
1996	Aliments – Groupe agroalimentaire de RFA	Venin de serpent	Criminelle
2004	Produits cosmétiques – Groupes européens	Divers	Criminelle
2007	Alimentation à emporter – Stations services UK	Alcool à brûler	Criminelle

Ces crises de contamination, de plus en plus nombreuses, sont particulièrement déstabilisantes pour les entreprises qui les subissent, soit en tant que victimes principales

(producteur, distributeur), soit en tant qu'utilisatrices des produits altérés.

Ces situations imposent des contraintes particulières.

• Elles suscitent un intérêt important et instantané de la part des médias et des journalistes.

• Elles impactent directement l'image de l'entreprise et porte atteinte à sa réputation de façon durable.

• Elles peuvent se révéler dangereuses pour la santé, voir mortelles dans certaines circonstances.

• Les coûts engendrés par de telles crises, quand elles sont avérées, sont colossaux : communication de crise, plan de rappel, plan de retrait, indemnisations des victimes éventuelles…

Les produits les plus fréquemment ciblés par les auteurs de contamination malveillante sont les produits alimentaires et les produits pharmaceutiques ou cosmétiques. En effet, le fait qu'ils soient ingérés ou appliqués sur la peau ou dans les yeux rend la menace de leur utilisation beaucoup plus crédible et beaucoup plus impressionnante. Mais ces produits ne sont plus les seuls à pouvoir être altérés de façon malveillante : récemment, des pirates informatiques ont introduit dans des disques durs amovibles un virus infestant le système informatique de leurs utilisateurs. Après expertise, les ingénieurs de la société fabriquant ces disques durs se sont aperçu que la contamination, en l'occurrence technique, avait eu lieu au sein même du site de fabrication du fait de complicités internes. Les pirates ont demandé le paiement d'une somme d'argent pour mettre fin à leur action destructrice. Ils ont fort heureuse-

ment été interpellés par la police au moment de la remise des fonds. Cette affaire a démontré que les agresseurs ne s'arrêtaient plus à l'altération de produits alimentaires, et que les moyens de contamination pouvaient également être physiques et informatiques.

Les motivations des auteurs de contamination malveillantes sont diverses.

• ***Politique :*** ce fut le cas en 1977 dans le cadre d'une contamination d'agrumes originaires d'Israël. Du Mercure avait été injecté au moyen d'une seringue pour nuire aux exportations israéliennes.

• ***Pathologique :*** un déséquilibré avait entrepris de verser du sucre en poudre dans les bidons d'huile vendus par une chaîne de stations services.

• ***Passionnelle :*** pour se venger de son contremaître qui l'avait éconduite, une employée d'une société de systèmes électroniques a altéré une partie de la production, après les phases de test, pour faire accuser son ancien amant. Ce sont les retours clients et une investigation spécifique qui ont pu permettre son identification.

• ***Criminelle :*** c'est de loin la principale cause de contamination malveillante. C'est le cas notamment de la contamination de sandwichs dans une chaîne de stations-service : les auteurs ont demandé le paiement d'une rançon pour cesser leur contamination.

LA CONTAMINATION COMME ARME DE TERREUR

> Les défenseurs de la cause des animaux ne sont pas tous des personnes pacifiques, se contentant de manifester dans les rues pour exprimer leur opinion. Les services de lutte anti-terroriste

français ont été alertés par leurs collègues britanniques sur le fait que des activistes français appartenant à l'ALF, l'Animal Liberation Front, organisation classée comme « éco-terroriste » en Grande Bretagne, étaient sur le point de commettre une contamination malveillante pouvant porter atteinte à la santé publique. Ces activistes ont revendiqué, sur le site du magazine du mouvement Bite Back, la contamination, avec de l'eau oxygénée de produits pour lentilles de contact vendus dans l'Hexagone. Selon leur message, ces éco-terroristes cherchaient « à faire subir aux humains les souffrances endurées par les animaux lors d'expérimentations menées par les laboratoires ». Dans ce même communiqué, des « militants pour les droits des animaux » ont affirmé que des flacons de solution pour lentilles avaient été contaminés dans tous le pays avec du peroxyde d'hydrogène, injecté au moyen de seringues dans les flacons mis en vente chez un certain nombre d'opticiens.

Ils ont choisi, pour réaliser leurs actions, quatre chaînes de magasins d'optique. La contamination n'était en fait pas dirigée directement contre le fabriquant de solution ni les distributeurs, mais contre le groupe Huntingdon Life Sciences, société anglaise pratiquant des expérimentations sur les animaux et travaillant avec le laboratoire à l'origine de la solution ophtalmologique.

Alerté par les services de police, le fabricant de la solution pour lentilles de vue a pris contact avec les quatre chaînes d'opticiens distributrices pour rappeler les produits susceptibles d'avoir reçu une injection d'eau oxygénée.

Mis à part un opticien ayant signalé qu'une de ces clientes avait ramené son produit parce qu'elle avait été irritée en le mettant dans ses yeux, aucun cas de contamination n'a été avéré. Les analyses pratiquées par le laboratoire de police scientifique n'ont pas révélé la présence de peroxyde d'oxygène dans les flacons incriminés.

Dans cette affaire, la société fabricant le produit s'est trouvée face à une menace de contamination sérieuse :

– le produit visé est un produit de santé publique, acheté sans ordonnance ;

– il est directement introduit dans les yeux des utilisateurs ;

– la menace porte sur quatre grandes chaînes de distribution, dispersées à travers tout le pays ;

– le produit contaminant n'est pas mortel mais très irritant, de nature à causer une altération sérieuse et des conjonctivites aux utilisateurs ;

– l'ALF, revendiquant l'acte de contamination, est connue pour ses passages à l'acte qui en restent rarement au stade de la menace.

Face à un tel risque, même si aucune contamination n'a été avérée, la société fabricante a décidé de mettre en œuvre un plan de rappel en accord avec l'Agence française de sécurité sanitaire des produits de santé en demandant à ces clients de ramener leurs produits pour remplacement.

> Une chaîne de stations services anglo-saxonne s'est trouvée confrontée à une telle situation : de nombreux clients ont eu la surprise de découvrir, en ouvrant les sandwichs achetés dans ces stations, une forte odeur d'alcool à brûler extrêmement désagréable. Devant le nombre croissant de retour de clients mécontents, la direction de la chaîne a décidé de lancer une investigation sur le problème. Rapidement, une contamination malveillante a été mise à jour : de l'alcool à brûler avait été injecté, au moyen d'une seringue, entre les tranches des sandwichs. La société étant assurée contre ce type de risque, une équipe de consultants dédiés est activée pour prêter main-forte dans la gestion de la crise. Très vite, l'origine criminelle de la contamination est avérée : un email parvient au siège de la société pour revendiquer l'action et demander le paiement d'une rançon pour y mettre fin.

La revendication s'avère sérieuse : les auteurs indiquent avec précision l'endroit où ils percent les sachets de sandwichs, à savoir exactement entre les deux mêmes lettres imprimées sur l'emballage de tous les paquets. Cette attitude, très professionnelle, montre la volonté des auteurs d'être clairement identifiés comme tels et de montrer leur sérieux. Après plusieurs échanges d'emails, le montant d'une somme d'argent est fixé et les conditions de la remise sont négociées. Sur les conseils des consultants, la police locale est informée et prépare une souricière Alors que les criminels se présentent sur les lieux de remise de la rançon, ils sont interpellés. Il s'avérera au fil de l'enquête que l'instigateur de cette contamination avérée était un employé de la société de station-service. Récemment licencié pour avoir volé dans la caisse, cet employé indélicat avait monté toute l'affaire pour se venger de ses anciens employeurs et pour leur soutirer de l'argent.

Cette seconde affaire de contamination démontre qu'il est facile de monter une telle action, et qu'avec une complicité interne, les auteurs peuvent ébranler leur cible, surtout quand l'altération touche des denrées alimentaires. Dans le cas de cette chaîne de stations services, le fait d'avoir été assurée et conseillée par des spécialistes a certainement contribué à la résolution efficace et rapide de l'affaire.

RÉDUIRE LE RISQUE DE CONTAMINATION ET D'ALTÉRATION MALVEILLANTE

Bien qu'elle soit nouvelle, la menace de contamination malveillante ou d'altération de produit peut se prévenir en s'appuyant sur les moyens mis en œuvre dans le cadre de la politique de sûreté des sites et de la politique qualité.

Le contrôle des accès

Dans le cadre de sa politique générale de sûreté, les entreprises mettent en œuvre des réglementations d'accès pour protéger leurs locaux et leurs sites. Les degrés de restriction et d'interdiction d'accès changent selon les métiers et les produits fabriqués, mais les zones à sécuriser pour réduire le risque de contamination malveillante sont :

• ***Les zones de fabrication :*** c'est généralement le lieu des contaminations appuyées par des complicités internes. La contamination de disques durs externes par un virus, récemment mise à jour par les services spécialisés, avait été effectuée au moment de la fabrication par un complice employé par le fabricant.

• ***Les zones de stockage :*** regroupant un grand nombre de produit dans un même lieu, elles sont un endroit propice à l'altération de masse.

Le contrôle de la chaîne de fabrication

L'ensemble des tests et contrôles-qualité intègre désormais la recherche des altérations, y compris malveillantes. Cependant, une bonne connaissance de la problématique et des modes opératoires utilisés par les agresseurs, selon les secteurs d'activité ou les types de produits, peut permettre une mise à jour régulière des moyens de contrôle.

La traçabilité des produits

Les dernières crises sanitaires, comme l'ESB, ont mis en avant la nécessité d'avoir un dispositif de traçabilité efficace. Etre capable d'identifier rapidement des produits

altérés et en gardant la possibilité de les rappeler de manière ciblée selon le lieu où ils se trouvent est aujourd'hui une obligation pour les entreprises concernées.

La collaboration entre les parties prenantes

Corollaire de la traçabilité, la collaboration entre les producteurs, les distributeurs et les autorités publiques permet de pouvoir réagir rapidement en cas de menace ou de contamination avérée. En connaissant les contraintes et les possibilités mutuelles, chaque partie prenante peut apporter aux autres ses compétences pour gérer ces situations non-conventionnelles.

Le plan de gestion de crise

En matière de gestion des crises de contamination, le plan repose sur trois volets :

• ***Le plan de retrait :*** c'est le dispositif qui va permettre de retirer les produits avant qu'ils ne soient mis à la disposition des utilisateurs. À ce stade, les produits sont encore dans les stocks du fabricant, du distributeur ou dans la chaîne logistique.

• ***Le plan de rappel :*** c'est le plan mis en œuvre quand les produits sont à la disposition des consommateurs. À ce stade, le plan de rappel implique une communication extérieure, souvent par voie de presse, pour demander aux utilisateurs de ramener les produits.

• ***Le plan de communication de crise :*** au vu de l'impact qu'une telle situation peut avoir sur l'image de la société, un plan de communication de crise est indispensable pour s'adresser efficacement aux médias et au public.

Les assurances

Il existe des polices d'assurances appelées MPT, *Malicious Product Tampering*, qui couvre les entreprises contre ce type de risque et qui prennent en charge l'intégralité des coûts engagés : retrait, rappel, coût de consultants, etc.

POUR EN SAVOIR PLUS

Capp G., *La sécurité sanitaire des aliments*, CES, 2001.
Lahellec C., *Risques et crise alimentaires*, Tec et Doc, 2005.

PARTIE 5

LES MENACES D'ATTEINTES AUX PERSONNES

15

LE TERRORISME

« Les actes de terrorisme ne peuvent jamais se justifier, quelle que soit la raison que l'on puisse faire valoir »

Kofi Annan

LES ENTREPRISES, NOUVELLES CIBLES DES ACTIONS TERRORISTES

Le terrorisme a toujours été difficile à définir, selon le côté duquel on se place : pour ceux qui le pratiquent, il est le moyen d'attirer l'attention sur leur cause ; pour ceux qui le subissent, il est une agression aveugle et une marque de lâcheté. Le terrorisme est généralement défini comme la menace de réalisation ou la réalisation, par une personne, un groupe ou un État, d'actions violentes destinées à produire sur leur cible un sentiment de terreur. Les attentats du 11 Septembre 2001, retransmis en temps réel sur toutes les télévisions du monde, et l'effondrement du World Trade Center en plein cœur de New York, ont définitivement changé la perception de tout un chacun quant à la détermination et à l'impact que peuvent avoir les terroristes aujourd'hui.

Nombres d'attentats terroristes par pays de 2000 à 2006 *Source : MIPT Terrorism Knowledge base*			
Irak	11 611	**Thaïlande**	305
USA	2 990	**Angola**	257
Colombie	1 177	**Sri Lanka**	251
Russie	945	**Espagne**	241
Inde	899	**Bangladesh**	189
Pakistan	855	**Turquie**	169
Afghanistan	790	**Népal**	156
Israël	728	**Algérie**	133
Bande Gaza	486	**Arabie Saoudite**	119
Philippines	485	**Égypte**	112
Indonésie	465	**Jordanie**	73
Uganda	450	**Yémen**	71

La violence aveugle a toujours été une stratégie des terroristes, mais de nouvelles cibles ont été désormais identifiées : les entreprises privées. Se développant dans des zones où se pratiquent attentats et attaques suicides, qu'elles soient de grands groupes internationaux ou des PME évoluant dans le sillage de ces grands groupes, les entreprises sont aujourd'hui clairement identifiées par les groupes terroristes comme des cibles principales. En mena-

çant les intérêts économiques et les sociétés qui y contribuent, les terroristes ont décidé de s'attaquer à l'activité économique des pays dans lesquels ils se trouvent en dissuadant les étrangers de venir y investir ou y développer leurs activités. L'affaire des caricatures de Mahomet a d'ailleurs montré cette nouvelle stratégie : Le chef de « l'État islamique d'Irak », Abou Omar Al-Baghdadi, autoproclamé par la branche irakienne d'Al-Qaïda, a lancé sur Internet un appel au meurtre de Lars Vilks et Ulf Johansson, respectivement dessinateur et journaliste suédois. Mais cette « fatwa » n'a pas suffi, car Abou Omar Al-Baghdadi a exigé des excuses des « croisés » suédois sous peine de s'en prendre aux grandes entreprises qu'il a clairement désignées : Ericsson, Scania, Volvo, IKEA et Electrolux.

Plusieurs actes ont confirmé cette nouvelle stratégie des groupes terroristes : le double attentat d'Istanbul, le 20 novembre 2003 en est une tragique démonstration. Les intérêts britanniques étaient visés, et les terroristes ont pris pour cible le consulat de Grande Bretagne d'une part, mais également les bureaux de la banque anglaise HSBC. Ce choix dans les objectifs n'a pas été anodin, et la désignation d'une cible économique, en l'occurrence une grande banque internationale, a ébranlé les entreprises agissant dans des zones à risque terroriste. Bilan : 27 morts, 449 blessés dont 30 dans un état critique.

Le terrorisme, et son impact sur les activités des entreprises privées, a mis à jour plusieurs menaces indirectes particulières.

• ***La première*** est le coût global des attentats : les pays de l'OCDE (Organisation de coopération et de développe-

ment économique) estiment le coût total moyen des attentats terroristes entre 42 et 210 milliards d'euros, en considérant les coûts humains, matériels et également les pertes d'activités liées.

• ***La seconde menace*** indirecte pèse sur l'assurance des entreprises. Après les attentats du 11 Septembre, les assureurs et les réassureurs ont réduit la couverture pour le risque lié au terrorisme, ou ont même cessé de le prendre en charge en raison des difficultés pour le tarifer. Les primes d'assurance ont largement augmenté dans plusieurs secteurs, surtout l'aviation et les autres modes de transport. Il y a eu également des hausses dans les domaines de la construction, de l'énergie et du tourisme. Les primes d'assurance pour les biens commerciaux et la responsabilité civile ont grimpé de 30 % en moyenne, et bien davantage pour les cibles les plus vulnérables comme les usines chimiques et les immeubles de grande hauteur à usage de bureaux.

• ***La troisième menace*** indirecte sur les entreprises est la responsabilité pénale induite par les actes terroristes. Cet aspect du risque terroriste sera développé plus bas dans l'étude de cas.

ATTENTAT AU PAKISTAN

> 8 mai 2002, la journée commence à Karachi, ville portuaire située au sud du Pakistan. Comme tous les jours, un certain nombre d'expatriés français attendent dans le hall de l'hôtel Sheraton que leur bus vienne les chercher pour les amener sur leur site de travail. Ce sont des employés de la DCN, Direction des Constructions Navales, qui travaillent au profit de la marine

> pakistanaise dans le cadre d'un contrat de modernisation des sous-marins de celle-ci.
>
> Le bus attendu vient de se garer devant l'hôtel, et les expatriés grimpent à l'intérieur comme ils ont l'habitude de la faire depuis le début de leur séjour. Ce véhicule de la marine pakistanaise doit les conduire à l'arsenal de la ville, lieu où ils assurent leur mission d'assistance technique pour la construction d'un sous-marin. Alors que tous les occupants du bus ne sont pas encore assis, un véhicule civil conduit par un kamikaze se gare contre le flanc gauche du bus ; avant que qui que ce soit n'ait le temps de réagir, le kamikaze actionne sa charge : l'explosion détruit l'autobus. Quatorze personnes vont perdre la vie dans cet attentant, dont onze expatriés français. Douze autres expatriés sont blessés… À Cherbourg, vile dont sont originaires la plupart des victimes, c'est la stupéfaction.

Cet acte terroriste, au-delà du fait qu'il cible une entreprise du fait de sa collaboration avec un état contre lequel agissent les terroristes, a mis en avant la notion de responsabilité de l'entreprise vis-à-vis de ces collaborateurs victimes d'un attentat terroriste. Après une plainte déposée par les familles des victimes de l'attentat de Karachi contre la DCN, le Tribunal des Affaires de Sécurité Sociale de la Manche rend une décision qui va faire jurisprudence et modifier lourdement l'impact du terrorisme sur les entreprises. Le TASS a en effet jugé que l'attentat, présentant tous les caractères d'un accident du travail, n'a été rendu possible que par la faute inexcusable commise par l'employeur, à savoir la DCN, qui n'avait pas pris les mesures propres à assurer la sécurité de ses salariés.

Le tribunal s'est en fait appuyé sur un certain nombre de faits indiquant que la DCN avait conscience de la montée de la menace terroriste au Pakistan. Trois notes notam-

ment, rédigées par le responsable de la DCN à Karachi, ont participé à motiver la décision de justice. La première, en date du 4 février 2002, s'inquiète de la découverte, à Islamabad, d'une bombe sous la voiture d'un diplomate français. La seconde, rédigée le 27 avril 2002, résume une réunion sur la sécurité au consulat général de France, évoquant en particulier le retour au Pakistan de nombreux talibans d'Afghanistan et le départ de nombreux expatriés américains, canadiens et britanniques. Enfin, le 2 mai, c'est-à-dire six jours avant l'attentat, le troisième document recommande aux expatriés une grande vigilance lors de leurs déplacements personnels.

La problématique de la responsabilité pénale de l'entreprise et de ces dirigeants est au centre de la prise en compte du risque terroriste. S'appuyant sur la jurisprudence DCN-Karachi, elle peut être mise en jeu lorsqu'une imprudence, une négligence ou le manquement à une obligation de sécurité ou de prudence imposée par un texte se trouve à l'origine d'un accident du travail ayant entraîné la mort ou une atteinte à l'intégrité de la personne du salarié (art. 221-6, 222-19 ou 222-20 du Code pénal). Pour ces délits non intentionnels, la loi n° 2000-647 du 10 juillet 2000 a introduit dans le Code pénal la notion d'auteur indirect, c'est-à-dire la ou les personnes physiques qui ont créé ou contribué à créer la situation ayant permis la réalisation du dommage, de même que celles qui n'ont pas pris les mesures permettant de l'éviter. L'auteur indirect n'est pénalement responsable que s'il a commis une faute caractérisée exposant autrui à un risque particulièrement grave qu'il ne pouvait ignorer (art. 121-3 du Code pénal). Autrement dit, pour que la responsabilité pénale de l'auteur indirect soit

retenue, il faut qu'il ait commis une faute particulièrement grave. On rejoint ici la notion de faute inexcusable décrite plus haut en ce qui concerne la réparation, sur le plan civil, du préjudice subi par la victime d'un accident du travail.

RÉDUIRE LE RISQUE TERRORISTE

Il existe de nombreux moyens de réaliser des actes terroristes, c'est-à-dire susceptible de produire un sentiment de terreur sur leurs cibles directes ou indirectes. Les actes terroristes les plus fréquents sont les attentats et les prises d'otages.

• ***Les attentats :*** les plus répandus sont les attentats à l'explosif. Le nombre de voitures piégées explosant au passage d'un véhicule ou d'une personnalité est en constante augmentation (Irak, Liban, Afghanistan). Ces dernières années, la multiplication des actes suicides réalisés par des kamikazes bardés d'explosifs a changé la perception des attentats et de leurs modes opératoires.

• ***Les prises d'otages :*** ces actes, comme la prise d'otage de l'ambassade du Japon au Pérou par le groupe terroriste Tupak Amaru, consistent à retenir un certain nombre de personnes dans un lieu déterminé, généralement entouré par les forces de l'ordre, pour exercer une pression ou réaliser une revendication.

La difficulté principale de la réduction du risque terroriste est la multiplicité des auteurs potentiels et la diversité des modes opératoires. Il existe cependant des politiques de prévention efficaces pour faire en sorte de minimiser l'exposition de l'entreprise à la menace terroriste, préparer

les personnels évoluant à l'international et réduire le risque de responsabilité pénale pesant sur les dirigeants.

La veille-pays

C'est la première étape incontournable d'une politique de prévention du risque terroriste. Cette veille permet de rester informer, au plus près du temps réel, de l'actualité sécuritaire d'un pays ou d'une zone particulière pour soit sensibiliser les expatriés ou voyageurs sur place, soit ordonner des mesures de sûreté appropriées aux évolutions de la situation locale.

La veille-pays peut être réalisée par l'entreprise en interne, en s'appuyant notamment sur les fiches d'information aux voyageurs réalisées par le Ministère des Affaires Etrangères[1]. Certaines compagnies d'assurance fournissent également des informations sur la situation sécuritaires d'une liste prédéfinie de pays.

La veille-pays peut également être externalisée vers des prestataires. Ces sociétés[2], se basant sur les flux d'informations d'actualités et également sur leurs implantations locales autour du monde, fournissent des analyses beaucoup plus précises et adaptées au monde de l'entreprise que les sites d'information institutionnels.

Les autorités diplomatiques françaises

Générer et maintenir un contact avec les autorités diplomatiques françaises est important. Cela permet d'avoir

1. www.diplomatie.gouv.fr
2. www.geostravelsecurity.com

accès à une information de qualité, et de bénéficier des conseils et consignes généralement dispensées par les postes diplomatiques. Il est donc recommandé de s'identifier et de s'enregistrer auprès de l'ambassade ou du consulat compétent sur la zone d'activité de l'entreprise.

Les ambassades de France à l'étranger disposent d'un Attaché de Sécurité Intérieure et d'un Attaché de Défense. Généralement représentants des ministères de l'Intérieur et de la Défense, ils disposent des réseaux locaux leur permettant de fournir des informations de prévention efficaces et d'actualité.

Les dispositifs de sûreté sur les sites

Des mesures techniques adaptées permettent de sécuriser des sites ou des bâtiments : l'adjonction de bornes anti-véhicules piégés, le positionnement de gardiens bien formés, la mise en œuvre de détecteur de létaux ou de produits explosifs peut dissuader bon nombre de terroristes potentiels.

La mise en disposition de Security Managers

Le Security Manager, généralement employé par une société de sûreté spécialisée, est mis a disposition de l'entreprise pour remplir les fonctions de responsable de la sûreté, et ce de façon temporaire sur des projets ponctuels ou particulièrement à risque, ou de manière définitive sur des implantations de longue durée.

Le Security Manager prend à sa charge l'ensemble des actions de sécurisation ; rédaction d'une politique de sûreté, accueil des expatriés et des voyageurs, sensibilisation

aux risques, sécurisation des déplacements et des convois, etc.

La formation des personnels

Dernier volet d'une politique de réduction du risque terroriste, la formation des personnels évoluant dans un environnement à risque est indispensable : modes opératoires des terroristes, lieu généralement visés, évènements festifs ou religieux à éviter, conduite à tenir en cas d'explosion, autant de conseils que l'on ne souhaite ne jamais devoir mettre en œuvre mais qui s'avèrent vitaux en cas de menace ou de réalisation d'un acte terroriste.

POUR EN SAVOIR PLUS

Blin A., Chalian G., *Histoire du terrorisme, de l'Antiquité à Al Qaida*,, Bayard, 2004.

Baud J., *Encyclopédie des terrorismes et violences politiques*, Editions Lavauzelles, 2003.

Géré F., *Les volontaires de la mort*, Bayard, 2003.

Courmont B., Ribnikar D., *Les guerres asymétriques. Conflits d'hier et d'aujourd'hui, terrorisme et nouvelles menaces,*, PUF, 2002.

16

LE KIDNAPPING

« Le nombre de kidnappings recensés
a plus que doublé depuis la dernière décennie »
Niel Hodge, consultant.

LE KIDNAPPING, UN BUSINESS EN PLEINE EXPANSION

On a longtemps cru que le risque de kidnapping et d'enlèvement politique ne planait que sur les journalistes de guerre évoluant en zone hostile, comme l'Afghanistan ou l'Irak, ou sur quelques touristes en mal de sensations fortes et sortant des sentiers balisés d'excursion au Yémen ou en Colombie. Il n'en est rien : le business du kidnapping n'a jamais été aussi florissant qu'aujourd'hui, et les statistiques, bien que grevées d'un chiffre noir impressionnant, ne laissent rien augurer de bon pour les prochaines décennies.

Le palmarès du kidnapping dans le monde (source UPNC[a])			
Amérique du Sud	**Asie Moyen-Orient**	**Afrique**	**Europe**
Colombie	Irak	Nigeria	Pologne
Brésil	Chine	Afrique du Sud	Rep Tchèque
Mexique	Russie	Algérie	Roumanie
Venezuela	Inde	Congo	Italie

a. Union Professionnelle des Négociateurs de Crise.

Les entreprises et les organisations, dans le cadre du développement de leurs activités à l'international, sont devenues des cibles privilégiées des kidnappeurs. Les cibles des agresseurs peuvent être des cadres expatriés ou des voyageurs d'affaires en déplacement. On constate aussi une augmentation du nombre de kidnappings d'employés locaux, enlevés dans leur pays, pour la seule raison qu'ils travaillent pour une entreprise internationale susceptible de pouvoir payer une rançon.

Cette nouvelle donne repose sur trois constatations :

• ***Les pays à risque*** sont soit des zones riches en matières premières (gaz, pétrole, minerai) avec une croissance économique importante et donc des opportunités de business réelles, soit des régions en plein développement manifestant d'importants besoins de construction d'infrastructures et de structures commerciales et économiques.

• ***Le risque de kidnapping*** est souvent mal apprécié par les expatriés et les voyageurs, qui ont tendance à méconnaî-

tre les risques spécifiques d'une zone et les modes opératoires pratiqués par les agresseurs potentiels.

• *L'organisation d'un kidnapping* est plus facile et moins risquée que le trafic d'armes ou de drogue. Une étude réalisée par la société Clayton Consultants, spécialisée dans la prévention des enlèvements, montre que 95 % des tentatives de kidnapping se soldent par une réussite.

Il existe plusieurs types de kidnappings, avec des modes opératoires différents selon les zones où ils se produisent, mais il est possible de les regrouper sous quatre catégories : le K4R, le *tiger kidnap*, l'enlèvement express et le kidnapping virtuel.

Le kidnapping avec demande de rançon

Appelé également *K4R* (*kidnap for ransom*), c'est un enlèvement destiné à obtenir le paiement d'une rançon, le plus souvent financière, en échange de la libération de l'otage. Il peut s'agir d'un enlèvement faisant suite à une « pêche miraculeuse », comme par exemple un barrage sur une route par un groupe de faux policiers, qui remontent ensuite la file de voitures bloquées pour choisir parmi les occupants ceux qu'ils vont emmener. Ce mode opératoire est répandu en Afrique sub-saharienne ou en Amérique latine. Il peut également s'agir d'un kidnapping d'opportunité, profitant de la présence d'un expatrié ou d'un voyageur dans un endroit propice à son enlèvement. Il peut enfin s'agir d'une opération ciblée contre une personne déterminée, identifiée du fait de son appartenance à une entreprise susceptible de pouvoir payer une rançon. Ce dernier type de K4R fait l'objet d'une préparation minutieuse (filature, repérages…) permettant de garantir son succès.

Le *tiger kidnap*

Nommé comme tel par les policiers anglais de Scotland Yard, c'est une situation au cours de laquelle un groupe de ravisseurs va retenir la famille ou les proches d'un homme d'affaire au sein de leur domicile, pour le forcer à délivrer des valeurs ou donner accès à un bâtiment normalement inaccessible. Ce type d'enlèvement touche les cadres d'institutions financières ou bancaires, ou ceux pouvant avoir accès à des informations confidentielles permettant aux malfaiteurs de commettre ensuite une infraction, comme l'accès à des serveurs sécurisés et des données confidentielles.

L'enlèvement express ou *kidnap flash*

C'est un enlèvement d'opportunité. La victime se trouve au mauvais endroit, au mauvais moment. C'est notamment le cas de voyageurs ayant recours à des taxis qui s'avèrent finalement être complices des agresseurs, et qui se détournent de leur itinéraire pour livrer leur victime à leurs complices. Ces situations, comme leur nom l'indique, ne durent que quelques heures et se finissent généralement par la remise de toutes les valeurs détenues par la victime, sur elle ou à son domicile local.

Le kidnapping virtuel

Il s'agit là d'une nouvelle forme d'enlèvement. La victime se trouve retenue contre son gré, comme par exemple lors d'une mesure de police, ou bien se situe pendant une certaine durée dans un endroit inaccessible aux moyens de communication (une réunion dans une salle en

sous-sol, une salle de sport obligeant de laisser les téléphones portables au vestiaire ou une salle de réunion hors de portée des réseaux GSM). Les ravisseurs « virtuels » contactent alors la famille de leur « victime », indiquent qu'elle est retenue par eux et demandent une rançon en échange de sa libération. Ne pouvant joindre leur proche par téléphone, les familles sont poussées à payer rapidement avant que la supercherie ne soit découverte. Plus de 50 % des familles victimes de ce type d'agression ont payé une somme d'argent dans les deux heures avant de s'apercevoir qu'il s'agissait d'une escroquerie.

ENLÈVEMENT AU MEXIQUE

Comme a son habitude, Martial est un homme d'affaires pressé : nouvellement nommé Président de la filiale d'un groupe industriel au Mexique, il sait que sa journée va être bien remplie et qu'il n'aura pas beaucoup l'occasion de lever la tête de son ordinateur. Bon connaisseur de la région pour y travailler depuis des années, Martial refuse d'avoir recours à un conducteur de sécurité, estimant que sa discrétion est la meilleure des protections dont il puisse bénéficier. Il monte dans sa voiture pour se rendre à son bureau, allume la radio pour écouter les informations locales, et démarre en direction du centre de Mexico. Après quelques minutes de circulation, la voiture de Martial est subitement bloquée par un gros véhicule 4x4 cabossé, qui s'est placé devant lui et qui vient de freiner. Un autre vient à son tour de le percuter par l'arrière, l'empêchant de reculer pour se soustraire à l'agression. En quelques secondes, trois hommes armés le menacent, l'obligeant à déverrouiller sa portière, puis l'arrachent de son siège et le jettent sans ménagement sur la banquette arrière de leur 4x4. En voyant les armes, Martial se trouve tétanisé et n'offre aucune résistance à ces agresseurs. L'un des hommes monte dans la voiture de Martial, prend le volant, et le cortège ainsi formé repart en direction d'un quartier populaire. L'opération

> n'a duré que quelques secondes, et Martial réalise qu'il vient d'être kidnappé.
>
> Après de longues minutes qui lui paraissent interminables, Martial, qui a les yeux masqués par une cagoule, est extirpé sans ménagement du véhicule puis jeté dans une pièce sombre d'où il ne sortira que trois jours plus tard, sans avoir pu ni manger ni boire. Abandonné au bord d'une route, il rejoindra à pied une maison isolée depuis laquelle il pourra faire prévenir la police et sa famille. De retour chez lui, Martial apprendra qu'une rançon de 25 000 US$ a été payée par son épouse contre sa libération. Ses ravisseurs n'ont à ce jour jamais été retrouvés.

L'aventure de Martial n'est malheureusement pas anodine. Bon nombre de collaborateurs d'entreprises internationales se retrouvent pris au piège de kidnappeurs et se voient contraints de payer pour sauver leur vie. En l'occurrence, Martial a été ciblé par ses agresseurs. Il a vraisemblablement été l'objet d'une filature, action facilitée par un certain excès de confiance l'amenant à partir tous les jours de son domicile à la même heure et à suivre le même itinéraire pour rejoindre son bureau. Par chance, la société de Martial avait souscrit ce que l'on appelle une assurance K&R, c'est-à-dire une police spécifique auprès d'une compagnie d'assurance. Grâce à cette police, un consultant spécialisé a été mis à disposition de la famille de Martial pour l'assister dans la gestion de la crise et mener les négociations. Le montant de la rançon ainsi payée, à savoir 25 000 US$, n'est pas très élevé par rapport à ce qui peut se pratiquer dans la région. La plus forte somme jamais payée, 132 millions de dollars, l'a été en Asie par un homme d'affaire chinois pour obtenir la libération de son fils.

Dans le cas de Martial, un certain nombre d'éléments sont à noter :

• Il a certainement commis une faute de sécurité en se déplaçant toujours à la même heure et par le même itinéraire. Ne pas se laisser entraîner par la routine est une façon de prévenir ce type d'agression, en modifiant ses habitudes pour ne pas donner de prises aux potentiels ravisseurs qui préfèrent souvent se rabattre sur des cibles considérées comme plus faciles.

• Son positionnement comme président d'une filiale d'un groupe industriel est un facteur l'identifiant comme une cible potentielle. Même s'il connaît bien la région, Martial aurait dû se montrer plus méfiant quant à sa visibilité et au fait qu'une telle situation professionnelle le mettait plus en risque qu'un expatrié « lambda ».

• En étant tétanisé par la peur, Martial n'a offert aucune résistance ce qui à certainement contribué à ce que son enlèvement se passe sans heurts. Une réaction mal adaptée, une résistance inconsidérée peut entraîner des réactions violentes de la part des agresseurs, pouvant être parfois fatales à la victime.

• La participation d'un négociateur professionnel, habitué à gérer ce type d'affaire, a permis de dénouer la situation rapidement, diminuant ainsi les risques physiques et psychologiques pesant sur Martial.

RÉDUIRE LE RISQUE DE KIDNAPPING

Le risque de kidnapping fait désormais partie de la cartographie des risques des entreprises qui se développent dans les zones où il est susceptible de se produire. Un plan de

prévention s'organise généralement en trois phases : information sur les zones à risque, formation des personnes potentiellement victimes et préparation à la gestion de crise.

L'information sur les zones à risque

Les kidnappings se produisent généralement dans les mêmes zones et selon les mêmes modes opératoires : des faux taxis à Mexico ou à Johannesburg, des coupeurs de route au Nigeria ou en Albanie, de soi-disant rendez-vous commerciaux qui sont en fait des pièges en Russie ou Indonésie… En étant informé de manière régulière des pièges qui existent sur sa zone d'évolution ou sur son itinéraire, en connaissant les modes opératoires les plus utilisés par les agresseurs, les expatriés, les voyageurs peuvent anticiper leurs déplacements et adapter leurs itinéraires pour ne pas se laisser piéger.

La formation aux comportements de prévention

La plupart des débriefings de kidnapping montrent que la victime a souvent commis une faute de sécurité, soit par ignorance, soit par dilettantisme, soit enfin par excès de confiance. Le fait de ne pas être attentif à son environnement, de ne pas mettre en œuvre des comportements tels que les changements réguliers d'itinéraires ou d'horaires de départ et de retours constituent des vulnérabilités et permettent aux éventuels agresseurs d'identifier une cible « facile ».

Il existe des modules de sensibilisation aux personnes qui sont envoyées par leurs entreprises dans des zones où le

kidnapping est pratiqué. Il peut s'agir de formations généralistes, s'adressant à tous ceux qui se déplacent et voyagent régulièrement. Il peut également s'agir de modules très spécifiques, adaptés à une zone ou une ville particulières, explicitant les endroits et itinéraires à éviter ainsi que les comportements adéquats pour travailler et se déplacer sereinement.

Il est à noter qu'aujourd'hui, des formations anti-kidnapping sont dispensées à des particuliers ainsi qu'à leur famille qui peuvent être victimes de ce type d'agression, et notamment le tiger kidnap.

La préparation à la gestion de crise

C'est la dernière étape d'un plan de prévention du risque de kidnapping. Savoir quoi faire en cas de disparition inquiétante d'un collaborateur, avoir les bons réflexes si une demande de rançon est faite lors d'un appel téléphonique, réagir efficacement à l'arrivée des forces de police sont des atouts pour un manager ou un dirigeant d'entreprise ayant des activités dans une zone à risque. Il existe là encore des modules de formation spécifiques, incluant des exercices de simulation pour former à la conduite de ce type de crise.

Signe que le phénomène est porteur, la technique se met depuis peu au service des victimes potentielles des kidnappings. Des moyens de géo-localisation discrets existent pour permettre le suivi en temps réel des déplacements d'un voyageur : de la taille d'un téléphone portable, ils peuvent fonctionner de manière continue ou bien être activés en cas d'incident, voir même retransmettre en direct ce

qui se dit autour de la victime tout en ayant l'air de ne pas être activé.

Les assureurs ne sont pas non plus en reste face au problème du kidnapping : un certain nombre de compagnies proposent des polices K&R, qui couvrent l'intégralité des frais générés par un enlèvement. Parmi eux, on trouve bien évidemment le remboursement de la rançon payée, et également la prise en charge des frais des consultants engagés. Le recours à des négociateurs de crise, spécialisés dans la gestion des kidnappings, est de plus en plus fréquent dans ce genre d'affaires. Ces experts de la négociation en situation complexe apportent leur expérience quand il faut affronter des situations aussi déstabilisantes pour les entreprises et pour les familles qui s'y trouvent mêlées.

POUR EN SAVOIR PLUS

« Le terrible marché », *L'Express*, 3 mai 2007.

« Kidnap, a booming industry », *Strategic Risk*, novembre 2007.

17

LE RACKET ET L'EXTORSION

« L'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque. L'extorsion est punie de sept ans d'emprisonnement et de 100 000 euros d'amende. »

Art. 312-1 du Code pénal.

LE RACKET DES ENTREPRISES EST UN BUSINESS À LA MODE

Longtemps cantonnés à certaines régions, les actes de racket et d'extorsion visant des entreprises sont devenus un business très à la mode un peu partout dans le monde. Qu'ils soient le fait de groupes criminels ou mafieux, ou qu'ils soient organisés par des autorités peu scrupuleuses, ils impactent l'activité de nombreuses entreprises, qu'elles cèdent au chantage ou non.

Le racket, l'usure, l'extorsion ont longtemps été les moyens d'action des organisations mafieuses. Les plus célèbres sont les mafias du sud de l'Italie : le racket des petites et moyennes entreprises italiennes a rapporté des dizaines millions d'euros à la mafia, selon un rapport publié par la Confesercenti[1]. Le phénomène prend de l'ampleur tous les

1. Association des PME et des commerces italiens.

ans, et on estime le nombre de commerçants victimes à plus de 200 000 pour la simple région sicilienne. Le racket n'est pas l'apanage des seuls mafieux siciliens : les triades chinoises le pratiquent depuis des siècles, et exportent leurs actes criminels jusqu'en France, en s'en prenant aux entreprises et aux commerces chinois installés sur le territoire. Les fronts pseudo-politiques qui sévissent partout dans le monde s'adonnent également à la pratique du racket pour soutirer des fonds à leurs victimes sous couvert de financement de leurs causes.

Le racket et l'extorsion sont le fait de réclamer de l'argent ou des biens matériels en utilisant l'intimidation, le chantage, la violence ou la menace de violence. On peut distinguer entre plusieurs formes d'extorsions, les plus fréquemment constatées étant les extorsions mafieuses, les extorsions criminelles, les extorsions politiques et les extorsions d'autorités.

Les extorsions mafieuses

Elles sont généralement le fait de groupes généralement bien organisés, mais d'envergures géographiques différentes : les mafias régionales sont parmi les principaux utilisateurs de l'extorsion : Camora italienne, triades chinoises, mafia albanaise… Ces rackets sont malheureusement souvent « culturels », comme c'est le cas pour le *pizzo* italien. Pour la seule Sicile, le pizzo imposé par Cosa Nostra se monte à 2 milliards par an, soit 2,5 % du PIB de l'île. Le pizzo est proportionnel au chiffre d'affaires réalisé par l'entreprise. Il existe même un barème selon le type de commerce pour ne pas ruiner la victime et continuer à

l'extroquer : de 60 euros mensuels pour un marchand à presque 1 000 euros mensuels pour un restaurant. Cosa Nostra s'intéresse aussi aux travaux de grande envergure : il se dit que 2 % des marchés de grands travaux et projets immobiliers ou d'équipement sont systématiquement reversés à la mafia. Certaines entreprises refusent de payer, et le font savoir. C'est le cas, par exemple, du groupe italien Italcementi, maison-mère de Ciments Français, qui a décidé de suspendre l'activité de sa filiale de Sicile pour ne pas se soumettre au pizzo.

Les extorsions criminelles

Organisées par des agresseurs de haut vol, elles peuvent prendre plusieurs formes. Cela peut aller de la menace directe contre un dirigeant d'entreprise ou sa famille pour exiger le paiement d'une « protection » jusqu'à l'exigence d'embauches de complices ou de membres de la famille des criminels en échange d'une « immunité » sur la zone. En Amérique Latine, ces personnes embauchées sous la contrainte sont parfois appelées *punteros* car elles sont les points de contacts entre les entreprises et les extorqueurs.

Les extorsions politiques

Elles sont perpétrées par des groupes nationalistes ou indépendantistes qui les utilisent officiellement pour financer leur cause : FLNC en Corse, ETA en Espagne, FARC en Colombie, FLEC au Cabinda font souvent l'objet de plainte de la part d'entreprises qu'ils tentent de racketter. Souvent appelé « impôt révolutionnaire », ces rackets sont

un moyen facile de soutirer des fonds pour des fins qui sont rarement politiques.

Les extorsions politiques prennent parfois des formes inattendues : la proposition de prestation. Un célèbre groupe de camps de vacances aurait été victime ce type de racket en Corse. La proposition était simple : soit vous avez recours à une société de gardiennage bien particulière, tenue en sous-main par un groupe nationaliste, soit vous prenez le risque que vos villages de bungalows soient régulièrement détruits. Bien que la victime ait longtemps nié ce racket, ce mode opératoire a déjà été utilisé sur l'île. La société Bastia Securita, dissoute depuis, proposait des convoyages de fonds en toute sécurité. Or, cette société était tenue par le FLNC, par ailleurs soupçonné d'organiser… des braquages de fourgons blindés !

Les extorsions d'autorités

Souvent corollaire de la corruption[1], les extorsions d'autorités sont le fait d'autorités qui menacent les entreprises de représailles « officielles » si elles refusent de payer ou de céder une partie de leurs droits ou de leurs marchandises. Les modes opératoires sont variés selon les pays dans lesquels ils sont mis en œuvre : détentions arbitraires, menace de procédures fiscales arbitraires, découvertes de fausses infractions permettent de faire peser sur les entreprises une menace suffisante pour « négocier » le paiement d'une protection.

1. Voir chapitre « La corruption ».

EXTORSIONS BIENS ORGANISÉES

La société X travaille dans le secteur pétrolier depuis des années. Agissant généralement avec de grands groupes internationaux, elle les accompagne dans toutes les zones sur lesquels ils travaillent. Les pays dans lesquels ils évoluent sont généralement des régions instables, et les agressions de toutes sortes sont monnaie courante. La société X est installée sur un grand chantier dans un pays d'Asie et participe à la pose de pipeline sur un territoire très étendu.

Un matin, le responsable d'un site de la société X est avisé que deux de ces ingénieurs ne se sont pas présentés à leur poste. Ils sont sortis la veille au soir en prenant un véhicule de la compagnie, et ne sont pas encore rentrés. Craignant un accident de la circulation, le responsable fait envoyer une équipe sur le trajet vraisemblablement emprunté par les deux ingénieurs. Après quelques dizaines de minutes, l'équipe de recherche revient avec les deux ingénieurs, encore blêmes de leur aventure nocturne : alors qu'ils rentraient de leur sortie et conduisaient en direction du chantier, ils ont été enlevés par un groupe armé qui les a retenus toute la nuit. Ils ont été libérés tôt le matin, seul leur véhicule a été gardé par les agresseurs. Il leur a été dit que le chef du chantier serait prochainement appelé.

Quelques heures plus tard, le responsable de la société X est demandé au téléphone dans son bureau : un individu, se faisant appeler Sacha, lui explique calmement qu'il est l'auteur de l'enlèvement de ces deux ingénieurs et qu'il est prêt à recommencer avec n'importe quel autre personnel du chantier si la somme de 500 000 $ ne lui est pas versée d'ici à une semaine. Sans attendre de réponse, Sacha raccroche après avoir indiqué que le véhicule dans lequel se trouvaient les ingénieurs serait gardé comme une avance. Abasourdi, le responsable de la société X averti son siège qui dépêche rapidement un expert. En entamant des négociations avec Marcos, l'expert a pu gagner le temps nécessaire à la mise en sûreté du chantier et au renforcement des mesures de sécurité par les forces locales.

Dans cette affaire, le kidnapping des ingénieurs constituent la marque de crédibilité des agresseurs qui ont commencé leur extorsion par une démonstration de leur capacité à nuire. Fort heureusement, l'implication rapide d'un négociateur de crise a permis de temporiser pour assurer la sécurité et terminer la mission.

> En arrivant à son bureau le matin, le secrétaire général d'un groupe de luxe ayant pignon sur rue est assailli d'appels téléphoniques : un email a été envoyé à plusieurs cadres de la société, dévoilant une information bien embarrassante. L'email dévoile en détail les dernières commandes de pierres précieuses réalisées par la division joaillerie du groupe auprès de leur principal fournisseur : quantités, dates, types de pierre, pays et mines d'origine… Or, la suite du message indique que la plupart des mines dans lesquelles s'approvisionne le fournisseur du groupe se trouvent dans des zones de conflits, et que les diamants et autres pierres achetées proviennent de mines exploitées par des forces rebelles aux gouvernements en place, qui ont généralement recours à des enfants pour travailler à l'extraction. La dernière phrase est sans équivoque : « Que penseraient vos fortunées clientes si elles savaient que les bijoux qu'elles portent ont été extraits par des enfants esclaves ? ».
>
> Vérifications faites, les informations données par les auteurs de l'email sont toutes véridiques, et les premières sollicitations faites au fournisseur montrent, dans ses réponses, qu'il n'est pas très sûr de l'éthique de tous ses propres fournisseurs. Un nouvel email des « informateurs » vient éclairer leurs intentions : « si vous ne souhaitez pas voir ces informations divulguées à la presse et aux organisations de défense des droits des enfants, faites parvenir par virement la somme indiquée ci-dessous ». La révélation était en fait une extorsion bien organisée car basée sur des informations réelles et particulièrement compromettantes.

À la suite de cette affaire, le groupe de luxe a fait auditer tous les sites de son fournisseur et a exigé une charte éthi-

que de sa part. Mais il n'a pas été possible de savoir si la somme demandée par les extorqueurs a été versée. Quoi qu'il en soit, les informations n'ont jamais été révélées à la presse.

PRÉVENIR LE RISQUE DE RACKET

La problématique du racket est assez proche de celle de la corruption, évoquée dans un autre chapitre. Accepter de payer et rentrer dans le jeu est un piège inextricable duquel il est très difficile de se sortir, refuser de payer, c'est s'exposer à des passages à l'acte parfois violents et destructeurs. Un grand groupe pétrolier a été victime d'attentats à répétition sur ses pipelines dans un pays du sud. Les auteurs de ces actes ont ensuite contactés les dirigeants locaux du groupe pour leur proposer un marché : soit les attentats continuent, engendrant des frais colossaux, soit le groupe accepte de payer des « agents de sécurité » le long de ses pipelines et les attaques cessent. En faisant ses calculs, le groupe pétrolier s'est aperçu que payer les extorqueurs lui coûterait cinq fois moins cher que la réparation des dégâts engendrés par un seul attentat. Résultat : le groupe a payé, et en acceptant le racket, s'est enfermé dans une situation de dépendance extrêmement risquée.

S'informer

Les actes de racket et d'extorsion, s'ils ne sont pas toujours portés à la connaissance des autorités dans le cadre de plaintes au pénal, sont connus de ceux qui évoluent dans les zones où ils sont utilisés. Dans leurs *ratings* sur l'évaluation des risques-pays à destination des entreprises,

les sociétés d'analyses géopolitiques prennent en compte ce facteur pour attribuer un niveau de risque. Par ailleurs, les modes opératoires sont également le plus souvent connus : extorsion à l'embauche, sollicitation de l'impôt révolutionnaire ou du pizzo local, menace de détention arbitraire…

Une bonne information en amont d'un développement de projet sur une zone « à risque » permet de prendre les précautions nécessaires à la diminution de la menace.

Alerter les forces de l'ordre

C'est la loi du silence qui favorise le business du racket et qui offre une impunité à ceux qui le pratique. En Corse, un restaurateur a fait la une des journaux en dénonçant publiquement le racket dont il était victime : soit il payait un « impôt » imposé par ses agresseurs, soit son restaurant allait faire l'objet d'attentats à l'explosif. Pour saluer son courage, le Président de la République Nicolas Sarkozy lui a rendu visite lors d'un de ces passages sur l'île de beauté.

Il existe des services spécialisés dans la lutte conte le grand banditisme et le crime organisé dans la plupart des pays « à risque » : les alerter de la situation permet d'enquêter sur les auteurs de l'extorsion pour faciliter leur interpellation et faire cesser la menace.

Anticiper la menace

Il est possible d'anticiper la menace d'extorsion en prenant de cours les agresseurs. Les revendications de ceux qui réclament des fonds ou des services en échange d'une « impunité » ont parfois des revendications sociales : il est alors possible de vider toute revendication de sa substance.

Dans ce cadre, une entreprise française se développant dans un pays africain a pris les devants : certaines populations ayant l'habitude de menacer les chantiers des sociétés occidentales en échange de l'embauche de membres de la communauté, l'entreprise a anticipé le risque en allant voir les responsables des communautés en cause pour leur proposer d'intégrer à leurs équipes des habitants locaux. Après cela, difficile d'aller extorquer la société pour lui demander de faire une chose qu'elle a déjà réalisée.

Les entreprises ayant des activités dans des zones à risque d'extorsion ont souvent recours, dans le cadre de leur politique de sûreté, à des CLO : *Communities Liaison Officer*. Ces « négociateurs » prennent les devant des racketteurs en allant, bien en amont des projets, rencontrer les communautés pour les associer aux projets et ainsi couper l'herbe sous le pied des extorqueurs.

Faire appel à des consultants spécialisés

Face à l'augmentation des situations d'extorsion et de racket dont sont victimes les entreprises, des sociétés spécialisées proposent leurs services de gestion des crises. Ces services peuvent être des actions de prévention et d'anticipation, mais également des actions de gestion de la menace quand elle se produit :

• ***Les actions de prévention :*** grâce à des analystes spécialisés, ces sociétés évaluent le risque de racket, ses modes opératoires potentiels selon les zones de développement, et anticipent les coûts liés à la prévention du risque.

• ***Les actions de conduite :*** des experts évaluent la véracité de la menace, car certains rackets reposent sur du bluff

et sur la crainte que génère leur survenue sur les victimes. Si la menace s'avère authentique, les consultants spécialisés évaluent la meilleure stratégie à appliquer en fonction des auteurs potentiels, des autorités locales et des coûts engendrés par les actions à mener. Ils peuvent préconiser une amélioration des mesures de sécurité ou toute autre mesure susceptible de dissuader les agresseurs de recommencer leur action.

POUR EN SAVOIR PLUS

Reymond W., *Mafia SA : Les Secrets du crime organisé*, Flammarion, 2001.

Gayraud J.-F., *Le monde des mafias, géopolitique du crime organisé*, Odile Jacob, 2005.

18

PANDÉMIES ET CRISES SANITAIRES

« Le coût de la prévention de la pandémie grippale est estimé à 425 millions de dollars »

David Nabarro[1]

DES VAGUES PANDÉMIQUES DÉVASTATRICES

Ces dernières années ont été le théâtre de situations de paniques collectives et de réactions de psychoses parfois irrationnelles liées à des phénomènes inattendus : les pandémies, et plus précisément les pandémies grippales susceptibles d'évoluer vers une transmission à l'homme. La mondialisation des échanges et des déplacements se développant, c'est un nouveau facteur à prendre en compte dans l'anticipation de telles crises. Ces phénomènes ne sont pourtant pas inédits : le XX^{e} siècle a connu trois grandes pandémies grippales dévastatrices : entre 1918 et 1920, la grippe espagnole a causé entre 20 et 40 millions de mort selon les estimations. En 1957, c'est la grippe asiatique qui faisait des milliers de morts. Enfin, en 1968, c'est la grippe de Hong Kong qui a défrayé la chronique.

1. Coordonnateur principal du système des Nations Unies pour les grippes aviaires et humaines.

La crise du SRAS[1] a rappelé à tous la fragilité des systèmes économiques et leur potentielle déstabilisation par des maladies pandémiques pouvant causer un nombre de décès indéterminés. La pneumonie atypique est une maladie hautement infectieuse provenant du virus SARS-CoV. Caractérisée par un syndrome respiratoire aigu sévère, elle est apparue pour la première fois en Chine en novembre 2002, et a provoqué une épidémie mondiale en mai 2003 du fait de sa transmission par voie aérienne, en touchant un grand nombre de personnes dans de nombreux pays.

Le virus de la grippe aviaire, également appelé H5N1, a généré à son tour une nouvelle panique à partir de 2005. En effet, en cas de pandémie de grippe aviaire, les conséquences au plan humain et au plan économique pourraient être dévastatrices. Après l'Asie, l'Afrique et l'Europe, le virus H5N1 a touché de façon épisodique l'Europe. Essentiellement propagée par les oiseaux migrateurs, la grippe a touché la France de façon sporadique mais de façon bien réelle, rappelant la vulnérabilité de tous face à ce type de crise. Ce qui rend très particulière cette épidémie, c'est sa vitesse de propagation du fait des phénomènes de migrations animales, et la possible mutation du virus : les experts de l'Organisation Mondiale de la Santé craignent une adaptation du virus H5N1 à l'homme qui rende possible la transmission interhumaine, ce qui pourrait engendrer une pandémie grippale à l'échelle mondiale. L'OMS a demandé que chaque pays se prépare à faire face à la survenue d'une catastrophe sanitaire. En France, la Direction Générale de la Santé a élaboré un plan de lutte contre une pandémie

1. Syndrome respiratoire aigu sévère.

grippale, distinguant différentes phases pour une mise en œuvre graduée des mesures de prévention et de lutte.

Définition des phases des plans de lutte contre une pandémie grippale	
Période interpandémique	
Phase 1	Pas de nouveau virus grippal circulant chez l'homme.
Phase 2	Pas de nouveau virus grippal circulant chez l'homme, malgré un virus animal occasionnant un risque substantiel de maladie humaine.
Période d'alerte pandémique (pré-pandémie)	
Phase 3	Infection humaine par un nouveau virus (pas de transmission interhumaine, ou cas rares et isolés liés à des contacts rapprochés).
Phase 4	Cas groupés (« clusters ») de transmission interhumaine limitée et localisée (virus incomplètement adapté aux humains).
Phase 5	Extension des cas groupés, encore géographiquement localisée (le virus s'adapte à l'homme).
Période pandémique	
Phase 6	Forte transmission interhumaine dans la population, avec extension géographique rapide.

La menace de pandémie a été un véritable électrochoc dans bon nombre d'entreprises. En effet, face au risque de propagation rapide d'une maladie mortelle à grande l'échelle, les conséquences économiques sont apparues

comme étant aussi importantes que les conséquences humaines. Encouragées par les instructions des autorités publiques et par la constitution des plans nationaux de lutte contre les pandémies, les entreprises se sont préparées à limiter leurs pertes et à assurer la continuité de leurs activités : distribution des produits de première nécessité (produits alimentaires, médicaments), services vitaux (services de santé, transports, énergie, télécommunications) mais également toutes activités économiques interdépendantes les unes des autres.

Les conséquences pour les entreprises d'une pandémie ou d'une crise sanitaire de grande envergure sont essentiellement de deux ordres, la réduction des effectifs et la réduction des activités.

La réduction des effectifs a été estimée, en cas de pandémie de H5N1, entre 25 % et 60 %, durant 4 à 8 semaines. Cet absentéisme peut avoir plusieurs causes :

– personnels décédés des suites de la maladie dans les cas les plus graves ;
– personnels malades ou en convalescence suite à la maladie ;
– personnels placés en quarantaine à domicile ;
– gardes malades ou gardes d'enfants suite à la fermeture des crèches et des écoles ;
– engagement bénévole de personnels dans les activités sanitaires : pompiers volontaires, Croix Rouge…

La réduction du personnel a bien évidement une conséquence directe sur la réduction de l'activité, mais elle n'est pas la seule. En cas de pandémie, il y aura d'autres phénomènes impactant l'activité :

– limitation de la clientèle du fait sa propre réduction d'activité ;
– limitation des déplacements, pouvant aller jusqu'à l'interdiction pure et simple de la part des autorités ;
– restriction du transport des matières premières ;
– restriction du transport des composants de chaînes de production ;
– réduction de la disponibilité des personnels de maintenance.

Les crises pandémiques posent le problème crucial de la continuité des activités en situation dégradée : comment continuer à assurer l'essentiel de l'activité stratégique de l'entreprise alors que les conditions optimales ne sont plus réunies, et cela pour une durée plus ou moins longue ?

UNE INFECTION TRÈS DÉSTABILISANTE

Stéphane, chef d'entreprise installé depuis de nombreuses années en Amérique latine, est un producteur de viande qui sait mener sa barque. Il se fournit chez les meilleurs éleveurs de la région, a monté ses propres chaînes d'abattage, de conditionnement, et exporte une bonne partie de sa marchandise vers l'Europe et l'Amérique du Nord. Grâce à son réseau dans les pays dans lesquels il exporte, Stéphane parvient à fournir les meilleurs restaurants, avec des niveaux de prix très intéressants, lui permettant de dégager une marge confortable. En bref, les affaires de Stéphane marchent très bien.

Stéphane fait le point avec une partie de ses contremaîtres sur l'activité de son site de conditionnement et examine l'efficacité des chaînes. Constatant un relâchement dans les statistiques, Stéphane en demande la cause au contremaître concerné : celui-ci lui répond que plusieurs personnes ont été malades cette semaine, mais que les choses vont rapidement rentrer dans

l'ordre avec le recrutement de remplaçants pour l'occasion. Sans y prêter plus d'attention, Stéphane continue son point de situation général.

Stéphane, qui a rejoint son bureau, entend frapper à sa porte : Raul, son contremaître en chef, à l'air des mauvais jours : plusieurs personnels ne se sont pas présentés ce matin, et cela commence à impacter le rendement et l'activité de plusieurs sites. Stéphane lui demande de préciser : on lui a dit ce matin que les quelques malades seraient remplacés dans la journée. Or, il s'avère que le problème est plus important que ce qui lui a été rapporté : il n'y a pas que quelques malades, mais une dizaine de collaborateurs sont absents, et plusieurs de ceux qui s'étaient présentés ce matin sont rentrés chez eux. Pris de crampes d'estomac insoutenables et de diarrhées hémorragiques, les malades ont été amenés à l'infirmerie rudimentaire de l'entreprise qui n'a rien pu faire d'autre que leur demander de rentrer chez eux. Quant aux remplaçants potentiels, essentiellement recrutés parmi les familles des employés, il semble qu'un certain nombre soient également malades.

En quelques heures, Stéphane a vu l'ensemble de sa production s'arrêter : entre les malades absents le matin, les malades rentrés chez eux et les collaborateurs chargés de raccompagner les malades, la moitié des chaînes de production a été arrêtée. Et la psychose a fait le reste : devant autant de malades, s'écroulant à leur poste de travail, la plupart des employés indemnes ont quitté leur poste pour rentrer chez eux. La rumeur n'a pas tardé à s'étendre, parlant d'une maladie redoutable touchant les employés des sites de production de viande. La crise de l'ESB étant encore dans tous les esprits, le lien a été vite fait pour générer une psychose complètement irrationnelle, jusqu'à l'arrivée des autorités locales venant savoir ce qui se passait dans l'usine. L'activité de l'entreprise a été arrêtée en quelques heures, pour une durée de quatre jours avant un retour à une situation quasi-normale. La cause de tout cela ? Une simple intoxication alimentaire. Il semble que la nourriture servie à la cantine de l'entreprise ait été faite avec des produits avariés. Ce sont les familles

> des salariés qui se chargent de faire la cuisine pour tout le monde, en utilisant notamment des morceaux de viandes non utilisés dans la production. Une partie des produits ayant servi à faire le repas de la veille a vraisemblablement été conservée dans de mauvaises conditions, générant une contamination attribuée dans ce cas d'espèce à une bactérie de type Escherichia Coli. Les salariés ayant l'habitude d'emporter chez eux la nourriture non consommée, cela pourrait expliquer les cas de contamination des membres de certaines familles ne travaillant pas sur le site.

Face à une contamination heureusement bénigne, Stéphane s'est trouvé confronté à la problématique que pourrait rencontrer toute entreprise face à une crise pandémique : diminution importante et rapide d'une partie des effectifs, impossibilité à trouver des remplaçants, effets de psychoses irrationnelles entraînant une réduction puis un arrêt complet de l'activité. Surpris par la rapidité du phénomène, et n'ayant aucunes procédures de continuité, Stéphane a vu toute son activité arrêtée en quelques heures.

SE PRÉPARER À AFFRONTER UNE PANDÉMIE MASSIVE

La problématique de situations telles que les pandémies de maladies mortelles transmissibles à l'homme, c'est qu'elles génèrent un effet de panique qui rend difficilement contrôlable un certain nombre de paramètres dans la conduite de la situation. Un plan de prévention face à une pandémie grippale comprend des mesures de sensibilisation des personnels impliqués et des mesures de planification des activités.

Impliquer les personnels

Pour éviter les effets de psychose que peut susciter une pandémie, a fortiori avec l'effet amplificateur des médias diffusant tous azimuts des données plus alarmantes les une que les autres, une implication des personnels est nécessaire. Cette implication peut passer par des modules de formation expliquant les effets de la maladie et les meilleurs moyens de s'en prémunir et d'éviter sa propagation.

La sensibilisation permet également d'expliquer à tous les personnels, quels que soient leur rôle ou leur fonction dans l'entreprise, ce que l'on attend d'eux en cas de survenue d'une pandémie impactant la continuité de l'activité.

La protection des personnels

La protection des personnels dans le cadre de l'exercice de leur activité professionnelle relève de la responsabilité du chef d'entreprise. La protection face à une pandémie fait partie de cette responsabilité.

L'ensemble des personnels doit faire partie de cette politique de protection personnelle, a fortiori ceux qui se trouvent en présence du public et qui pourraient avoir des contacts avec des personnes contaminées.

La protection des personnels, dans le cadre d'un maintien de l'activité et de la présence au sein de l'entreprise, se fera selon les recommandations des autorités médicales. Dans le cas de la pandémie de H5N1, la protection des personnels porte essentiellement sur le port d'un masque facial pour éviter les contaminations interhumaines. Ces masques, de type FFP2, ont été achetés en masse au point

d'en arriver une pénurie et à voir se développer un marché parallèle sur Internet.

Il est à noter que, dans le cas d'une pandémie, avant même que les recommandations des autorités ne soient de cesser toutes activités professionnelles non essentielles, les salariés peuvent exercer leur droit de retrait. Dans ce cadre, tout salarié qui s'estime en danger dans le cadre de son exercice professionnel peut se retirer de sa mission de sa propre initiative, sans qu'il ne puisse être sanctionné pour cela. Il est donc possible d'envisager, dans le cas d'une menace de pandémie non encore avérée, un nombre important d'exercices de droit de retrait préventif impactant lourdement l'activité de l'entreprise.

Les plans de continuité

Le plan de continuité d'activité, également appelé PCA ou BCP (Business Continuity Plan), est un élément essentiel du plan de gestion d'une pandémie ou d'une crise sanitaire. Ce PCA doit se mettre en œuvre en plusieurs étapes :

• ***Identification des activités essentielles :*** parmi toutes les activités ou les services délivrés par l'entreprise, quelles sont celles qui sont indispensables à la continuité de l'activité ? Ce sont en fait celles qui permettent un fonctionnement minimal. Les fonctions supports, par exemple, peuvent être mises en stand by, alors que certaines fonctions de production doivent être maintenues coûte que coûte.

• ***Identification des personnels clés :*** ce sont les personnes qui peuvent assurer la continuité des activités essentielles.

• ***Identifier les moyens logistiques*** nécessaires à la continuité minimale de l'activité.

Les modes de travail alternatifs

Une des premières mesures, en cas de pandémie, serait la restriction ou l'interdiction de circulation des personnes. Dès lors, impossible pour les personnels n'étant pas engagés dans des activités d'importance vitales (énergie, alimentation des populations, soins médicaux) de rejoindre leur lieu de travail. L'expérience récente du virus H5N1 a permis de démontrer l'existence de modes de travail alternatifs, au premier rang desquels le télétravail. En identifiant les fonctions pouvant être assurées à distance et en s'organisant pour faire travailler une partie du personnel depuis leur domicile, bon nombre d'entreprises ont trouvé un moyen de continuer leur activité malgré des restrictions importantes de circulation des personnes.

La gestion de la connaissance

L'expérience du H5N1 a également démontré qu'une bonne partie des personnels des entreprises était capable d'assumer d'autres fonctions que celles qui leur étaient attribuées. De par leurs expériences passées, leurs formations initiales, leurs capacités personnelles, des collaborateurs peuvent être affectés à des missions considérées comme essentielles et changer leurs habitudes professionnelles pour faire face à la situation.

Une gestion efficace des connaissances, en recensant précisément les aptitudes de chacun et en assurant un minimum de remise à niveau régulièrement, permet à

toute entreprise de trouver parmi son personnel les outils de sa continuité d'activité dans le cadre d'une crise pandémique grave.

POUR EN SAVOIR PLUS

Gilbert C., *Les crises sanitaires de grande ampleur : un nouveau défi ?*, Documentation Française, 2007.

Graeme L., « Origin and control of Pandemic Influenza », *Science*, vol. 293, 2001.

CONCLUSION

VERS UNE NOUVELLE CULTURE DE LA MENACE

L'homme et les organisations qu'il bâtit sont enclins à mettre leur environnement en équation pour le comprendre, l'anticiper, et éliminer tous les paramètres non prédictibles. Alors, face à ces nouvelles menaces en constante évolution et qui sortent des équations traditionnellement utilisées, quel est le niveau de conscience et de préparation des entreprises ?

Il est possible d'utiliser des modèles d'analyse déjà existants pour anticiper les nouveaux prédateurs. Citons, par exemple, le référentiel d'analyse SWOT, aussi appelé matrice SWOT[1]. Ce modèle, axé sur la recherche des atouts, faiblesses, opportunités et menaces conduit à mener deux types d'audits :

• ***Un audit interne***, identifiant les forces et les faiblesses du domaine d'activité de l'entreprise. Cet audit peut se mener à cœur de cible, c'est-à-dire dans l'entreprise elle-même. Il peut aussi se mener dans l'environnement direct de la société, notamment par l'étude des concurrents et des partenaires ainsi que leur vision du marché et l'entreprise objet de l'audit.

1. Strengths Weaknesses Opportunities Threats.

• ***Un audit externe***, qui identifie les opportunités et les menaces dans l'environnement au sens large. Elles peuvent être déterminées grâce à des modèles d'analyses stratégiques, comme le modèle de Michael Porter par exemple.

Dans le cadre de la méthode SWOT, il est intéressant d'élargir l'analyse vers les menaces non-conventionnelles et la façon dont elles pourraient impacter l'activité de l'entreprise. Mais avant même la création et l'application d'une méthode d'audit particulière, anticiper les nouvelles menaces et les nouveaux prédateurs demande une ouverture d'esprit et une capacité à regarder en dehors des cadres classiques du risk management, une aptitude à reconstruire sans cesse de nouveaux outils de détection adaptés à un environnement incertain.

Cette nouvelle perception des menaces impose une globalisation du processus de gestion des risques, enchaînant des étapes transverses :

• ***Audit des risques :*** cet audit envisage les menaces en se plaçant au cœur de l'entreprise. Associé notamment à la démarche SWOT, il permet de couvrir l'ensemble des situations de vulnérabilité de la société. Ce premier pas d'une politique de gestion des risques doit s'accompagner de l'implication de tous les services dans la démarche, en sollicitant chacun pour apporter sa vision des failles potentielles de l'organisation. Chaque service pourra ensuite observer les failles des autres départements de la société, en se positionnant en recul par rapport à eux, et ainsi apporter un nouvel angle de vue et d'analyse.

• ***Audit d'environnement :*** l'audit d'environnement est une analyse des menaces non plus en se plaçant au cœur de l'entreprise elle-même mais plutôt dans le secteur d'activité

au sens large. Cette étude permet d'identifier des menaces qui pourraient venir des partenaires ou adversaires déclarés : fournisseurs, partenaires financiers, économiques, commerciaux, concurrents, autorités de régulation, groupes de pression, utilisateurs… Cet audit recense également les situations non conventionnelles vécues par des acteurs de l'environnement sectoriel.

• ***Cartographie des menaces :*** identifiées, les risques et les menaces sont placés dans une cartographie mentionnant pour chacun la probabilité d'occurrence et la criticité de la réalisation du risque. Cette cartographie a pour objectif de recenser les risques les plus probables et/ou les plus critiques pour s'assurer que les mesures de prévention sont adaptées en conséquence. Il est rare de voir apparaître sur une cartographie des risques « classiques » des menaces non conventionnelles, alors que c'est justement parce qu'elles sont nouvelles et rarement anticipées qu'elles peuvent s'avérer critiques.

• ***Assurances :*** les grands groupes d'assurances proposent de plus en plus de polices spécifiques, identifiées parfois sous les thématiques « risques spéciaux » ou « risques non convetionnels ». Associer son courtier et son assureur dans l'identification des menaces nouvelles n'est pas incongru, chacun ayant sa part dans la détection précoce des risques auxquels s'expose l'entreprise.

• ***Politique de prévention :*** le premier objectif d'une politique de gestion des risques, c'est de prévenir leur survenue et/ou de réduire leurs conséquences. La politique de prévention prévoit des mesures spécifiques pour chacune des menaces et met en œuvre les moyens dédiés pour les éviter.

• ***Gestion des crises :*** la politique de prévention ne suffit pas toujours, et il faut parfois piloter une crise avérée. Une organisation dédiée, comprenant une cellule de crise, des moyens logistiques et des modes opératoires dédiés à la conduite d'une situation dégradée permet de gérer les évènements imprévus.

Au-delà de toutes les procédures et de tous les plans de prévention, la gestion des nouvelles menaces planant sur les entreprises de demain repose sur une prise de conscience de leur existence et du fait que leur survenue ne relève plus du film hollywoodien ou de la science-fiction. La politique de l'Autruche n'ayant jamais sauvé personne, savoir évaluer ses vulnérabilités est une démarche responsable pour tout manager souhaitant mener sa barque au travers des écueils d'un environnement économique en perpétuelle mutation et face à des prédateurs qui ne doutent de rien pour tirer profit d'une telle instabilité.

Il faut de nombreuses qualités pour être un entrepreneur aujourd'hui, a fortiori pour se préparer à évoluer sur des marchés complexes. Mais il est indéniable que la qualité primordiale qui fera les succès de demain, c'est l'optimisme. François Guizot disait : « le monde appartient aux optimistes, les pessimistes ne sont que des spectateurs ». Face à un environnement dans lequel l'efficacité repose sur 80 % de préparation et sur 20 % d'improvisation, l'optimisme est la clé pour affronter et vaincre les menaces de demain.

STRATÉGIES ET MANAGEMENT

Laurent Combalbert

ENTREPRISES : HALTE AUX PRÉDATEURS !

OPA hostiles, débauchages agressifs, contrefaçons, détournements de marchandises, corruption…, quelles que soient leur taille ou leur activité, les entreprises sont confrontées à des situations de crise de plus en plus déstabilisantes.

Ces menaces, **nouvelles par leur forme**, **leur impact ou leur caractère aléatoire**, obligent les dirigeants à revoir leurs stratégies de défense.

L'auteur analyse ici une vingtaine de menaces ayant réellement touché des entreprises au cours des dix dernières années. Il s'appuie sur son expérience quotidienne de la gestion des risques et des crises pour proposer **des solutions adaptées, permettant d'éviter l'agression** ou de la contrer.

Chaque menace est abordée de manière synthétique et pratique, suivant une méthodologie efficace :

- définition de la menace ;
- illustration par un cas réel ;
- moyens de défense à mettre en œuvre.

Un guide indispensable, à lire d'urgence !

LAURENT COMBALBERT

Licencié en Droit et Criminologie, diplômé de l'Ecole Nationale Supérieure des Officiers de Police, formé à la National Academy du Federal Bureau of Investigation, il a été Officier-négociateur au sein d'un groupe d'intervention spécialisé dans la gestion des crises et la résolution de prises d'otages (RAID). Il est aujourd'hui directeur du développement du groupe Geos.
Expert APM, il intervient au sein de nombreuses entreprises.

ISBN 978-2-10-053579-8

www.dunod.com

DUNOD