Club des Directeurs
CDSE
de Sécurité des Entreprises

LIVRE BLANC

La fonction sûreté dans l'entreprise

Quelles réponses à quelles problématiques ?

CDSE

Club des Directeurs de Sécurité des Entreprises

Livre blanc
CDSE, Paris
décembre 2011

Directeur de la publication
Olivier Hassid

Rédaction
Mathieu Pellerin/Julien Marcel

Création graphique
Aurélie San Emeterio
www.pointcommun.fr

Crédit photo
Vincent Gérard

Impression
Morvan Fouillet imprimeurs

Au fil des années, le CDSE est devenu une association européenne majeure regroupant les directeurs de la sécurité et de la sûreté de plus de 80 entreprises internationales. Leur engagement quotidien concourt à la définition des normes de demain et à la formation d'une communauté partageant expériences et idées. Présidé par Alain Juillet, ancien Haut Représentant à l'Intelligence Économique en France, qui a succédé à François Roussely, ancien PDG d'EDF, le CDSE se veut être :

- un réseau européen de réflexion entre acteurs de la sûreté, à travers le Colloque Annuel à l'OCDE, ou les travaux réalisés au sein de huit commissions thématiques ;
- une plateforme de soutien technique et relationnel auprès de ses membres ;
- un vecteur de diffusion de la connaissance en matière de sûreté, en s'appuyant notamment sur la revue *Sécurité & Stratégie* et le journal des DSE ;
- un interlocuteur phare des pouvoirs publics, symbolisé par les partenariats avec le SGDSN, l'ANSSI, la DCRI, le ministère de la Défense et le Centre de crise du ministère des Affaires étrangères.

SYNTHÈSE

DES PROPOSITIONS ET RECOMMANDATIONS D'ACTIONS

À DESTINATION DES ENTREPRISES

- Identifier les vulnérabilités de chaque entreprise en matière de sûreté et définir une politique de protection adaptée à celles-ci.
- Faire évoluer la fonction sûreté vers un rôle plus global de gestion des risques et des crises.
- Rattacher le directeur sûreté à un membre du Comité Exécutif afin de renforcer l'efficacité de son action.
- Positionner la fonction sûreté dans un processus global et une approche décloisonnée.
- Intégrer la sûreté dans les cursus de formation des futurs managers.
- Systématiser les retours d'expérience et les faire partager.
- Assurer la protection de l'ensemble du personnel qu'il soit local ou en mobilité.
- Veiller au respect des règles d'éthique dans la mise en œuvre de la politique de sûreté.

À DESTINATION DES AUTORITÉS

- Promouvoir une accréditation « Confidentiel Entreprise ».
- Porter la loi sur « le secret des affaires » à un niveau européen afin d'harmoniser et de réglementer les pratiques des entreprises.
- Créer un groupe de réflexion public/privé et interministériel sur les normes existantes en matière de sûreté, avec une mise en perspective comparée européenne et internationale.
- Associer le CDSE à la rédaction des textes législatifs et réglementaires relatifs à la sûreté.
- Communiquer par anticipation aux directeurs sûreté accrédités les informations sensibles qui concernent leur entreprise.
- Impliquer les entreprises dans la conception des dispositifs de gestion de crise.

SOMMAIRE

Note aux lecteurs

Les termes sécurité et sûreté sont employés distinctement ou parfois de manière couplée pour définir un même monde, celui de la protection de l'entreprise.

Le choix du terme varie selon l'entreprise, son secteur d'activité, sa taille, et selon le domaine de compétences du directeur de sécurité/sûreté.

Par conséquent, dans les textes qui suivent, certains directeurs parleront de sécurité, d'autres de sûreté, ou bien de sécurité/sûreté, et ce, pour respecter l'intitulé de leur poste au sein de leur entreprise et représenter au mieux le rayon d'action de leur fonction.

INTRODUCTION

ALAIN JUILLET

Président du CDSE

Alain Juillet

Président du Club
des Directeurs de Sécurité
des Entreprises

Dirigeant de nombreuses entreprises françaises et étrangères, avant d'être nommé directeur de la stratégie à la DGSE de 2002 à 2003. Il a ensuite occupé jusqu'en 2009 les fonctions de Haut Représentant à l'Intelligence Économique, rattaché au Premier Ministre. Il intègre ensuite le cabinet d'avocats ORRICK en qualité de conseiller senior. Il fut élevé au grade de Commandeur de la Légion d'honneur le 14 juillet 2009.

Vous souvenez-vous de ces vieux westerns dans lesquels on trouvait ce personnage sympathique de l'éclaireur accompagnant discrètement troupes et immigrants vers la terre promise ?

Il connaît parfaitement le terrain, les populations locales et leurs mœurs, ainsi que les risques spécifiques de l'environnement. Rusé mais loyal, expérimenté, il contribue au succès de l'aventure en définissant avec le chef de l'expédition la stratégie d'évitement des pièges, les caps à tenir. Sans lui la réussite finale reste hypothétique. Il ne prétend pas remplacer les troupes. Il ne s'intéresse pas trop aux affaires des voyageurs, sauf quand des brigands se mêlent au convoi. Il reste un peu à l'écart, en avance sur la marche des autres, garantissant ainsi la sûreté du chemin et la possible réussite de l'aventure collective.

C'est exactement le rôle du directeur de sûreté d'une entreprise aujourd'hui. Et il serait aussi imprudent, voire inconscient, pour un dirigeant de s'en priver que pour nos voyageurs d'hier de s'aventurer dans des contrées inconnues sans ses conseils.

Aujourd'hui le danger est partout. Les indiens, les voleurs, les serpents, les chausse-trapes sont même souvent derrière les lignes. Par l'informatique, la globalisation, les risques se sont multipliés au moment même où nos sociétés promettaient de plus en plus de sécurité et imposaient aux entrepreneurs de participer à la création globale de sécurité. Les textes se multiplient. Les jurisprudences se font de plus en plus strictes et contraignantes alors que Fort Apache n'existe plus dans sa simplicité physique. Il a été remplacé par un monde souvent virtuel, mouvant, polymorphe. La vérité se dérobe. La confiance n'est plus au rendez-vous. Les pactes ne sont pas respectés.

Face à ce monde instable et insaisissable, la tentation peut être grande de se lancer à l'aveuglette dans l'aventure en prenant une bonne assurance, en fermant les yeux et en adressant une prière au ciel. Pourtant, les solutions à ces défis existent. Encore faut-il choisir les bonnes portes.

Tout l'enjeu de ce livre blanc est là.

Il s'agit de convaincre tant les industriels que les pouvoirs publics que le directeur (ou directrice) de sûreté d'une entreprise a le savoir-faire, l'expérience et les connaissances requis pour déjouer la plupart des risques encourus par celle-ci.

À la lecture des textes qui suivent, on en sera amplement convaincu. Il y a ici non seulement la démonstration d'une compétence mais des idées prospectives qui honorent cette nouvelle profession en plein essor. Le CDSE remplit parfaitement son rôle en livrant ces textes à un public qui ignore encore trop souvent ce métier, son contenu et son utilité.

Le directeur de sûreté n'est ni un barbouze reconverti, ni un homme ou une femme de l'ombre, pas plus un empêcheur de tourner en rond ou encore un pantouflard vieillissant. C'est quelqu'un qui contribue à la richesse et au succès de l'entreprise en se montrant à la pointe du savoir et des techniques nécessaires à son exercice quotidien.

Il ne fait aucun doute pour moi que les actuels responsables de sûreté sauront en conséquence relever le défi de la démonstration qu'on leur demande et qu'ils sauront également installer définitivement cette fonction dans l'entreprise, la rendant indispensable à l'avenir. On se demandera même sans doute un jour comment on faisait « sans » avant !

Cette dernière remarque est pour moi l'occasion de dire ici deux choses qui me tiennent à cœur et que ce livre blanc contient d'ailleurs de façon sous-jacente :

■ **L'État ne peut pas fournir tous les moyens de protection de l'entreprise.** Il se désengage même fortement dans certains cas de ce terrain pour plusieurs raisons qu'il serait trop long d'évoquer ou de démontrer ici. **Il revient donc aux entreprises de garantir leur propre sécurité.** Même celles qui seront retenues dans la nomenclature des infrastructures sensibles, dont la liste pourrait utilement être revue soit dit au passage. On ne peut prétendre importer, dupliquer les services d'État dans une société commerciale. À chacun son travail. Ce qu'il faut faire, c'est favoriser les fenêtres de communication entre ces deux mondes du privé et du public, le dernier se mettant au service du premier chaque fois que c'est légitime. L'éthique de ces mouvements de va-et-vient entre le public et le privé est donc au cœur même de la réflexion du CDSE et de ses adhérents. Ce sera de plus en plus ainsi. Sûreté et responsabilité sociale ont des recoupements de plus en plus fréquents.

■ **Le profil du directeur de sûreté évoluera probablement à l'avenir.** D'un côté se situent tous les techniciens de la sécurité matérielle, physique, informatique, de la propriété intellectuelle, etc. Ces techniciens ont besoin d'un corps de connaissances de plus en plus étendu et précis sans lequel ils prendraient des risques légaux. Ce sont les managers de la sécurité dont le niveau peut être très élevé en fonction de la taille de l'entreprise. D'un autre côté, il faudra un chef d'orchestre de tous ces savoirs, dont le rôle est de faire que la partition soit bien rendue, ce qui suppose l'harmonie de tous les instruments précédents. Il faudra à ces responsables un sens aigu de la stratégie, sans parler d'une certaine capacité à faire face à l'imprévu. C'est le nouveau domaine de la sûreté globale, sans limite bien définie mais qui va au-delà de la simple conformité aux textes ou jurisprudences. Directement intégré au plus haut niveau de l'entreprise, ce directeur ou cette directrice doit avoir les moyens tant budgétaires qu'humains de mettre en œuvre sa stratégie d'accompagnement des activités commerciales. De la route reste à faire dans ce sens. Ce livre blanc en est le premier pas.

Bonne lecture à tous, surtout aux chefs d'entreprise qui se demandent encore parfois à quoi servent ces drôles de "messieurs-dames" de la sécurité : soyez rassurés, faites leur confiance, ils vous aident tout simplement à traverser les territoires indiens et à arriver à bon port ! ■

1 DÉFINITION DE LA FONCTION SÛRETÉ

SÉCURITÉ ET SÛRETÉ DANS LA STRATÉGIE DES ENTREPRISES

ÉRIC LE GRAND

Éric Le Grand

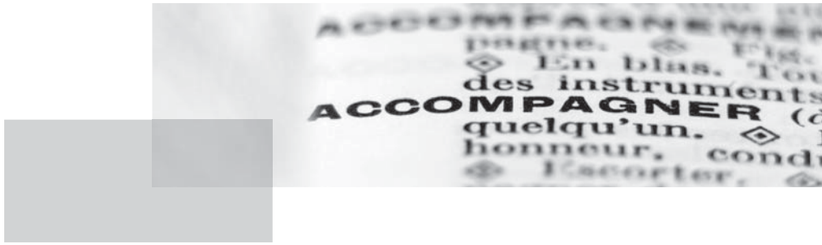
Directeur de la prévention et de la protection du groupe RENAULT

Directeur de la prévention et de la protection du groupe RENAULT SAS. A effectué toute sa carrière professionnelle à des postes de responsabilité sécurité dans des grandes entreprises, dont la direction sécurité/sûreté du groupe LA POSTE.

Depuis plusieurs décennies, évoluant dans un environnement réglementaire et normatif de plus en plus responsabilisant, l'entreprise a progressivement pris en compte la maîtrise de ses risques endogènes, c'est-à-dire ceux qui sont générés par son activité propre (accidents du travail, accidents de process…). En ce qui concerne les risques exogènes, la protection vis-à-vis des menaces externes, qu'elles soient de natures naturelles (séisme, pandémie…), géopolitiques (guerre, terrorisme…) ou criminelles (vol, fraude, contrefaçon, espionnage industriel…) l'entreprise attendait généralement de la part des États dans lesquels elle opérait, qu'ils garantissent sa sécurité.

Les attentats du 11 septembre, la jurisprudence Karachi, les menaces de pandémie, les catastrophes majeures au Japon, les troubles géopolitiques dans les pays arabes, font peu à peu prendre conscience à l'entreprise qu'elle doit se soucier de sa sûreté, car elle porte désormais également de lourdes responsabilités en la matière.

L'entreprise est bien entendu confrontée à des risques nouveaux, elle évolue dans des environnements instables, elle est la cible de prédateurs en tous genres, mais c'est également en raison de sa stratégie d'organisation qu'elle s'est fortement vulnérabilisée ces dernières années. Les interdépendances d'activités, l'externalisation de fonctions vitales, le travail en flux tendus, la dépendance totale aux systèmes d'informations, la mondialisation, la concurrence exacerbée l'ont énormément fragilisée en faisant que le moindre impact peut avoir des conséquences critiques, pour les clients, les personnels, les biens, le patrimoine, l'information, l'image, mais également pour la résilience globale de la société civile à laquelle elle contribue.



LA SÉCURITÉ ET LA SÛRETÉ AU CŒUR DE LA MAÎTRISE DES RISQUES

Entreprendre c'est prendre des risques. Condamnée à aller de l'avant, l'entreprise qui ne prend pas de risques (nouveaux produits, nouveaux marchés, nouvelles organisations…) ne sera probablement plus là demain. Il en est de même pour celles qui en auront trop pris. La juste prise de risques et la maîtrise de ceux-ci sont donc au cœur même de la stratégie de l'entreprise.

Elle doit, en amont du processus de décision, analyser les risques, les évaluer, les anticiper. Dans la phase de réalisation, elle doit les prévenir, s'en protéger, et en cas d'impact, mettre en place des dispositifs de continuité et des dispositifs de gestion de crise. La sûreté et la sécurité sont donc le nécessaire accompagnement de la prise de risques du décideur. **La fonction de sécurité/sûreté longtemps considérée comme une fonction secondaire, devient maintenant une fonction stratégique au sein des entreprises.**

LA SÉCURITÉ ET LA SÛRETÉ AU CŒUR DE LA GOUVERNANCE

La lecture des codes de conduite et des règles de gouvernance affichés par de très nombreuses sociétés le montre, **la sécurité et la sûreté ont une place fondamentale dans la gouvernance de l'entreprise.** Les obligations envers les clients intègrent prioritairement la sécurité et la sûreté des produits et des services. Les obligations envers les actionnaires imposent l'exigence de la sûreté des biens et actifs. La sécurité du travail, la sûreté des déplacements sont à la base des obligations envers le personnel. Quant à la continuité d'activité des fonctions essentielles, la contribution à la résilience des États, elles font partie désormais des obligations envers la société civile. Pour être bien gouvernée, l'entreprise doit être sûre et sécurisée.

LA SÉCURITÉ ET LA SÛRETÉ AU CŒUR DES POLITIQUES DE QUALITÉ ET DE DÉVELOPPEMENT DURABLE

D'énormes chantiers ont été menés ces dernières années au sein des entreprises en matière de qualité mais aussi en matière de développement durable. **Comment vanter la qualité d'un produit ou d'un service si celui-ci n'est pas sûr ?**

Un système d'information doit être sécurisé et sûr pour garantir sa qualité. La qualité d'un environnement de travail tient également à la sécurité qui y prédomine. Il en va de même pour les politiques de développement durable qui reposent sur la sécurité des produits et la sûreté des process. Dans les études de dangers, la prise en compte d'une pollution accidentelle n'est plus suffisante, il faut dorénavant intégrer les menaces d'actes criminels ou terroristes.

Il n'est donc pas vain de rappeler qu'une démarche qualité repose avant toute chose sur un pré-requis, la sécurité.

LA SÉCURITÉ ET LA SÛRETÉ AU CŒUR DE LA CONFIANCE

De mauvais résultats de sécurité impactent fortement le résultat de l'entreprise, engagent sa responsabilité et portent atteinte à son image et à celle de ses dirigeants.

Depuis quelques années, la production par les entreprises, sur une base volontaire, de données non financières, constitue à l'évidence une information importante pour les différentes parties prenantes (actionnaires, consommateurs, salariés, États…) et constitue désormais un des paramètres essentiels de la confiance. Parmi ces données non financières, les données sociales et environnementales sont généralement les plus utilisées. Il n'existe cependant à ce jour aucune prise en compte des données relatives à la sécurité et la sûreté, alors qu'elles sont autant d'indicateurs pertinents sur la manière dont l'entreprise intègre les menaces et met en œuvre son dispositif de maîtrise des risques.

La sécurité et la sûreté sont devenues un enjeu indéniable de confiance et de compétitivité. ■

Recommandations opérationnelles

- **Promouvoir la mise en place d'une notation en matière de sécurité/sûreté évaluant les politiques, les organisations, les plans d'actions et les résultats obtenus dans ce domaine, nous semble indispensable pour évaluer le bon niveau de gouvernance des entreprises. Le CDSE dispose des conclusions du groupe de travail « Notation ».**
- **Promouvoir la sûreté auprès des chefs d'entreprise et organisations qui les représentent, afin d'accélérer la prise en compte de la sûreté dans la stratégie des entreprises. Le CDSE joue un rôle majeur dans ce domaine.**
- **Intégrer la sécurité et la sûreté dans les cursus de formation des futurs managers. Le CDSE peut contribuer activement à ces formations.**
- **Accompagner la nécessaire évolution réglementaire et normative, par la participation du CDSE en tant qu'expert de la sécurité et de la sûreté d'entreprise aux travaux menés dans ces domaines.**

LE DIRECTEUR SÛRETÉ

PASCAL CRÉPIN

Pascal Crépin

Directeur services généraux et sûreté du groupe AIR LIQUIDE

Diplômé de l'ESLSCA Paris, formé à l'Institut des Hautes Études de Défense Nationale en Intelligence Économique. Il a débuté son parcours en PME-PMI puis chez RENAULT dans des fonctions de développement commercial à l'export avant de rejoindre le groupe AIR LIQUIDE en 1989. Il a été nommé à plusieurs postes de directeur de région puis à un poste de DRH Mobilité Interne et Développement Professionnel France. Élu membre de la Chambre de Commerce et d'Industrie de Vaucluse et président national du réseau des Écoles de Gestion et de Commerce jusqu'en 2010, il est aujourd'hui membre du conseil d'administration du CDSE.

Par son rôle d'« éclaireur » évoqué par Alain Juillet en préambule de ce livre blanc, le directeur sûreté aide les entreprises à évoluer dans des environnements incertains, des géographies nouvelles où elles peuvent être confrontées au surgissement d'événements inédits. Le directeur sûreté concourt au développement de l'activité en aidant les dirigeants à la prise de décision et en sécurisant les opérations.

LES MISSIONS DU DIRECTEUR SÛRETÉ

Le directeur sûreté définit et s'assure de la bonne application des politiques de mise en sûreté dans l'ensemble des pays où l'entreprise est présente. L'ensemble des dispositifs concourt à protéger les parties prenantes (employés, dirigeants, clients…) et les actifs (matériels & immatériels) de l'entreprise, ce qui constitue *in fine* la véritable valeur économique d'une entreprise, contre des menaces ou des risques épars.

Aussi doit-il identifier et cartographier en continu les risques et menaces pouvant peser sur l'entreprise, procéder à une analyse des écarts permettant de mettre en évidence les vulnérabilités et fixer les priorités de sûreté à traiter en fonction des occurrences et des conséquences possibles.

Le directeur sûreté tient en permanence trois postures :

Une posture de prévention

Le directeur sûreté est consulté en amont des principaux projets. Il mesure en permanence le niveau de protection en fonction du degré d'exposition aux risques. Il prévoit les processus de gestion de crise, et forme les managers et leurs équipes à la sûreté économique. Il s'assure de l'actualisation des Plans de Continuité d'Activité (PCA). Il assure l'interface avec les services des États, des organismes européens ou internationaux compétents dans ses domaines.

Participant à la bonne application du devoir de protection de l'entreprise vis-à-vis de ses salariés, il déploie des politiques et des dispositifs de protection au sein des établissements, durant les déplacements dans les pays identifiés à risque et au cours de manifestations ou événements majeurs.

De même, le directeur sûreté s'assure de la protection des actifs matériels, immatériels et informationnels.

Une posture de conseil

L'analyse approfondie des retours d'expérience et l'adaptation en continu des procédures permettent la mise en place d'un véritable système de management de la sûreté globale. À l'instar de la qualité, la sûreté doit en effet aussi pouvoir s'appuyer sur un référentiel dédié.

En apportant les réponses adaptées aux risques et menaces identifiés et pesés, le directeur sûreté aide le dirigeant à décider en toute connaissance.

Il peut si nécessaire traiter les sujets ou informations sensibles avec l'interlocuteur adéquat, jusqu'au plus haut niveau de l'organisation.

Une posture de réaction

En cas de crise procédant d'un incident de sûreté, le directeur sûreté intervient en première ligne dans le cadre d'une cellule *ad hoc* en proposant des réponses pertinentes et en assurant le suivi de la mise en œuvre des décisions. Ainsi, dans le cadre de la gestion de la crise, il est en charge de l'activation des contacts avec les organisations compétentes ainsi que des dispositifs sûreté prévus. Avec les autres managers impliqués, le directeur sûreté s'assure de la défense des intérêts et de la poursuite des activités de l'entreprise dans le cadre d'un PCA.

Au-delà du noyau central de ses responsabilités, les missions globales du directeur sûreté dépendent étroitement de l'entreprise, de son secteur, sa présence à l'international, dans des pays à risques élevés, de sa stratégie, de son exposition.

La veille peut ainsi être rattachée à la direction sûreté. Le recueil, l'interprétation et la valorisation de l'information (sectorielle, économique, géopolitique etc..) à des fins stratégiques représente un outil précieux d'aide à la décision.

Enfin, l'influence peut également reporter à la direction sûreté. En faisant connaître et prévaloir ses points de vue auprès des organisations nationales, européennes ou internationales, l'entreprise se place en capacité d'agir au mieux de ses intérêts.

LES MODES OPÉRATOIRES

La fonction sûreté est une fonction support au même titre que les ressources humaines, la communication ou les finances par exemple. Naturellement, le directeur sûreté travaille en étroite coordination avec les autres directions fonctionnelles et opérationnelles. Il s'applique à faire adhérer en expliquant, en communiquant, en s'attachant à convaincre.

La direction sûreté est idéalement positionnée au plus haut niveau de l'organisation, rattachée à la Direction Générale (DG) ou directement à l'un des membres du Comité Exécutif.

Pour agir, le directeur sûreté s'appuie sur la politique et le référentiel sûreté, ainsi que sur les grands principes de gouvernance de l'entreprise (valeurs clés, guide de bonne conduite, principes d'action, code éthique…).

Le directeur sûreté veille à ce que les ressources de la direction sûreté soient proportionnelles aux enjeux économiques et aux impacts possibles des menaces. Il s'appuie sur des compétences et des expertises internes ou obtenues au sein de réseaux dédiés (CDSE), qu'il complète auprès de services de l'État (D2IE, SGDSN, ANSSI, MAEE, INHESJ, IHEDN, DCRI, DPSD…) pour obtenir des conseils, bénéficier de formations ou de sensibilisations.

D2IE
Délégation Interministérielle à l'Intelligence Économique

SGDSN
Secrétariat Général de la Défense et de la Sécurité Nationale

ANSSI
Agence Nationale de la Sécurité des Systèmes d'Information

MAEE
Ministère des Affaires Étrangères et Européennes

INHESJ
Institut National des Hautes Études de la Sécurité et de la Justice

IHEDN
Institut des Hautes Études de Défense Nationale

DCRI
Direction Centrale du Renseignement Intérieur

DPSD
Direction de la Protection et de la Sécurité de la Défense

LES PROFILS ET TRAJECTOIRES

Quels que soient sa formation initiale et son parcours professionnel, **le directeur sûreté réunit à la fois une bonne connaissance de l'entreprise, une expérience avérée et des connaissances approfondies dans les domaines de la sûreté et de la gestion de crise.** Son leadership est alors naturellement reconnu de même que son esprit critique, ainsi que son courage pour adopter une position indépendante et objective si nécessaire. **Le directeur sûreté fait preuve d'une aptitude prononcée à gérer la complexité, les paradoxes de même que les sujets sensibles.**

Dans un contexte de guerre économique, qu'il s'agisse de faire face à l'audace sans borne et à la sophistication des outils utilisés par des prédateurs de toutes sortes, ou de conduire des projets innovants qui exposent à des risques inédits sur de nouveaux territoires, les dirigeants savent s'appuyer sur le directeur sûreté pour permettre à l'entreprise de délivrer une performance économique de manière responsable.

Le directeur sûreté se forme et forme en continu son équipe dans le cadre d'un parcours professionnel auprès des Instituts tels que par exemple l'INHESJ, l'IHEDN, ou l'École Nationale Supérieure de la Police ainsi qu'en participant à des événements organisés par les différents Clubs Professionnels. Afin de distiller la culture de sûreté économique, il s'appuie sur la DCRI, la DPSD et la Gendarmerie en particulier dans le cadre des séances de sensibilisation qu'ils organisent pour le personnel des entreprises. De même, il veille à la formation des collaborateurs en mission à l'international ou en expatriation dans des pays à risques.Il sait se tenir informé et recueillir l'information utile et pertinente sur les domaines ou les zones géographiques stratégiques pour son entreprise. ■

Recommandations opérationnelles

- **Le rattachement du directeur sûreté à l'un des membres du Comité Exécutif ou son appartenance au Comex favorise bien évidemment l'efficacité de son action.**
- **La professionnalisation de la fonction passe par un parcours reconnu de directeur sûreté avec, au-delà des formations et trajectoires initiales, des modules de formation spécifiques répondant aux nouveaux besoins ainsi que des formations intégrant les problématiques de la sûreté à l'international.**
- **Les instituts ou écoles supérieures gérés par l'État pourront ainsi encore mieux accompagner l'évolution de la profession en intégrant ces dernières dimensions.**
- **Un véritable Système de Management de la Sûreté reposant sur un référentiel normatif pourrait être élaboré par un groupe de normalisation *ad hoc* intégrant des directeurs sûreté d'entreprises françaises largement ouvertes à l'international.**
- **Les missions du directeur sûreté reposent aussi sur la confiance que lui portent les dirigeants et les autres parties prenantes. Aussi doivent-elles être régulièrement auditées et leurs performances mesurées.**

LA CRÉATION D'UNE DIRECTION SÛRETÉ

CHRISTIAN AGHROUM

Christian Aghroum

Directeur sécurité
du groupe SICPA

Commissaire divisionnaire en disponibilité de la fonction publique. Il est dorénavant directeur de la sûreté du groupe SICPA, leader mondial des encres de sécurité, basé à Lausanne (CH). Il a dirigé quatre années durant l'OCLCTIC, l'office de lutte contre la cybercriminalité. Il totalise une trentaine d'années au service de la Police Nationale française dans la lutte contre la criminalité organisée et le terrorisme. Il est président honoraire de l'Amicale des Cadres de la Police Nationale et de la Sécurité Intérieure, auteur et coauteur de nombreux ouvrages.

Direction incontournable d'une entreprise moderne, la direction sûreté est entourée de mystères. Cette absence de transparence inquiète souvent l'équipe de gouvernance en marche vers la création d'une direction sûreté. Il convient après avoir abordé les facteurs de nécessité, d'étudier les étapes essentielles à la bonne installation de cette nouvelle direction et propres à assurer la stabilité de l'entreprise.

UN CHOIX ASSUMÉ AU PLUS HAUT NIVEAU DE L'ENTREPRISE

Créer une direction sûreté répond à un besoin parfois diffus et impose un choix assumé au plus haut niveau de l'entreprise. Les besoins de sécurité croissent et la réponse à y apporter demande de plus en plus de compétences croisées. Ces exigences concernent les entreprises de toute taille.

Augmentation générale de l'insécurité, globalisation, développements à l'étranger, corruption, multiplications des voyages en zone à risque, explosion des moyens sophistiqués de communication, cyberinsécurité et cybercriminalité sont autant de facteurs requérant une approche matricielle. L'absence souvent rencontrée de convergence entre sûreté et sécurité informatique illustre parfaitement l'éparpillement des responsabilités au sein des différentes directions de sécurité, empêchant la direction générale d'avoir une vision globale et un éclairage *ad hoc*. La réactivité nécessaire au traitement d'événements mettant rapidement en péril l'image et ou les responsabilités civiles et pénales de l'entreprise impose une centralisation éclairée, d'autant que le recours à des entreprises spécialisées sous-traitantes est souvent de rigueur. Le traitement de cette sous-traitance présente souvent pour le néophyte l'écueil du jargon et de l'expérience d'un domaine plus spécialisé qu'il n'y paraît de prime abord. **Une analyse des risques menée avec objectivité permet rapidement au comité exécutif ou à toute instance similaire de mesurer le besoin de création.** Cette analyse veillera, outre l'identification des risques, à mesurer les redondances et écarts d'information existants ainsi que les sujets non traités. Cette analyse permettra d'identifier où précisément positionner la direction sécurité ; elle sera soumise au directeur nouvellement recruté.

Le choix de la structure et de son responsable sont déterminants. Sens éthique, connaissances juridiques et techniques, sens des responsabilités, disponibilité, compétences managériales, entregent… Tel un inventaire à la Prévert, ces critères fondent traditionnellement le choix. Le poste doit être rattaché au moins à l'un des membres du comité exécutif, seul gage de confiance et d'autorité nécessaires au bon exercice de l'activité. Le profil de directeur sûreté est dorénavant connu : une littérature abondante existe en la matière ; le recours à de classiques chasseurs de tête est encore peu efficace en ce domaine, l'éclairage d'une organisation neutre et stable telle le CDSE est de bon conseil.

La structure entourant le directeur sûreté doit être proportionnée à la taille de l'entreprise ; il ne fait à cet égard aucun doute que si le poste peut être occupé à temps partiel dans une PME, il est difficilement envisageable qu'un groupe international en fasse l'économie.

Une formation continue, un contact permanent avec les autorités publiques et leurs pairs assureront à l'ensemble des membres de l'équipe de sûreté une adéquation réelle aux exigences de leur métier. **L'intégration dans la nouvelle équipe de collaborateurs issus d'autres directions favorise l'acceptation générale du dispositif.**

LA DIRECTION SÛRETÉ INTÉGRÉE AU CŒUR DE L'ENTREPRISE CONTRIBUE À SA PÉRENNITÉ

La direction sûreté peut rapidement devenir un tour d'ivoire ; quelques conseils de bon sens permettent d'en éviter le travers. Le directeur et ses futurs collaborateurs doivent rapidement comprendre le fonctionnement de l'entreprise, sa complexité, son ou ses cœurs de métier. Un programme d'intégration ouvert, des visites de sites, des rencontres directes avec les différents niveaux de responsabilité hiérarchique, syndicale, sociale permettent de démystifier la nouvelle direction et de rassurer les collaborateurs.

La discrétion qu'impose la mission n'exclut aucune information sur l'existence de cette nouvelle direction tant en interne qu'en externe. Savoir qu'il existe une direction sûreté dans une entreprise n'expose pas cette dernière mais permet au contraire à cette direction d'asseoir sa légitimité et d'accroître sa sphère d'influence, son relationnel et de rassurer clients et partenaires sur le sérieux de l'entreprise.

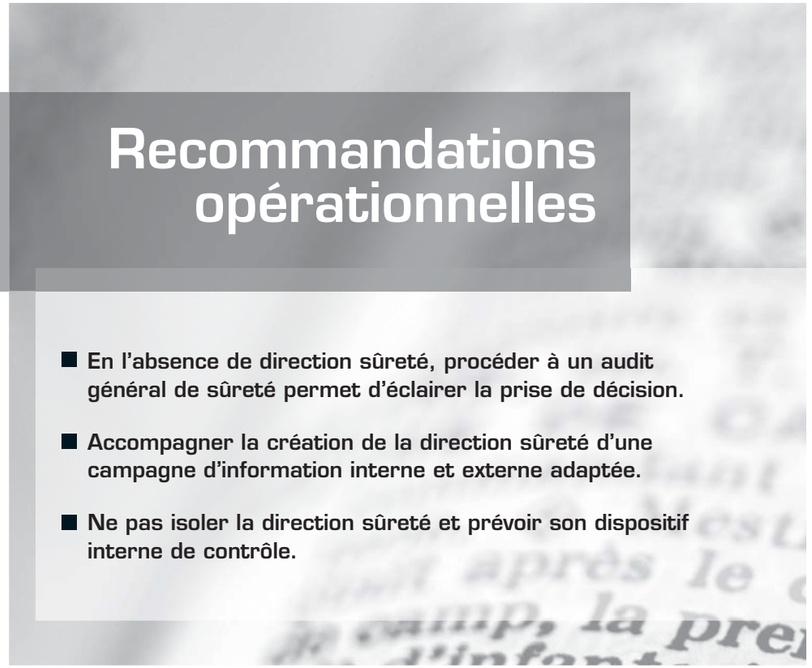
Une présentation claire des missions permet d'en rappeler l'objectif principal : protéger l'entreprise et ses collaborateurs ! Cette démarche s'accompagnera rapidement de la diffusion de la documentation assortie, d'autant qu'un arbitrage de compétences est souvent nécessaire. La direction sûreté ne fonctionne bien qu'en coordination avec les autres directions, cette aisance est facilitée par l'absence de chevauchement de responsabilités.

Le temps est l'allié de la nouvelle direction. Une première année permet souvent de saisir les besoins fondamentaux de l'entreprise et de mesurer efficacement la voilure nécessaire et les champs d'action à traiter. À chaque entreprise correspond une structuration particulière de la direction de la sûreté, selon sa taille, son organisation interne et son secteur d'activité.

Trois compétences essentielles peuvent pourtant aisément lui être rattachées : protection des biens et des personnes, sécurité des systèmes d'information et enquêtes internes. Le management du risque ou l'hygiène et la sécurité (au sens des règles ISO et OHSAS) peuvent lui être adjointes à plus ou moins long terme ou demeurer à l'écart tant que les échanges sont sains et fructueux. Attendre des résultats immédiatement palpables relève d'une méconnaissance de cette matière reposant principalement sur le facteur humain et pour laquelle les indicateurs d'activité sont difficiles à standardiser. Le choix de correspondants intégrés ou *ad hoc* dans les divisions, départements ou filiales s'apprécie en fonction du nombre, de la taille et de la nature d'activité de ces derniers. Le temps permet enfin la mise en place d'un centre de coût idoine, souvent difficile à estimer antérieurement à la première année de fonctionnement.

Une direction sûreté ne peut toutefois se suffire à elle-même et sous-traite une grande partie de son activité à des entreprises spécialisées. La plus-value de la sûreté réside dans la maîtrise de ses dossiers, dans la confrontation des résultats aux spécificités de l'entreprise et dans les éclairages apportés par les analyses de la direction.

Si la sûreté ne doit pas freiner le commerce ou le développement industriel, elle en est l'incontournable facette dans un univers de plus en plus global et complexe, où les risques s'échelonnent de l'incivilité au banditisme, voire à l'acte terroriste. Dans ce contexte, la spécialisation permet à la gouvernance une prise de décision plus éclairée tout en profitant d'un instrument pertinent de réputation et de fiabilité juridique. ■



Recommandations opérationnelles

- **En l'absence de direction sûreté, procéder à un audit général de sûreté permet d'éclairer la prise de décision.**
- **Accompagner la création de la direction sûreté d'une campagne d'information interne et externe adaptée.**
- **Ne pas isoler la direction sûreté et prévoir son dispositif interne de contrôle.**

LES RAPPORTS ÉTAT-ENTREPRISE DANS LE DOMAINE DE LA SÛRETÉ

MARIE GEROSA - LAURENT MEREYDE

Marie Gerosa

Directrice-adjointe
sécurité du groupe THALES

Titulaire d'une maîtrise de droit public, d'un DEA de science politique et d'un diplôme de criminologie, commissaire divisionnaire, actuellement en disponibilité. Chef d'unités de recherche à la 1re Division de Police Judiciaire de la Préfecture de Police en 1994, chef de section à la Division Nationale Anti Terroriste de la Direction Centrale de la Police Judiciaire en 1998. En 2004 elle est nommée responsable du service des violence urbaines à la Direction Centrale des Renseignements Généraux. En 2009 elle intègre le groupe THALES en qualité de directrice-adjointe.

La sûreté du patrimoine de l'entreprise passe par une coopération avec les institutions étatiques puisque les conditions sécuritaires de protection des personnels, des biens et de l'information, impliquent de façon directe ou non le soutien de l'État.

Ce constat qui varie selon les secteurs d'activité et le degré d'internationalisation des entreprises ne confère pas pour autant un rôle de premier plan à l'État dans la création ou le développement des missions de sûreté dans les entreprises. Il peut être un partenaire privilégié dans trois domaines principaux à savoir : la prise de conscience prévalant à la création d'une direction sûreté, le processus même de création, le fonctionnement au quotidien.

LA CONTRIBUTION ÉTATIQUE À LA CRÉATION D'UNE DIRECTION SÛRETÉ

Un incident sérieux voire tragique tel un enlèvement, un assassinat, une destruction d'équipements ou encore la captation d'informations stratégiques sont des éléments favorisant la prise de conscience de la nécessité, pour une société, de s'organiser afin d'anticiper la réitération d'une telle situation et de prendre les mesures destinées à réduire au maximum l'exposition aux risques. Dans cet esprit, l'État peut aider à la création d'une direction sûreté, et ce à travers trois axes :

Laurent Mereyde

Directeur sûreté
du groupe TECHNIP

A rejoint TECHNIP en 2004 au poste de directeur sûreté du groupe. Auparavant, il a servi au sein de l'État et à la sûreté d'AIR FRANCE. Laurent Mereyde est diplômé du Conservatoire National des Arts et Métiers (Master Énergie, Master Économie Internationale) et titulaire d'un DEA de géopolitique. Auditeur du Centre des Hautes Études de l'Asie Moderne et de l'Institut des Hautes Études de la Sécurité Intérieure (IHESI). Il est co-auteur d'un ouvrage collectif sur la politique méditerranéenne (éd. Mac Millan et Université de Reading). Il est actuellement administrateur du CDSE et président de la commission sûreté internationale du CINDEX/CDSE depuis sa création en 2004.

- **La formation initiale : l'investissement dans les futurs cadres**

  Les universités et les écoles qui abordent dans leur cursus les questions de sûreté dans le management restent encore marginales. Il paraît souhaitable que l'État aide à la prise de conscience de la nécessité de formations sensibilisant de futurs « managers » à la mise en place d'outils de veille, de gestion des risques, d'aide à la création de structures dédiées à la prise en compte de l'exposition des entreprises aux actes de malveillance d'origine humaine.

- **La formation continue : l'investissement dans le plus grand nombre**

  Le partenariat État-organisations professionnelles à travers des cycles de conférences permet de mieux sensibiliser les acteurs de la sûreté en actualisant leurs connaissances et en partageant les bonnes pratiques.

- **Les exposés donnés par les dirigeants des administrations : l'investissement à haut niveau**

  Ces conférences destinées aux cadres dirigeants d'entreprises contribuent à affiner leur prise de conscience des enjeux de sûreté en mettant en exergue l'évolution des menaces de tous genres et de leurs impacts économiques potentiels.

LA CRÉATION D'UNE DIRECTION SÛRETÉ

Le niveau hiérarchique qui décide de la création d'une direction sûreté est déterminant dans l'orientation générale de cette entité. Cet acte « originel » consacre l'importance que l'entreprise donnera aux missions de la sûreté. L'État, sans se substituer à cette démarche interne ni interférer dans le choix des personnes qui conduiront les actions de sûreté, peut contribuer à la réussite du processus à travers deux axes :

- **Encourager la rédaction d'un code de bonnes pratiques**

Cet élément est essentiel à la qualité des missions de la sûreté et surtout à la transparence de ses actions à l'égard des salariés. Cette transparence, gage de la crédibilité d'une direction sûreté et de sa pérennité, peut être encouragée par l'État en distinguant les domaines dans lesquels l'entreprise intervient seule et ceux où l'action étatique peut venir ponctuellement aider cette dernière (en cas de captation d'information par une puissance étrangère, ou pour la protection de ses ressortissants dans le cadre d'une évacuation d'un pays en crise).

- **Soutenir un processus d'aide et de conseils**

À travers la mise en place d'une structure qui reste à définir, l'État pourrait mettre à disposition, si besoin, des experts pouvant aider à la création ou l'évolution d'une direction de sûreté. Cette aide ponctuelle, délivrée à la demande d'une direction de sûreté en cours de création ou de restructuration pourrait fournir une sorte « de trame générale » définissant les missions globales, ainsi que les voies et moyens pour les réaliser.

LE FONCTIONNEMENT AU QUOTIDIEN

La protection des collaborateurs en déplacement ou en affectation dans des pays difficiles, la protection des systèmes d'information et du patrimoine de l'entreprise sont des missions essentielles de toute direction sûreté. Dans ces domaines, l'État peut apporter sa contribution tout en respectant l'indépendance - valeur fondamentale - de l'entreprise à travers deux axes :

- **L'échange d'informations de point-situation-pays**

Le site Internet « conseils aux voyageurs » n'apporte pas encore toute la valeur ajoutée que les entreprises, compte tenu de la spécificité des moyens qu'elles mettent en œuvre, peuvent attendre de l'État. Aussi, un site dédié aux entreprises serait une contribution attendue dans le fonctionnement des directions sûreté pour leur permettre de mieux recouper les informations de situation dont elles disposent. Là aussi, une approche régionale serait un premier pas.

- **La diffusion d'alertes sur les menaces visant les systèmes informatiques ou l'apparition de nouveaux modes opératoires frauduleux**

Ici aussi, les services spécialisés de l'État tels les services de répressions judiciaires, peuvent contribuer à la protection des intérêts des entreprises via leurs directions sûreté en communiquant selon un protocole *ad hoc* les informations précises visant les éléments constitutifs de telles infractions ou tout au moins les attaques signalées contre les réseaux.

La sûreté est un domaine dans lequel les États et les entreprises partagent un objectif commun majeur : la protection des femmes et des hommes qui y travaillent, et au-delà, les savoirs-faire des industries stratégiques. ■

LES TECHNOLOGIES DE LA SÉCURITÉ

CHRISTIAN AGHROUM

Christian Aghroum

Directeur sécurité
du groupe SICPA

Commissaire divisionnaire en disponibilité de la fonction publique. Il est dorénavant directeur de la sûreté du groupe SICPA, leader mondial des encres de sécurité, basé à Lausanne (CH). Il a dirigé quatre années durant l'OCLCTIC, l'office de lutte contre la cybercriminalité. Il totalise une trentaine d'années au service de la Police Nationale française dans la lutte contre la criminalité organisée et le terrorisme.
Il est président honoraire de l'Amicale des Cadres de la Police Nationale et de la Sécurité Intérieure, auteur et coauteur de nombreux ouvrages.

Face à un éventail de risques toujours plus étendu et une responsabilité accrue en matière de sûreté consécutive au retrait de l'État vers le cœur primitif de ses fonctions régaliennes, les entreprises se livrent à une course aux technologies de sûreté. Cette course est rendue nécessaire par la sophistication accrue des moyens utilisés par les délinquants ou par la nécessité d'apporter des preuves incontestables lors du procès pénal ou civil.

De natures variées, complémentaires des moyens traditionnels, ces technologies sont un atout incontournable à la sûreté de l'entreprise. Sans cesse renouvelées, elles nécessitent d'être maîtrisées et leur pertinence doit toujours être remise en question. De ce constat naissent trois propositions à partager avec le monde privé et les pouvoirs publics.

LE CHAMP DES TECHNOLOGIES DE LA SÛRETÉ EST LARGE ET COLLE AUX BESOINS SÉCURITAIRES DE L'ENTREPRISE

L'État lui-même externalise tout ou partie de sa sûreté pour alléger les charges indues de la police et de la gendarmerie nationales et recentrer celles-ci sur ses missions régaliennes; **il ne s'agit donc pas de renforcer l'implication des forces publiques de sécurité intérieure dans les missions de protection, de filtrage ou de gardiennage d'entreprises privées.** La charge en revient au secteur privé. Les technologies de la sûreté évoluent et leur marché s'accroît. La biométrie a de longue date fait son entrée dans les outils de contrôle d'accès ; la vidéo-surveillance a rejoint récemment l'espace public alors qu'elle est un outil confirmé et indissociable de la protection périmétrique ; la lecture automatisée des plaques d'immatriculation aide au filtrage des véhicules dans les parkings tant publics que privés...

L'adéquation des techniques colle à la diversité des besoins de sûreté et à leur évolution : surveillance périmétrique, contrôles d'accès des personnels et des véhicules, géolocalisation des biens et des moyens de transports, marquage et détection des contrefaçons, surveillance et protection des réseaux de communication (téléphonie, internet...). Ces technologies avancées ne remplacent pas pour autant les moyens traditionnels : clôtures, portes, coffres et autres blindages, outils d'appui à la surveillance physique (communication, équipement de protection...). Naturellement, les moyens d'hygiène et de sécurité qui concourent à la sûreté de l'entreprise (lutter contre l'incendie, c'est aussi prévenir le sabotage...) sont à prendre en compte.

L'extension des technologies de protection au monde de la sûreté d'entreprise garantit l'expansion d'un marché boosté par un accroissement des menaces. Selon l'Atlas 2009-2010 d'*En Toute Sécurité*, 22 créneaux segmentent le marché de la sûreté en France pour un montant avoisinant les 19 millions d'euros en 2008, contre 11 millions en 1999 (soit une augmentation de 172 % en moins de dix ans). L'ouverture au privé de salons de la sécurité traditionnellement réservés aux services de l'État est révélatrice également de l'évolution du marché.

LA MAÎTRISE DES TECHNOLOGIES DE LA SÛRETÉ EST INDISPENSABLE : ELLE GARANTIT À L'ENTREPRISE UNE DÉMARCHE ÉTHIQUE

L'accès non maîtrisé aux technologies de protection peut rapidement rouvrir la boîte de Pandore des maux de la sûreté que sont l'amateurisme, la « barbouzerie », l'illégalité. La protection des libertés publiques et individuelles doit demeurer la règle. Ce n'est pas sans raison que le législateur encadre tout ou partie des activités de protection et de surveillance (loi informatique et liberté, lois d'orientation et de programmation de la sécurité...). Les technologies de la sûreté, en perpétuelle évolution, sont complémentaires, interactives et permettent d'établir des recoupements comportementaux. Une utilisation déviante ou autonome de ces technologies conduit à plus ou moins long terme aux tribunaux. Le directeur sûreté trouvera dans le code pénal, le code du travail et bien d'autres supports juridiques les réponses à ses préoccupations déontologiques.

L'impact managérial impose aussi formation et information tant des utilisateurs que des collaborateurs. La collaboration de la direction sûreté avec les autres départements de l'entreprise doit ainsi être privilégiée : comment installer un système biométrique de contrôle d'accès sans une communication appropriée levant les doutes légitimes des employés ? Aidé en interne par la direction juridique, la direction des

ressources humaines, la direction de la communication, mais aussi par un réseau externe solide et compétent (comme celui qu'offre le CDSE), le directeur sûreté évitera les pièges du tout sécuritaire, la démesure paranoïaque ou l'espionnage des collaborateurs.

L'anticipation et la veille technologique sont primordiales afin d'éviter de choisir des solutions techniques rapidement surannées. Ces qualités permettent aussi de ne pas succomber à la mode et de faire les frais d'une technologie si novatrice que son usage est mal encadré légalement et sa sécurité mal maîtrisée. Le moins disant, les technologies achetées dans des pays peu scrupuleux en termes d'équité sociale ou de lutte anti contrefaçon ne garantissent ni la qualité des produits ni la réputation de l'acheteur. La sûreté a un prix, il faut l'assumer. Une analyse rationnelle assure cependant une corrélation entre les capacités financières, l'image et le besoin réel de protection. L'externalisation peut souvent être choisie par souci de rationalité mais la confiance dans le partenaire doit alors être totale.

Le recours aux technologies de la sûreté jouit d'un avenir radieux dans un monde de plus en plus imprévisible. Ces technologies n'ont de sens que si elles restent au service de l'entreprise en particulier, et de la société en général dans un contrat social qui soit clairement défini. Audits interne et externe, comptes-rendus hiérarchiques clairs et réguliers, transparence à l'égard des institutions de contrôle (services déconcentrés de l'État, CNIL…) sont autant de garanties que la gouvernance de l'entreprise doit assurer pour veiller à sa propre sécurité. ■

Recommandations opérationnelles

- **Associer le secteur privé plus activement dans la rédaction des actes législatifs et réglementaires relatifs aux technologies de la sûreté. Le CDSE, représentatif, pourrait être un interlocuteur plus régulier des autorités gouvernementales et législatives.**
- **Développer les domaines de recherche et de développement en technologies de la sûreté dans un effort de partenariat public-privé en associant activement aux administrations traditionnelles et aux entreprises de sécurité, les universités et les entreprises clientes.**
- **Lancer une étude d'évaluation du coût de la sûreté qui permettrait de mieux cerner le poids des technologies de sûreté dans le chiffre d'affaires des entreprises et dans celui du PIB national.**

2 LES **MISSIONS** DE LA FONCTION SÛRETÉ

LA SÛRETÉ À L'INTERNATIONAL

JÉRÔME FERRIER

Jérôme Ferrier

Directeur sûreté
du groupe TOTAL

Ingénieur de formation, a fait toute sa carrière au sein des groupes ELF puis TOTAL, a occupé différentes responsabilités au siège ou dans les filiales du groupe à l'étranger dont celles de directeur de la zone Amériques puis de directeur général du groupe en Argentine avant de prendre la direction sûreté du groupe en 2008. Il est vice-président de l'Union Internationale de l'Industrie du Gaz.

Les événements survenus depuis le début de l'année 2011 ont fortement pesé sur les activités des entreprises françaises présentes à l'étranger, du fait notamment de leurs conséquences sur la sûreté de leurs activités ; ils appellent à l'attention de tous que la dimension sécuritaire de nos entreprises dépasse de loin les frontières de l'hexagone.

Ces crises ont un caractère exceptionnel, si l'on tient compte du nombre de pays affectés, de la diversité de leurs causes et de l'exposition politico-médiatique qui en a résulté.

Les menaces pesant sur une entreprise et son personnel se présentent sous des formes différentes qui relèvent d'une analyse spécifique. Ces menaces peuvent être à caractère terroriste, probablement les plus graves en termes de conséquences, prendre la forme de troubles à caractère politico-social ou, plus généralement, résulter d'actions criminelles allant des enlèvements avec demandes de rançons à des actes de piraterie maritime et à la cybercriminalité. Ces deux derniers types de risques, qui n'existaient pas ou peu il y a encore dix ans, sont devenus depuis lors plus complexes, et parfois plus violents. Pour chacune de ces nouvelles menaces il a fallu trouver des ripostes adaptées et conformes aux codes d'éthique et de conduite de nos entreprises, dans le respect de la légalité des pays qui y sont confrontés.

L'efficacité de la sûreté d'une entreprise est jugée à l'aune de trois critères essentiels :

La capacité d'anticipation

Elle s'appuie sur les analyses de situation des services publics français ou de consultants spécialisés. Cette capacité a été récemment mise à mal par le « printemps arabe » que personne n'a vu venir, ni dans sa composante sociale comme en Tunisie ou en Égypte, ni dans sa dimension guerrière comme en Libye. Par contre, il a été possible d'anticiper les conséquences de certaines élections en Afrique sub-saharienne (Côte d'Ivoire) ou en Asie (Thaïlande). À chaque fois, la finesse d'analyse et la rigueur dans l'interprétation des signaux faibles se sont révélées pertinentes. Une bonne compréhension au sein de l'entreprise de l'utilité de cette vigilance est indispensable.

La capacité de réaction

Celle-ci tient beaucoup à l'organisation mise en place. Dans les pays où l'insécurité sévit de manière endémique et où l'exposition de l'entreprise présente sur la scène internationale est importante compte tenu des intérêts en jeu, il est recommandé de mettre en place localement une organisation de sûreté auprès de chaque filiale. Cette organisation constituée de personnels statutaires ou contractuels est placée sous l'autorité du directeur général de la filiale ou du représentant de la société lorsque plusieurs filiales sont présentes. L'unicité de commandement pour les prises de décision de cette nature constitue une règle d'autant plus importante que toute intervention hors du territoire national peut être lourde de conséquences politiques. Mais il faut parfois également savoir faire preuve d'une capacité d'adaptation lorsque la situation l'exige, notamment lorsque la crise prend une tournure imprévue non conforme aux différents scénarios imaginés à l'avance. L'ensemble de ces éléments doit permettre de gérer les crises dans les meilleures conditions, d'autant que l'on se sera préparé à l'avance avec les interlocuteurs appropriés à la survenance de ces événements imprévus (la gestion de crise est traitée par ailleurs dans cette partie par X. Graff).

Le retour d'expérience et l'analyse post-événementielle

Ces instruments sont toujours nécessaires. Quelle que soit l'efficacité de la gestion de la crise ou l'expérience de ceux qui y sont impliqués, il est essentiel de tirer les leçons des décisions prises et des actions qui en ont résulté. La capacité d'une entreprise à évaluer de manière continue la pertinence de ses procédures internes et à mettre en place un système de management de la sûreté apte à répondre aux situations imprévues deviendra progressivement indispensable à son bon fonctionnement sur la scène internationale (le retour d'expérience sur les événements qui ont affecté le groupe Areva est traité par ailleurs dans cette partie par JM Chéreau).

Ces considérations étant prises en compte, toute société présente et active sur la scène internationale doit avoir dans son organisation une direction de la sûreté rapportant aux plus hauts échelons de l'exécutif et remplissant au moins trois missions essentielles :

- **Une mission de veille et d'analyse de la menace, indispensable pour un traitement des données adapté aux particularités de l'entreprise.** Cette mission qui aide à la compréhension des événements et à leur anticipation, doit pouvoir s'appuyer efficacement sur les services publics français compétents, notamment au sein des ministères de la Défense, de l'Intérieur et des Affaires étrangères.
- **Une mission opérationnelle organisée en autant de zones géographiques que nécessaires,** capable en situation de crise d'organiser dans les différentes filiales la protection des infrastructures mais surtout la sûreté des personnes, qui constitue la priorité absolue dans l'ordre des missions qui nous sont conférées. Cette mission de sécurisation du personnel et des installations qui est en premier lieu de la responsabilité des États dans lesquels la société exerce ses activités doit s'opérer avec le concours de responsables sûreté mis en place dans les filiales, qui doivent en particulier s'assurer des bonnes règles d'engagement des personnels militaires et civils directement en charge de leur protection, en conformité avec les codes de conduite et d'éthique de la société.
- **Une mission de protection du patrimoine informationnel, afin de garantir l'intégrité de l'entreprise contre toute forme de cybercriminalité.** Cette mission, qui contribue à la compétitivité de l'entreprise et à la pérennité de ses intérêts, s'appuie sur des réseaux de vigilance, une expertise apportée par la direction des systèmes d'information, et une politique de communication et de formation adaptée au personnel concerné. ■

Recommandations opérationnelles

- **Faire appel aux compétences des services publics français notamment dans les domaines de l'information et du conseil ; ces services doivent être en mesure de répondre aux sollicitations des entreprises.**
- **Avoir le souci d'une gestion de l'ensemble du personnel, qu'il soit expatrié ou local, même si l'on peut être amené à prendre pour chacun des dispositions différentes notamment dans les situations d'évacuation.**
- **Veiller au strict respect des règles d'éthique et de bonne conduite, non seulement par le personnel statutaire ou contracté mais également par les forces de sécurité publiques et privées qui doivent assurer la protection des personnes et des biens dans les pays où nos entreprises sont impliquées.**

L'ENTREPRISE FACE À UN ENLÈVEMENT DE SALARIÉ

JEAN-MICHEL CHÉREAU

Jean-Michel Chéreau

Directeur de la protection du groupe AREVA

Diplômé de l'ENSTA et de l'école de guerre, il participe à la montée en puissance du Commandement des Opérations Spéciales (COS). Après différentes affectations, il devient chef des opérations du COS en 1998. Après avoir dirigé différentes brigades, il est nommé directeur-adjoint de la Direction du Renseignement Militaire (DRM) avant d'être promu général de corps d'armée en août 2008, date à laquelle il rejoint le contrôle général des armées. Il est directeur de protection du groupe AREVA depuis novembre 2010.

Nuit du 15 au 16 septembre 2010 : un salarié d'Areva, son épouse et cinq salariés du groupe Vinci sont enlevés par des membres d'AQMI sur le site minier d'Arlit au Niger. Les entreprises sont sous le choc. Il faut réagir rapidement.

Dans un premier temps, en liaison avec les autorités politiques françaises, des mesures d'urgence sont prises sur place : tous les expatriés sont invités à quitter les sites miniers du nord. La quasi-totalité d'entre eux seront rapidement rapatriés en France.

Là, s'agissant d'Areva, la plupart d'entre eux seront débriefés par une équipe mise sur pied par la direction de la protection afin de tirer « à chaud » les enseignements de ce qui s'est passé et de prendre sans tarder les premières mesures correctrices qui s'imposent.

Ensuite, le groupe s'est mis en ordre de marche pour accompagner dans la durée :

- la famille de ses otages ;
- les salariés choqués par cette prise d'otages.

Il n'y a pas là de recette miracle mais les actions suivantes qui ont été déclinées se sont avérées pertinentes :

- **communication interne régulière via le réseau Intranet du groupe** en portant un effort particulier sur les dates anniversaires pour assurer, d'une part, la famille de nos otages du soutien total du groupe et de l'ensemble de ses salariés et, d'autre part, les salariés eux-mêmes que le groupe n'oublie pas (sans, toutefois, rentrer dans le détail des actions engagées) ;
- **espace ouvert sur l'Intranet afin que les salariés qui le souhaitent puissent exprimer leur soutien à la famille ;**
- **accueil à échéances régulières des membres de la famille** (en complément des réunions d'information périodiquement organisées par le ministère des Affaires étrangères et européennes) au sein du groupe pour rappeler sa présence permanente à leurs côtés et leur commenter la situation du moment lorsque cela est possible.

En parallèle, il était important de prendre toutes les dispositions pour renvoyer au plus vite les expatriés sur les sites miniers. Cela, afin de ne pas donner l'impression à l'agresseur que le groupe avait capitulé et, par ailleurs, d'assurer aux salariés nigériens (qui, en l'absence des cadres expatriés, ont fait un travail absolument remarquable) que nous ne les abandonnions pas.

Cette étape fut compliquée et douloureuse pour certains parce qu'elle a nécessairement débuté par un retour d'expérience objectif du déroulement de cette nuit de septembre 2010. Mais ce travail est absolument indispensable, voire incontournable face à une telle épreuve. Et plus tôt il est réalisé, mieux cela vaut.

Partant de là, il s'agit ensuite de :

- **mettre en œuvre toutes les mesures correctrices identifiées** dans le cadre de plans et de procédures consolidés, vérifiés et partagés avec les autorités françaises et nigériennes ;
- **mener des campagnes d'explication itératives en direction des salariés** pour leur indiquer comment va s'organiser leur protection lorsqu'ils retourneront sur place afin qu'ils reprennent confiance.

Aujourd'hui, alors que quatre des nôtres sont toujours retenus en otage quelque part dans le Sahel, les premiers expatriés du groupe sont retournés sur les sites miniers du nord du Niger dans le strict respect des documents encadrant leur retour qui seront désormais régulièrement contrôlés par des audits internes et externes selon une fréquence aujourd'hui fixée à quatre mois. Ces documents seront donc remis à jour en tant que de besoin.

Mais, au-delà de ces documents et des procédures mises en œuvre par les responsables de protection, il importe que le management et les plus anciens soient parfaitement sensibilisés à cette problématique et n'oublient plus jamais que, désormais, « le principe de primauté de la sécurité des personnes doit être intégré dans la stratégie de l'entreprise » dans les pays à risques comme le Niger. Cela signifie en particulier un changement des modes de travail et de vie, plus contraignants que ceux qu'ils ont pu connaître par le passé. Ce n'est malheureusement qu'à ce prix que leur sécurité sera assurée. ■

Recommandations opérationnelles

- **Effectuer au plus tôt un retour d'expérience afin de pouvoir mettre en œuvre sans délai les mesures correctrices nécessaires.**
- **Accompagner les familles des otages en maintenant, en liaison avec le MAEE (qui, dans ce cadre, fait un travail exemplaire), des relations régulières : la société - ou le groupe - doit dans une telle situation se comporter comme une famille…**
- **Accompagner les salariés en leur démontrant l'engagement de l'entreprise à œuvrer pour la libération de leurs collaborateurs.**
- **Échanger/dialoguer avec les salariés sur les dispositions prises pour assurer leur protection.**
- **Si l'entreprise est acteur dans la négociation avec les ravisseurs, le faire en liaison étroite avec les services de l'État, seuls aptes à éviter que se multiplient des filières de négociation qui seraient contre productives voire dangereuses.**
- **Dès lors que l'on est dans une affaire d'otages, privilégier la discrétion en matière de communication de manière à ne pas mettre à mal les négociations qui courent.**

GESTION DES RISQUES ET MANAGEMENT DES CRISES

XAVIER GRAFF

Xavier Graff

Directeur de la gestion des risques du groupe ACCOR

Directeur de la gestion des risques du groupe ACCOR depuis 4 ans. Il est en charge du développement, du déploiement et de l'animation des dispositifs de gestion des risques et des crises du groupe. Il était précédemment directeur sécurité, hygiène et santé du CLUB MÉDITERRANÉE où il a développé et piloté le dispositif de gestion de crise du groupe après avoir fait à l'étranger une grande partie de sa carrière à la direction technique. Xavier Graff est ancien auditeur de l'Institut National des Hautes Études de la Sécurité et de la Justice.

Événements dans les pays du Moyen-Orient et en Côte d'Ivoire, tsunami au Japon, tremblement de terre en Nouvelle-Zélande, crise économique mondiale, cyclone balayant la côte est des États-Unis, enlèvement de collaborateurs, toutes ces crises récentes ont démontré que les entreprises doivent faire face à des risques hétérogènes susceptibles d'impacter la sécurité de leurs clients, leurs collaborateurs ou bien encore leurs résultats ou leur réputation.

GESTION DES RISQUES

L'exposition aux risques liés à la sécurité/sûreté est de plus en plus forte et nécessite la mise en place d'un dispositif d'identification et de cartographie des risques liés aux activités de l'entreprise. Cela doit tout d'abord passer par la mise en place d'une culture du risque en son sein qui doit être insufflée par la direction générale et partagée par tous les dirigeants de l'entreprise.

La cartographie des risques est une démarche qui doit profiter à tous :

- **Pour les opérationnels,** il s'agit de mieux identifier les risques liés à l'atteinte de leurs objectifs et d'améliorer le pilotage de leur activité.
- **Pour la direction générale,** la cartographie est prise en compte dans l'élaboration du plan stratégique et l'aide à la prise de décisions. Il s'agit d'un outil de pilotage interne.

Ses risques clairement identifiés, cartographiés et hiérarchisés, l'entreprise doit mettre en place des plans d'action pour en réduire l'impact, les transférer (assurances), voire les éliminer. Cela doit lui permettre d'atteindre plus sereinement ses objectifs par une bonne anticipation des crises potentielles.

Toutes ces étapes nécessitent un important travail transversal impliquant toutes les grandes directions opérationnelles et les fonctions support de l'entreprise dont la direction sécurité au niveau du siège et des sites. Ce travail sera fortement favorisé par une culture partagée du risque.

Ce processus de cartographie doit être réalisé annuellement afin d'assurer un suivi régulier des risques majeurs auxquels l'entreprise est exposée.

Le partage des résultats avec l'audit interne doit permettre de garantir une véritable prise en compte de ces risques et de leur suivi par les propriétaires des risques.

L'environnement légal des sociétés faisant appel public à l'épargne ayant évolué ces dernières années au niveau européen, l'exercice de gestion des risques permet aussi de répondre aux nouvelles contraintes juridiques suivantes :

- Ordonnance du 8 décembre 2008 (8e directive) : encadrement du suivi de l'efficacité des systèmes de gestion des risques de la société par le Comité d'audit et des risques.
- Loi du 3 juillet 2008 (4e et 7e directives) : le rapport du président doit désormais rendre compte des procédures de gestion des risques mises en place par la société.

Pour un certain nombre de risques majeurs identifiés (inaccessibilité des sites, évacuation de collaborateurs, etc.) il sera nécessaire de rédiger des Plans de Continuité d'Activité (PCA) auxquels le directeur sécurité/sûreté devra être fortement associé.

MANAGEMENT DES CRISES

Lors d'un sondage effectué en 2010 auprès des entreprises membres du CDSE, il ressortait que 78 % de celles ayant répondu disposaient d'un département ou d'un service dédié à la gestion de crise et que dans 48 % d'entre elles, celui-ci existait depuis moins de 5 ans.

Pour 15 % d'entre-elles, c'est la direction sécurité qui pilotait le dispositif. Néanmoins, le fait que 23 entreprises participent aux travaux de la Commission Gestion de Crise au sein du CDSE, et que les nouvelles demandes de participation affluent, témoignent d'une implication grandissante des directions de sécurité sur ce sujet. 63 % des entreprises avaient de fortes attentes en matière de diffusion de bonnes pratiques et 21 % souhaitaient travailler sur une meilleure coordination des accès aux contacts des pouvoirs publics.

Ce processus, qui lui aussi doit avoir le soutien de la direction générale, doit se construire en plusieurs phases :

- création des outils (manuels de gestion de crise, fiches réflexes, pocket-mémo, logiciel informatique de communication et de coordination) ;
- mise en place d'un réseau interne de coordinateurs de crise ;
- mise en place d'un dispositif de veille et de réponse téléphonique H24 ;
- identification et formation des membres des cellules de crise ;
- réalisation de la carte des acteurs (ressources internes, partenaires, institutions, médias, environnement, etc.) ;
- réalisation d'exercices.

Au sein de la cellule de crise, on trouvera un noyau d'acteurs incontournables issu des ressources humaines, de la communication, de la direction juridique, voire dans certains cas des assurances en fonction de la nature de la crise.

Dans toutes ces étapes, il est souhaitable que l'entreprise puisse être accompagnée par un intervenant externe qui pourra également apporter une aide pendant la crise et lors du retour d'expérience.

En raison de la complexité des nouvelles crises, celles-ci ne peuvent plus être gérées seulement par l'entreprise. L'interaction avec d'autres sociétés (clients, fournisseurs, prestataires) et les pouvoirs publics devient alors indispensable. Cela nécessite tout un travail d'anticipation qui doit être réalisé en « temps de paix » pour créer les liens entre les différents acteurs, partager les procédures et, si possible, réaliser des exercices de crise en commun.

Ce travail de partenariat public - privé sur la gestion de crise dans lequel le CDSE s'est engagé depuis 2008 en participant activement à la rédaction du document *« Maîtrise des risques et des crises : une réflexion croisée »* sous l'égide de l'INHESJ (un document du groupe de travail partenarial public-privé, ou GT3P, sur l'approche commune des crises) démontre l'importance du sujet et doit continuer à être un axe de travail important. La convention signée en 2009 entre le CDSE et le CDS (Centre De Crise) du ministère des Affaires étrangères et européennes doit être davantage développée avec les autres ministères de tutelle des grandes entreprises françaises (Intérieur, Défense, Environnement, Finances, Industries, Santé, Transports, etc.).

Afin de permettre également aux directeurs sécurité/sûreté des entreprises de correspondre de manière privilégiée avec les différents services français et d'accéder plus rapidement à des informations, il serait souhaitable que ceux-ci puissent bénéficier d'une accréditation « Confidentiel Entreprise». Cela leur offrira une étape d'avance en début de crise afin de gérer celle-ci le plus efficacement possible et de mieux protéger l'entreprise, ses collaborateurs et ses clients. ■

Recommandations opérationnelles

- **Faire évoluer la fonction de directeur sécurité/sûreté en l'impliquant dans la gestion des risques et des crises.**
- **Développer de nouveaux partenariats public-privé entre le CDSE et les ministères de tutelle des grandes entreprises françaises.**
- **Création par les pouvoirs publics d'une accréditation « Confidentiel Entreprise » pour les directeurs sécurité/sûreté.**

LA LUTTE CONTRE LA FRAUDE

NADIA CHELGHOUM

Nadia Chelghoum

Directrice sûreté
d'AXA FRANCE

Entrée à l'École Nationale Supérieure de Police de Saint-Cyr au Mont-d'Or en 1989-1990, elle a exercé successivement les fonctions de commissaire de police à la sécurité publique de Saint-Étienne, commissaire de police de Vauls-en-Velin et de Lyon, et en 2001 au cabinet du secrétaire général de la mairie de Paris chargée des questions de sécurité. En 2003, elle est nommée directrice sûreté chez AXA.

“ Chez nous aucun risque, nous sommes une petite entreprise familiale, on se connaît tous. Avec mon dispositif de contrôle interne, impossible de frauder. ”

Quel directeur de sûreté, aussi modeste soit-il, n'a pas entendu ce type de réflexion alors même qu'il essayait en vain de convaincre les dirigeants de son entreprise de lui donner les moyens de lutter contre la fraude. Le risque traditionnel lié à la fraude - dont la plus classique est le détournement d'actifs - est une réalité reconnue par beaucoup aujourd'hui. La crise économique a accentué l'impact de ce type de comportement frauduleux dans tous les domaines de la vie économique et il devient prioritaire pour l'entreprise de s'y investir afin de préserver son image et son patrimoine.

RECONNAÎTRE LA FRAUDE

Pourtant, il n'est pas rare que les entreprises oscillent entre déni, inconscience ou choix délibéré de ne pas s'investir dans un sujet qui rapporte peu. En effet, quel est l'intérêt d'investir dans une politique à long terme pour lutter contre la fraude alors que le préjudice financier causé par sa réalisation sera toujours moins important ? **Reste que la quantification de l'impact réel et des économies réalisées par une politique de lutte efficace s'avère bien souvent difficile par un manque d'outils adaptés.**

De même, la fraude reste un sujet tabou qui incite certaines entreprises à ne pas faire preuve de transparence, entre crainte des conséquences médiatiques d'une fraude révélée (notamment au sein des organismes financiers) et volonté de ne pas révéler les faiblesses de son organisation ou de sa gestion des hommes.

L'origine de la fraude peut être externe à l'entreprise (émanant de clients, de partenaires économiques ou commerciaux) mais également provenir de l'intérieur de l'entreprise (comportement frauduleux de ses propres représentants ou collaborateurs). Nous allons plutôt orienter nos recommandations vers la fraude interne, dont les conséquences en termes d'atteinte à l'image sont bien plus préjudiciables pour l'entreprise.

Reconnaître l'existence même de ce type d'incident et l'assumer en toute transparence est un préalable non négociable à la mise en place d'un service dédié à la lutte contre la fraude au sein d'une direction sûreté connue et reconnue. De même, la transparence doit s'imposer dans l'élaboration et la diffusion d'une politique de lutte contre la fraude, qui soit simple et compréhensible par tous. Cette politique doit intégrer l'identification de la fraude, son traitement, l'investigation sur les auteurs éventuels, le déclenchement des procédures internes de sanction et la saisine des autorités de police et de justice compétentes s'il y a lieu.

UN DISPOSITIF AVANT TOUT DISSUASIF

La peur du « gendarme » reste selon nous un facteur clef de la prévention de la fraude dans l'entreprise. La conduite de l'enquête, la recherche et l'obtention de preuves de l'existence d'une fraude ainsi que de l'identification de son auteur se doivent d'être réalisées dans un cadre strictement légal et objectif. Ainsi, la collecte d'informations financières publiques et librement accessibles, l'analyse de transactions, des flux financiers dans le cadre notamment de fraude financière peuvent être des sources d'information non négligeables et conformes aux droits des salariés mais également de la société qui est propriétaire de ces données.

La veille générale tant sur les réseaux que par le biais d'Internet ou les vérifications sur différentes banques de données disponibles et ouvertes constituent un premier niveau d'une vigilance générale. L'utilisation d'outils performants de contrôle interne et de détection de la fraude basés sur l'analyse de données permet d'anticiper le risque le plus en amont possible.

Le déploiement d'investigations très rapides, à charge et à décharge, permettent de rassembler les preuves nécessaires et d'identifier l'auteur afin d'aboutir à l'ouverture d'une procédure disciplinaire et pénale le cas échéant. Pour ce faire, les collaborateurs dédiés à cette mission seront formés à l'investigation et à la conduite de l'enquête dans le strict respect du code de déontologie et de la législation du droit du travail en vigueur. Toutefois, le service chargé de l'enquête n'est pas décideur en dernier ressort. Les RH et la direction juridique sont également parties prenantes de l'ensemble de la procédure dans l'intérêt de l'entreprise et des salariés.

Parmi les outils déployés, l'instauration d'une charte ou d'un code éthique et de déontologie est un bon moyen de protéger l'entreprise contre les risques de fraude ou de vol mais également contre tout comportement contraire à la loi. Cette charte se doit d'être accompagnée d'un dispositif d'alerte professionnelle adapté à la législation en vigueur permettant à chacun de remonter tout incident ou alerte pouvant s'assimiler à un risque de fraude éventuel. La prise en charge le plus en amont possible de ce type de risque engendre un impact financier et humain minimum.

Pareille charte doit être accompagnée d'un plan de sensibilisation de l'ensemble des managers de l'entreprise. Une communication appropriée à propos de la politique déployée s'avère indispensable pour construire une culture du risque partagée par l'ensemble des collaborateurs, qui soit réaliste et bénéfique. À titre d'exemple, le fait d'alerter sur les sanctions encourues, d'évoquer la mise en œuvre systématique d'une procédure disciplinaire interne pouvant conduire au licenciement, voire à la saisine des autorités judiciaires, joue un rôle dissuasif certain.

Le dépôt de plainte n'a pas pour seule vertu d'être dissuasif, il peut également s'avérer indispensable pour instaurer une exemplarité. Il est tout autant nécessaire à la protection du marché économique et financier qui pâtit de ces fraudes. Cette démarche permet enfin aux entreprises de profiter du savoir-faire d'experts enquêteurs et de bénéficier de pouvoirs d'investigation de puissance publique. Le recours à des prestataires de sécurité privée se révèle parfois nécessaire mais il doit être strictement encadré afin de ne pas contrevenir aux règles déontologiques et aux dispositions légales.

La lutte contre la fraude, c'est l'affaire de tous. Elle requiert l'appui des autres directions de l'entreprise concernées par ce risque : les RH, la direction juridique, la communication, la direction financière, le *risk manager*, etc. Elle demande également une véritable collaboration avec les services de l'État, ceci dans l'intérêt des décideurs publics comme privés.

La construction d'une éthique d'entreprise ne s'avère pas coûteuse pour l'entreprise. En retour, elle se présente sur le long terme comme un rempart utile contre les risques de fraude. ■

LA PROTECTION DE L'INFORMATION

CYRIL NGUYEN - JEAN-PIERRE VUILLERME

Cyril Nguyen

Directeur sûreté, sécurité, prévention des pertes du groupe CRÉDIT AGRICOLE

Âgé de 42 ans, membre du conseil d'administration du CDSE. Il est auditeur de la 21e INHESJ. Diplômé d'un Master II d'information et sécurité de l'Université de Marne-la-Vallée. Actuellement directeur sûreté, sécurité, prévention des pertes du groupe CRÉDIT AGRICOLE, il fut directeur sûreté de NESTLÉ FRANCE et manager sûreté et prévention des pertes de TECH DATA France. Il a passé 14 années dans un bureau spécialisé du ministère de la Défense.

La protection de l'information stratégique est encore un sujet de préoccupation réservé aux initiés, alors que l'efficacité opérationnelle des moyens de protection repose pour une large part sur la compréhension des enjeux par tous les acteurs de l'entreprise, quel que soit leur niveau hiérarchique. **Le facteur humain, en effet, apparaît toujours déterminant dans l'analyse des causes des fuites d'information (souvent non intentionnelles) : il doit donc retenir toute notre attention.**

APPROCHE DIRIGISTE OU APPROCHE CANDIDE ?

Devant ce constat, la tentation est forte d'établir et d'imposer un corpus de règles internes contraignantes (classification des informations, dispositions de protection, durée d'archivage, processus de destruction…), assorties de sanctions lourdes lorsqu'elles ne sont pas respectées. **Cette approche « dirigiste » a cependant peu de chances d'être efficace dans la durée sans une adhésion forte du personnel, qui passe par une bonne compréhension des enjeux.** Observons que nous agissons là dans un domaine peu réglementé (mais avec une jurisprudence assez défavorable) en attendant qu'une législation claire voit le jour en ce qui concerne la protection des informations confidentielles de l'entreprise (projet du député Bernard Carayon).

Une autre approche, sans doute plus « candide », consisterait à obtenir que chaque collaborateur de l'entreprise adapte, naturellement et sans contrainte, son comportement à ces enjeux. Il faudrait pour cela que chacun ait la capacité à identifier le caractère stratégique de l'information qu'il utilise, et à protéger de façon efficace des informations de plus en plus souvent « dématérialisées ». Le résultat serait pour le moins incertain d'autant que le sentiment d'appartenance à l'entreprise n'est pas toujours au niveau que l'on pourrait souhaiter !

Jean-Pierre Vuillerme

Directeur du management des risques de l'ADIT

Docteur-ingénieur. Débute sa carrière comme enseignant-chercheur à l'Université pendant 4 ans. Rejoint le groupe MICHELIN en 1972, groupe dans lequel il exerce différentes fonctions (responsable industrialisation, recrutement ingénieurs et cadres, directeur de la communication et des affaires publiques et enfin directeur des services Environnement et Prévention des risques du groupe et directeur sécurité du groupe avant de prendre sa retraite fin 2009). Rejoint l'ADIT en janvier 2010 pour créer le Centre français des affaires de Bagdad et devient directeur du pôle management des risques.

La réponse efficace se trouve sans doute dans la recherche d'un équilibre entre ces deux extrêmes. Encore faut-il que le *top management* soit lui-même convaincu de la nécessité de développer une véritable culture « sûreté » dans l'entreprise et le démontre au quotidien ! Et il s'agit là d'un exercice difficile tant les fuites d'information (conduisant dans la plupart des cas soit à des pertes de marché soit à des atteintes à l'image de l'entreprise, de ses produits ou de ses dirigeants), comme d'autres sujets sensibles tels que la fraude par exemple, sont encore tabous dans nos entreprises !

UNE RÉPONSE ADAPTÉE AUX ENJEUX

Confortablement installés à l'abri derrière des codes d'éthique ou des codes de conduite des affaires, **certains dirigeants considèrent trop souvent que les manoeuvres délictueuses qu'ils s'interdisent ne peuvent exister de la part de la concurrence.** De plus, ils n'ont pas toujours pris conscience que l'organisation du tissu industriel (la plupart des entreprises concurrentes opérant dans une même filière sont totalement interconnectées par le même réseau de sous-traitants ou de fournisseurs de matières premières notamment) et la nomadisation des systèmes d'information (PC portables, Smartphones, etc… qui permettent à tous les collaborateurs de rester en permanence « connectés » à l'entreprise) bousculent, à la fois les limites géographiques de l'entreprise et les limites temporelles séparant le professionnel du privé. C'est ainsi que des ordinateurs personnels sont fréquemment utilisés à des fins professionnelles et qu'ils peuvent contenir de ce fait des données sensibles appartenant à l'entreprise… sans que l'on ait songé, ou eu la possibilité, de mettre en place sur ces outils des moyens de protection adaptés.

Quant aux relations dites « sociales », elles sont la source de fuites importantes : il est fréquent d'entendre des conversations touchant à des projets confidentiels en prenant les transports en commun, ou au café situé en face de la porte du siège de l'entreprise. Sans oublier les « réseaux sociaux » dont la fréquentation à partir de son domicile donne l'illusion d'être dans sa sphère privée alors que l'on a rejoint la sphère publique…

Comme on le voit, le risque de fuite d'information est multiforme et les canaux sont multiples.

Face à ce constat, il est indispensable d'envoyer un message clair à l'ensemble des acteurs de l'entreprise, en évitant le jargon technique et en se focalisant sur les conséquences d'une perte d'informations stratégiques : c'est bien l'emploi qui est menacé et, dans certains cas, la pérennité même de l'entreprise. Ce message doit être porté par les plus hautes instances de l'entreprise, dont le comportement à cet égard se doit d'être exemplaire.

La mission du directeur sûreté devient alors légitime : il n'est pas seulement celui qui établi la règle - souvent contraignante - en ce qui concerne la mise en place des dispositions et dispositifs de protection, il est aussi le principal acteur des actions de sensibilisation qui auront pour conséquence de développer une motivation suffisante chez l'ensemble des personnels.

Dans ce domaine, le recours aux organismes institutionnels tels que la DCRI ou la Gendarmerie, suivant leur zone de compétence, est extrêmement efficace pour au moins deux raisons. En premier lieu, un message est d'autant mieux écouté et compris lorsqu'il provient d'un expert extérieur qui, de surcroît, représente l'État. En second lieu, ces sensibilisations ne se limitent pas à donner des conseils utiles dans la vie professionnelle, ils abordent aussi largement les risques de mauvais comportements et leurs conséquences dans la vie personnelle. C'est ainsi que des opérations « d'ingénierie sociale », des détournements, des actes de prédation sexuelle... ont été facilités par les bavardages des internautes sur leur vie personnelle sur les réseaux sociaux (adresse, hobbies, départs en vacances, lieux visités...). **La sensibilisation devient alors très efficace par l'écho qu'elle trouve dans la vie personnelle de chacun.** Ces formations sont désormais très prisées des entreprises qui doivent s'armer de patience pour en bénéficier. Le projet récent de labellisation de conférenciers en sécurité économique active conduite par le D2IE et l'INHESJ (projet Euclès) offrira une solution alternative. Notons, non sans chauvinisme, qu'à ce jour seules les autorités françaises produisent ce service pour les entreprises privées !

Dans un second temps, il convient d'organiser de façon récurrente des sessions internes à l'entreprise, centrées sur ses risques spécifiques et en les étayant, si possible, d'exemples vécus. Ces formations doivent être très interactives et auront pour finalité de démontrer la pertinence des moyens de protection mis en œuvre par l'entreprise (mise à disposition de moyens dédiés pour les voyageurs, logiciels d'effacement des données, destruction des disques durs des photocopieurs avant leur départ en maintenance ou en réforme...). Des jeux de rôles (tour à tour attaquant et défenseur) sont aussi de bons moyens pédagogiques pour démontrer combien il est facile de capter de l'information stratégique qui bien souvent est transmise involontairement dans des lieux publics ou par des techniques simples d'ingénierie sociale, de faux appels d'offres ou de faux entretiens de recrutement.

Enfin, un support documentaire rappelant les grands principes (souvent basés sur le bon sens) assortis de didacticiels en ligne, permet de compléter le dispositif de sensibilisation. Bien entendu, n'oublions pas les quelques opérations de contrôle (bureau rangé ou « clean desk » par exemple) nécessaires pour entretenir la conscience collective. ■

LA PROTECTION DES INFRASTRUCTURES CRITIQUES

JEAN-MARC SABATHÉ

Jean-Marc Sabathé

Directeur sécurité
du groupe EDF

Formé au commissariat de la Marine nationale, passé par les cabinets ministériels et les collectivités locales, lui-même élu local et secrétaire général d'un parti politique dans les années 90, Jean-Marc Sabathé a créé le porte-parolat du Ministère de la Défense avant de devenir sous-préfet en 1999 en occupant plusieurs postes en métropole et outre-mer, puis administrateur civil au ministère de l'Intérieur où il fut chef du bureau des officiers de police à la DAPN de 2004 à 2007. Il est depuis, en service détaché, directeur sécurité d'EDF.

La protection des infrastructures critiques est au cœur de la préoccupation de l'État et des grands opérateurs publics et privés. Le concept évolue cependant de la lutte contre la malveillance et le terrorisme, vers une approche multirisques prenant en compte les capacités de résilience de la Nation en cas de crise grave.

Dans un contexte de forte évolution des menaces, notamment terroristes, au début des années 2000, naît en France en 2006 le dispositif des Secteurs d'Activités d'Importance Vitale (SAIV), intégré au code de la défense. L'État s'engage alors dans une démarche de planification, en y associant les opérateurs sur lesquels pèsent de nouvelles obligations.

Ainsi, *« les opérateurs (...) sont tenus de coopérer à leur frais à la protection desdits établissements (...) »* (article L 1332-1 du code de la défense).

Les activités d'importance vitale sont réparties en 12 secteurs (transports, énergie, santé...). Chaque ministère coordonnateur d'un secteur fixe dans une Directive Nationale de Sécurité (DNS) les objectifs de protection souhaités et les *scenarii* de menaces susceptibles de se réaliser. Chaque entreprise, désignée comme Opérateur d'Importance Vitale (OIV), doit présenter un Plan de Sécurité Opérateur (PSO), document unique qui est sa réponse aux prescriptions de l'État.

Chaque OIV propose alors avec son PSO une liste de Points d'Importance Vitale (PIV) qui sont les établissements, installations ou ouvrages nécessitant une protection particulière.

Enfin, chaque PIV se voit doté par l'entreprise d'un Plan Particulier de Protection (PPP) qui est approuvé par le préfet du département concerné, qui à son tour doit préparer un Plan de Protection Externe (PPE).

UNE IMPLICATION FORTE DU DIRECTEUR SÛRETÉ

C'est sur le directeur sûreté que va peser l'essentiel du travail de coordination et de rédaction du PSO et des PPP. Cela suppose une grande capacité à assimiler les exigences de l'État, réunir les métiers concernés par les installations à protéger, mobiliser des capacités d'ingénierie, réévaluer les analyses de risques, repenser les schémas d'organisation, notamment en gestion de crise, réfléchir au dimensionnement et à la pertinence des dispositifs de sécurité, vérifier la bonne mise en œuvre du plan Vigipirate, enfin étudier les interdépendances avec d'autres opérateurs pour apporter des réponses coordonnées visant une capacité de résilience dans la durée.

Les contraintes sont financièrement lourdes. Les menaces et les *scenarii* sont toujours susceptibles d'être revus à la hausse, poussant au réexamen des dispositifs.

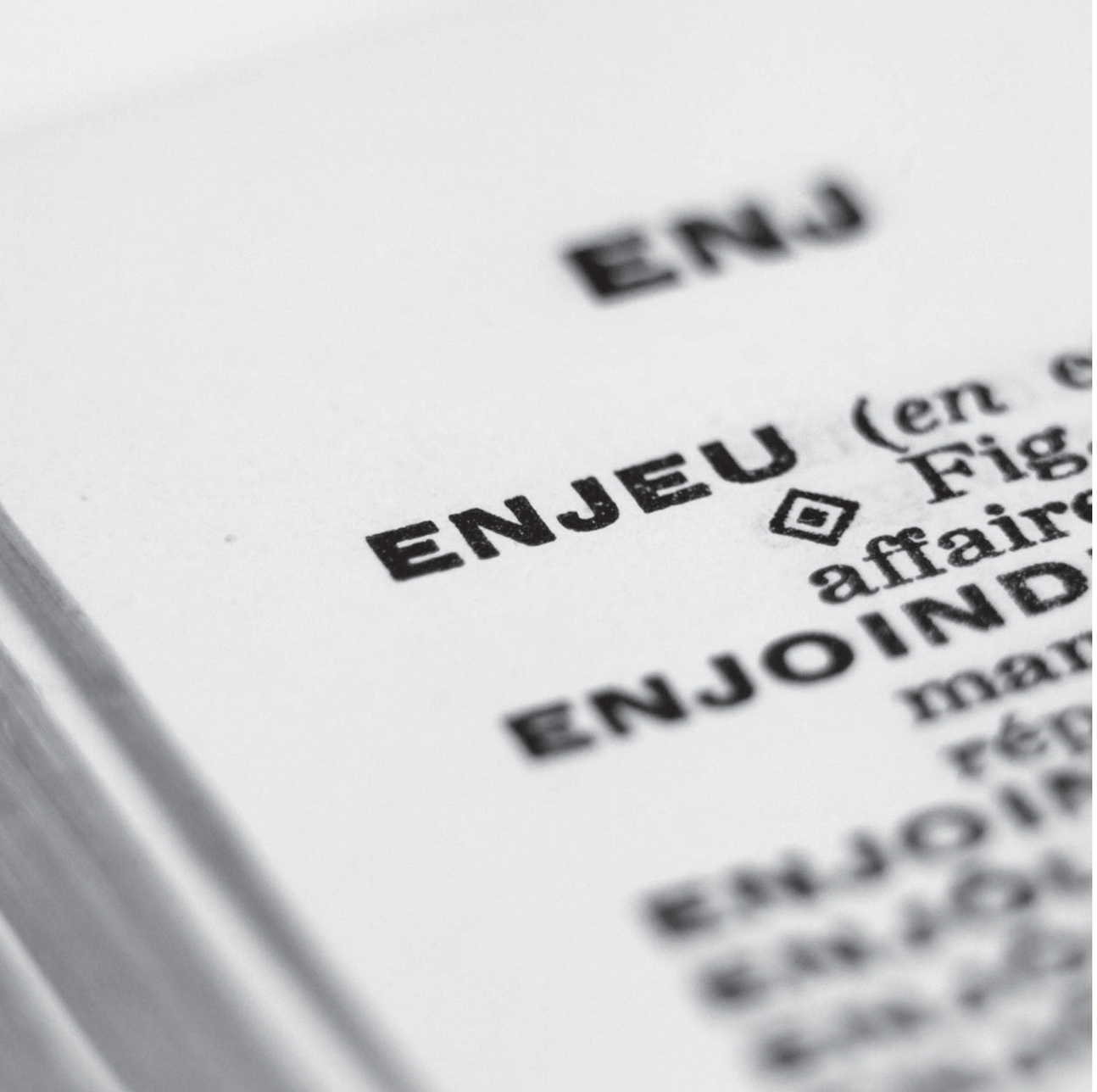
UNE APPROCHE DE PLUS EN PLUS INTERNATIONALE ET MULTIRISQUES

On constate deux évolutions notables. Si les États restent légitimes à évaluer eux-mêmes les menaces, et à adopter les réglementations nationales pour y faire face, les instances internationales, notamment l'Union Européenne, ont tendance à vouloir s'emparer de la question. C'est ainsi que la directive européenne de décembre 2008 sur la sécurité des infrastructures critiques traite des ouvrages transfrontaliers. L'UE souhaite dans l'avenir aller plus loin (réglementation européenne, référentiels communs, gestion de crise…).

Enfin, avec la multiplication d'événements climatiques majeurs, et singulièrement la catastrophe nucléaire au Japon en 2011, les États souhaitent faire évoluer leurs dispositifs de planification de lutte contre le terrorisme vers une approche « multirisques », avec la volonté de s'assurer des capacités de résilience des administrations et des principales activités économiques. La planification a de beaux jours devant elle ! ■

Recommandations opérationnelles

- **L'État doit améliorer son approche interministérielle pour mieux appréhender les interdépendances entre secteurs économiques. Il doit s'efforcer de stabiliser le processus pour donner de la visibilité aux entreprises.**
- **Le directeur sûreté doit avoir un positionnement corporate et avoir le soutien de la direction générale lui permettant de mobiliser les énergies et de surmonter les obstacles.**
- **Le directeur sûreté doit faire procéder aux évaluations financières et mesures d'impacts indispensables à la réussite de la démarche et à son acceptabilité.**



3 LES NOUVEAUX **ENJEUX** DE LA SÛRETÉ

LA PROTECTION DE L'INFORMATION

GUILLAUME CAPOIS - PHILIPPE DULUC

Guillaume Capois

Directeur sûreté du groupe EADS

Diplômé de l'École Spéciale Militaire de Saint-Cyr, il occupe successivement différentes fonctions opérationnelles dans des unités parachutistes et de forces spéciales puis de renseignement. Après un séjour en ambassade, il revient en France et dirige la DSIRP (Direction de la Sécurité Industrielle en Région Parisienne) et devient membre du Groupe Permanent d'Intelligence Économique (GPIE) du Haut responsable à l'Intelligence Économique Alain Juillet. En 2007, il rejoint le groupe EADS dont il est le directeur sûreté.

L'environnement dans lequel évoluent les entreprises s'est profondément modifié au fil des ans. La gestion des informations, leur partage en temps réel au sein d'une entreprise « étendue », œuvrant dans un cadre mondial, et dans un contexte d'indispensable réactivité, a rendu l'usage intensif des systèmes d'information incontournable. Parallèlement, la multiplication des systèmes et des outils a transformé les méthodes de travail, jusque dans les actions les plus courantes, conduisant en outre à rendre floues voire perméables les frontières entre vies privée et professionnelle.

Dans un environnement de très forte compétitivité où la déontologie et le respect des lois sont transgressés par certains, les menaces sur l'intégrité des informations sont d'autant plus importantes et nombreuses que les technologies et méthodologies qui les supportent évoluent en permanence en étant, pour certaines, accessibles facilement sur le net.

TYPOLOGIE DES MENACES

Les principaux attaquants peuvent se regrouper en trois ensembles qui parfois interagissent entre eux :

- des organismes supportés par des structures étatiques.
- des concurrents agissant directement ou au travers de sociétés « spécialisées » voire en relation avec le crime organisé ;
- des « hackers » à la recherche de notoriété, motivés par une idéologie ou encore agissant par « opportunité ».

Philippe Duluc

Directeur de l'activité sécurité du groupe BULL

Diplômé de l'École Polytechnique, ingénieur de l'armement, il assure d'abord des responsabilités opérationnelles en cryptographie, puis devient chef de département au ministère de la Défense jusqu'en 1999, il est alors nommé conseiller du secrétaire général de la défense nationale, en charge des affaires scientifiques et techniques. En 2003, il met en place la direction de la sécurité du groupe FRANCE TÉLÉCOM ORANGE qu'il dirige jusqu'en 2011. Aujourd'hui directeur de l'offre sécurité de BULL, il exerce également la fonction de directeur sécurité groupe. Il préside le groupe permanent cybersécurité de l'Alliance pour la Confiance Numérique (ACN).

Les attaques ont évolué en dangerosité, en complexité et en taille et sans être exhaustif se traduisent en général par des :

- vols de données personnelles (numéros de carte bancaire…) motivés par la cupidité (escroquerie, fraude, spam, chantage…) ;
- atteintes ciblées à la disponibilité ou l'intégrité des systèmes (défiguration ou saturation de sites…) avec une motivation idéologique (« Anonymous »…) ;
- attaques ciblées et sophistiquées visant à voler de l'information sensible (attaque de type APT ou Advanced Persistant Threats), motivées par l'espionnage économique ou stratégique ;
- cyberattaques visant à endommager des équipements ou à perturber voire neutraliser des productions ou des services (attaque des centrifugeuses nucléaires iraniennes en 2009 par l'utilisation du ver Stuxnet).

Les actualités de ces derniers mois ont montré l'ampleur et la fréquence de ce type d'attaque, même si la réalité est très certainement plus importante encore, de nombreuses victimes évitant d'ébruiter leur cas, ou pire encore, ignorant qu'elles sont attaquées.

QUELLES SOLUTIONS ?

Face à ces menaces, certains axes de progrès peuvent orienter l'action des structures de sécurité. Il s'agit de replacer la sécurité de l'information au cœur des préoccupations, des projets et des actions des acteurs de tous les niveaux de l'entreprise, tout en lui donnant les moyens de conduire une politique adaptée.

En premier lieu, assurer une approche globale de la sécurité de l'information en définissant une gouvernance claire, garantissant une liberté d'appréciation et de jugement sur les préconisations et les choix des solutions, et en veillant à préserver une cohérence dans la protection de l'information. Pour ce faire, la sécurité des systèmes d'information doit être partie intégrante de la direction sûreté, en charge non des architectures et des opérations de sécurité pilotées par la DSI (Direction des Systèmes d'Information), mais de la définition des spécifications et des contraintes à

prendre en compte, puis de la validation des solutions et enfin de la réalisation des audits. Cette organisation assure une meilleure homogénéité de la sécurité (physique, logique et humaine) et permet d'éviter tout conflit d'intérêt. Pour conduire efficacement son action, les budgets alloués à la sécurité ne doivent pas être la variable d'ajustement des coûts informatiques, les récentes attaques ayant rappelé les lourdes conséquences directes et indirectes induites par une attaque réussie.

En second lieu, face à ces menaces multiformes et permanentes, la sécurisation centrée sur la seule protection de type périphérique est devenue obsolète. Elle doit être remplacée par une défense en profondeur, doublée d'une capacité de détection et de traitement d'une attaque sophistiquée. Il ne s'agit plus de se reposer sur une « Muraille de Chine » mais de construire une protection dans la profondeur (ségrégation, chiffrement, authentification forte, preuve…) en se dotant d'une capacité à détecter et analyser une attaque lorsque celle-ci a réussi à pénétrer le système, pour mieux la gérer et l'éradiquer. Les créations d'un SOC (Security Operation Center) et d'une structure de type CERT (Computer Emergency Reaction Team) sont indispensables pour améliorer la réactivité et les savoirs-faire dans ces domaines, capitaliser les expériences, entretenir un réseau d'experts internes et externes pour confronter et échanger, et enfin collaborer avec les structures étatiques dédiées (ANSSI).

Enfin, il faut replacer l'individu et les utilisateurs au centre du système, comme acteurs principaux de la sécurité des informations. La mise en œuvre d'un plan de sensibilisation ciblé, récurrent et personnalisé, permet de créer une motivation et un éveil suffisant pour éviter les pièges et les imprudences les plus courants (phishing, usurpation, réseaux sociaux…), provoquer les rapports d'étonnement, et une réactivité à la remontée d'incidents. Une politique claire de responsabilisation doit en outre être mise en place (charte opposable, objectifs, évaluation…). Toute mise en place de nouveaux projets ou de modifications des systèmes d'information (outils, architecture, logiciels, externalisation, off shoring…) doit faire l'objet d'une procédure incluant la structure de sécurité.

Il n'existe pas de protection parfaite et la modestie, la vigilance et la remise en cause permanente des solutions choisies doivent prévaloir. La recherche permanente d'amélioration de l'existant et son adaptation à l'évolution incessante des menaces passe notamment par la mise en œuvre à tous les niveaux de boucles vertueuses de type PDCA (Plan-Do-Check-Act) et par la mise en place d'un plan de sécurité pluriannuel glissant, réactualisé annuellement, impliquant l'ensemble des acteurs (IM, opération, finances, RH…) et légitimé par une validation du plus haut niveau de l'entreprise. ■

LA SÉCURITÉ ÉCONOMIQUE DES ENTREPRISES

Bernard Galéa

Directeur sûreté
et de l'intelligence stratégique
du groupe FM LOGISTIC

Diplômé d'un Master II en Gestion Globale des Risques et des Crises (Paris 1 - Sorbonne) et de plusieurs certificats en management opérationnel de l'ESSEC Business School en analyse financière, Bernard Galéa a effectué une première partie de carrière au sein de l'aéronautique navale, puis a été détaché durant plus de 17 ans aux ministères de la Défense et des Affaires étrangères. Alternant des postes en administration centrale et dans de nombreux pays à l'étranger. Il rejoint le groupe FM LOGISTIC en janvier 2008 sur la fonction de directeur sûreté du groupe. Après avoir structuré cette direction, ses fonctions sont alors élargies à l'intelligence stratégique. Nommé directeur sécurité 2010 lors des derniers trophées de la sécurité privée, il prend la présidence de l'ASIS pour la France la même année.

Le monde est en plein bouleversement. Nous vivons de manière quasi simultanée des conflits armés persistant, un « printemps arabe » dont la propagation et les conséquences restent encore imprévisibles, un tsunami au Japon qui ébranle les certitudes de sûreté nucléaire, immobilise les chaînes de production et menace la santé publique régionale voire mondiale, et une crise financière à rebond qui ne cesse de modifier les rapports de forces entre les pays.

L'évolution de l'économie mondiale et la globalisation ont eu et continuent d'avoir des conséquences géopolitiques et géoéconomiques qui renforcent la concurrence commerciale sur tous les continents. Comme le soulignait si justement Bernard Carayon, député du Tarn, lors de la conférence des ambassadeurs à Paris le 26 août 2004, paraphrasant Diderot : « *Sans la 'dépravation des hommes', nous n'aurions pas à craindre la guerre économique, cette 'maladie compulsive et violente du corps' économique et nous pourrions accomplir 'notre état naturel' en jouissant de la paix économique…* ». L'actualité quotidienne démontre qu'il n'en est rien.

Dans ce contexte, les entreprises doivent continuer à saisir les opportunités de développement et, surtout, comprendre les menaces portant atteinte au patrimoine économique de l'entreprise ; celles dites classiques (espionnage industriel, pillage technologique, etc.) ou et celles plus récentes (cybercriminalité, désinformation, etc.). La pratique de l'intelligence économique (ou intelligence stratégique) permet cette approche : *« l'intelligence*

économique consiste en la maîtrise et la protection de l'information stratégique pour tout acteur économique. Elle a pour triple finalité la compétitivité du tissu industriel, la sécurité de l'économie et des entreprises et le renforcement de l'influence de notre pays » précise Alain Juillet dans son référentiel de formation en Intelligence Économique. Sur un plan opérationnel, cette approche ne saurait dissocier sécurité économique, recherche et partage d'informations (veille, réseaux d'experts et communautés de pratiques) et lobbying (en tant que pratiques d'influence auprès des décideurs publics et privés).

L'évolution de ces menaces et leur prise en compte supposent la nécessaire adaptation de la fonction sûreté dans les entreprises. S'il est désormais acquis que le directeur sûreté doit être positionné au plus haut niveau des organisations, voire dans les Comex, les bons directeurs sûreté doivent par leurs actions contribuer aux objectifs commerciaux de leur entreprise. **Nos amis outre atlantique ont déjà parfaitement intégré ce paramètre dans leur organigramme en transformant cet « homme sûreté » en « VP Insight », notion qui pourrait se traduire par directeur de la sûreté et de l'intelligence stratégique.** Il ne s'agit pas là de définir la stratégie de l'organisation mais bien de l'accompagner en l'éclairant et en la protégeant (voir à cet effet les travaux du professeur Jonathan Calof, de l'université d'Ottawa).

Au-delà des enjeux classiques tels que la mise en sûreté des sites et la sécurité des salariés à l'étranger, cette fonction doit également participer pleinement à la sécurité économique pour se protéger :

- de l'espionnage industriel et du pillage technologique ;
- des risques informationnels (rumeurs, désinformation, sous-information, attaque de l'image, la e-réputation) ;
- des risques commerciaux et concurrentiels (contrefaçon, risque client, risques concurrentiels, débauchage de salariés disposant de savoirs-faire ou d'informations-clés etc.) ;
- de la criminalité économique organisée (blanchiment, corruption, paradis fiscaux, organisations criminelles). À ce titre, la mise en place d'une charte d'éthique appuyée sur un système légal d'alertes professionnelles renforce la sécurité de l'organisation ;
- de la cybercriminalité (piratage, virus, etc.) ;
- des risques géopolitiques et sociétaux (évolutions sociétales et technologiques, impact économique du terrorisme, etc.) ;
- des risques liés aux fusions et acquisitions : c'est-à-dire la nécessité d'avoir une analyse poussée du risque pays (« savoir où je mets les pieds »), acquérir des informations fiables - probantes, validées et recoupées - sur un futur partenaire local (« savoir à qui j'ai réellement affaire »), identifier un réseau d'appui local (« ne pas agir seul sans appui fiable »). L'intérêt est d'apporter, lors de la *due diligence* stratégique, tous les éléments pertinents à l'éclairage des prises de décisions. ■

Recommandations opérationnelles

- **Faire voter et publier par le parlement la loi sur « le secret des affaires » et reconnaître dans son corollaire l'existence du timbre « confidentiel entreprise ».**
- **Porter celle-ci à un niveau européen afin d'harmoniser/ réglementer les pratiques des entreprises.**
- **Promouvoir la collaboration public-privé avec notamment un meilleur engagement des services de l'État dans le soutien au développement économique des entreprises.**
  Cela passe nécessairement par une égalité de traitement des entreprises dans l'accès aux informations économiques auprès des services spécialisés.
- **Favoriser le développement du CDSE à l'échelle européenne à l'instar de l'International Security Management Association (ISMA) ou de l'American Society for Industrial Security (ASIS).**

RESPONSABILITÉ DE L'ENTREPRISE ET « SÛRETE »

RÉGIS POINCELET

Régis Poincelet

Corporate security department GDF SUEZ

Formé à l'Université de Droit et de Sciences Économiques d'Aix en Provence. Diplômé de l'Institut des Assurances. Après une carrière dans l'insurance et le risk management au sein de compagnies étrangères, il intègre en qualité de responsable de grands comptes le cabinet de courtage MARSH. Directeur risques et assurances de LYONNAISE DES EAUX, puis de SUEZ. Directeur sûreté du groupe GDF SUEZ où il crée le département d'Intelligence Économique et membre du conseil d'administration du CDSE.

D'UNE RESPONSABILITÉ CLASSIQUE VERS UNE RESPONSABILITÉ SOCIALE

Il y a encore quelques années, la notion de responsabilité de l'entreprise était essentiellement perçue comme le résultat d'un concept juridique dont l'application pouvait donner lieu à des sanctions civiles ou pénales.

C'est aussi la raison pour laquelle, parce qu'il s'agissait - au travers de la réparation financière d'un préjudice - de faire face à une éventuelle augmentation du passif de son bilan, que les entreprises ont cherché imparfaitement à transférer sur un assureur les conséquences de cette même responsabilité.

De façon très marginale, les manuels de droit évoquaient parfois la responsabilité morale et encore, pour l'éliminer aussitôt puisque la sanction relevait de la seule conscience des individus et par voie de conséquence se situait en dehors de la sphère financière.

Il faut se rendre aujourd'hui à l'évidence : si ces notions classiques de responsabilité civile et pénale existent toujours et se trouvent même renforcées (voire dévoyées par le jeu pervers de ce qu'il est convenu d'appeler la « judiciarisation »), force est de constater l'émergence au travers du concept de RSE (Responsabilité Sociale des Entreprises) d'une nouvelle forme de responsabilité « morale » qui fait appel à l'éthique (même si ces deux notions sont fondamentalement différentes). Selon la définition de la Commission européenne, il s'agit *« d'un concept qui désigne l'intégration volontaire par les entreprises de préoccupations sociales et environnementales à leurs activités commerciales et leurs relations avec les parties prenantes ».*

La sanction d'une éventuelle défaillance de l'entreprise dans ce domaine est d'une autre nature en ce qu'elle impacte d'abord et avant tout sa réputation, c'est-à-dire son image, avant d'avoir les conséquences financières catastrophiques que l'on sait, lesquelles de toute façon ne sont pas assurables.

LE DÉBUT D'UNE NOVATION : DE LA FONCTION « SÉCURITÉ » VERS UNE MISSION « SÛRETÉ »

Dans ce cadre particulier d'élargissement de la notion de responsabilité et d'aggravation de ses conséquences, nous assistons à l'amorce d'une novation dans le contenu des missions confiées aux professionnels de la sécurité et des objectifs poursuivis. Évolution dont ils sont eux-mêmes à l'origine en écrivant chaque jour leur doctrine au sein d'instances comme celle du CDSE.

Il suffit pour illustrer cette thèse, de prendre pour exemple celui de la protection des personnels en mission ou en expatriation. La jurisprudence « Karachi » qui remonte au 15 janvier 2004 a rappelé brutalement que l'entreprise était tenue à une obligation de sécurité de résultat et que sa responsabilité pouvait être reconnue sur le fondement d'une faute inexcusable même à l'occasion de la survenance d'un attentat terroriste que chacun, jusqu'alors, imaginait naïvement réunir toutes les caractéristiques de la force majeure exonératoire.

Les professionnels ont alors dans un premier temps, réagi en adoptant une série de mesures « classiques » de prévention et de protection visant à assurer et à renforcer la sécurité des personnels. Dans une phase ultérieure, ils ont aussi compris que cette mission ne pouvait pas s'accomplir sans faire appel au renseignement au travers d'une « veille pays » trop longtemps négligée.

On peut penser désormais que l'entreprise va s'orienter vers de nouveaux concepts d'implantation dans des zones à risques plus conformes à une politique de RSE en vivant « avec » et non « dans le pays », ou encore en se posant la question de savoir non pas ce que nous pouvons produire là-bas mais ce que nous pouvons faire avec ses habitants qui sont aussi et souvent nos salariés.

C'est cette nouvelle approche que les directeurs sûreté devront intégrer, s'ils ne veulent pas continuer à réagir face à la survenance de situations « non conventionnelles » par la trop traditionnelle « évacuation » de nos ressortissants. À l'exception de quelques cas justifiés car extrêmes, chacun sait que la vraie motivation d'une évacuation relève bien sûr de la volonté louable de protéger nos personnels expatriés ou missionnés mais aussi du souci illusoire de ne pas engager sa responsabilité (ou du moins de la diluer) par l'adoption d'un comportement grégaire mais confortable.

C'est aussi la raison pour laquelle un comportement éthique des directeurs sûreté supposera l'adoption de mesures appropriées à l'attention des personnels de l'entreprise qui ne sont pas des expatriés au sens juridique du terme et pour lesquels l'évacuation n'a pas de sens. Négliger cet aspect de la problématique sera probablement considérer comme discriminatoire dans les années qui viennent.

DE NOUVELLES PERSPECTIVES…

Ce simple exemple démontre que les professionnels de la sûreté devront à l'avenir élargir leur champ de compétences traditionnel pour être perçus au sein de l'entreprise comme capables d'accompagner son développement par une prise de risques calculée mais aussi par une prise en compte d'autres impératifs que strictement sécuritaires, notamment dans le domaine de l'éthique.

Nos objectifs qui sont ceux de la conquête des marchés et de la continuité d'activité (même lorsque les circonstances les rendent difficiles) devront nécessairement tenir compte de ces nouveaux impératifs.

Pour y parvenir, il faudra que les directeurs sûreté fassent preuve d'imagination et surtout que nous endossions clairement nos responsabilités. ■

VERS LA COPRODUCTION DE SÉCURITÉ/SÛRETÉ

CHARLES YVINEC

Charles Yvinec

Directeur sûreté
du groupe AIR FRANCE

Entré à l'École Nationale Supérieure de Police de Saint-Cyr au Mont-d'Or en 1982, il a exercé successivement les fonctions de commissaire de police en Police Judiciaire, à la Police aux Frontières, en sécurité publique, au cabinet du directeur général de la Police Nationale, puis, après avoir exercé en tant que zonal PAF aux Antilles-Guyane, au Secrétariat Général de Sécurité Intérieure à la Présidence de la République où il a été promu contrôleur général de la Police Nationale. Directeur sûreté d'AIR FRANCE depuis 2004 et membre du conseil d'administration du CDSE.

LE RESPECT D'UN CADRE RÉGLEMENTAIRE

Lorsque l'on évoque les fonctions d'un directeur sécurité/sûreté d'une entreprise, celle qui vient en premier lieu à l'esprit concerne la gestion des affaires « confidentielles » en relation avec les pouvoirs publics, mission sensible dont la conduite serait affaire de spécialistes. Cette image ne correspond plus véritablement à la réalité actuelle, celle d'une sécurité/sûreté de plus en plus réglementée, encadrée, progressivement soumise aux mêmes normes que celles qui régissent l'ensemble des activités de toute entreprise.

Cette évolution fait qu'aujourd'hui le directeur sécurité/sûreté a pour mission première d'assurer la mise en conformité réglementaire du dispositif sûreté de son entreprise.

Dans ce cadre, la nature de la relation qu'il établit avec les services publics s'apparente plus à celle de l'administré vis-à-vis de son administration, qu'à celles plus secrètes nouées par nos anciens avec leurs correspondants au sein des services spécialisés civils et militaires.

Cette relation de nature administrative est plus contraignante et impose des échanges avec les autorités compétentes à chaque étape de la mise en place d'une organisation de la sûreté au sein d'une entreprise.

- Lors de la préparation des procédures, tout d'abord. Il s'agit pour le directeur sûreté d'obtenir des services publics compétents des avis, des éclairages sur le droit applicable, surtout en cas d'incertitude juridique.
- Lors de la mise en œuvre ensuite, notamment lorsque le programme et les procédures sûreté sont soumises à un agrément d'un service de l'État.
- Enfin, de façon continue à l'occasion des opérations de surveillance et du traitement des éventuelles non-conformités relevées par les services compétents de l'État.

UNE GESTION PARTAGÉE DE LA SÉCURITÉ

Ce type de rapports, qui relève d'une certaine forme de « subordination » dans la mesure où l'entreprise est en grande partie tributaire des décisions prises par les pouvoirs publics, laisse de plus en plus place à une relation plus partenariale. **Les services de l'État ont en effet pris progressivement conscience de la nécessité d'associer les professionnels concernés au processus normatif, afin d'éviter la publication de textes inadaptés voire inapplicables.**

Les responsables sûreté des entreprises sont ainsi amenés à contribuer à titre individuel ou collectif, en bilatéral ou au sein de conseils et commissions, à une gestion de la sécurité partagée entre pouvoirs publics et partenaires privés. Ce travail de réflexion, de conceptualisation participe indubitablement à la valorisation de la fonction.

Le cadre étant fixé, l'entreprise attend de son directeur sûreté une gestion des risques efficace, qui nécessite une grande capacité d'anticipation, de réaction et d'adaptation permanente, prenant en compte l'expérience des crises vécues.

Quelles que soient les performances, les qualités des entreprises privées de conseil, force est de constater que la contribution, l'avis des pouvoirs publics dans la mise en place d'une politique de sûreté par une entreprise privée est irremplaçable. L'État joue en effet un rôle inégalable en matière de validation de l'information sensible.

L'INFORMATION AU CŒUR DE LA COPRODUCTION DE SÉCURITÉ

Si les entreprises se sont depuis longtemps efforcées d'obtenir une information frappée du sceau de l'État, confiant à leur directeur sûreté cette mission, les pouvoirs publics ont quant à eux beaucoup hésité à s'engager dans une collaboration dont ils n'ont souvent perçu qu'un aspect négatif, celui de la diffusion non-maîtrisée d'informations sensibles.

Cette situation a toutefois évolué, et à l'exemple traditionnellement cité des pays anglo-saxons, les autorités françaises intègrent de plus en plus la sphère économique et avec elle, l'intérêt des entreprises dans leur domaine d'activité naturelle.

Les ministères, en premier lieu celui des Affaires étrangères, voire même certains services spécialisés, mettent progressivement en place des dispositifs destinés à améliorer une communication essentielle pour les entreprises au travers de colloques, de commissions associant le secteur public au privé.

La commission internationale créée par le MAEE (Ministère des Affaires Étrangères et Européennes) le CINDEX (Centre Inter-entreprises de l'Expatriation) et le CDSE est une excellente illustration de ce partenariat destiné à faciliter les échanges d'informations, à partager l'évaluation de la situation dans les pays dits « à risque ».

Si l'échange d'informations ne souffre donc pas de difficulté majeure lorsqu'il porte sur des domaines dont la confidentialité est limitée, on observe que la communication est plus délicate lorsqu'il s'agit d'informations très sensibles.

Les services spécialisés, légitimement prudents, veillent à ne communiquer ces informations qu'à des correspondants auxquels ils accordent leur confiance, soit en raison de leur origine professionnelle, soit parce qu'ils ont pu évaluer leur capacité à gérer ce type d'information, au travers notamment d'une habilitation « confidentiel » ou « secret défense ».

Afin de faciliter ces échanges, notamment lorsque l'urgence l'impose, y compris sur des domaines sensibles, il est donc recommandé d'organiser ces relations, si possible aux travers de protocoles, et de désigner voire d'accréditer les correspondants en charge de ces contacts au sein de l'entreprise.

Il est également important de préciser les objectifs de ce partage de l'information afin d'éviter d'éventuelles confusions des genres entre intérêt public et privé, l'intérêt de l'État n'étant pas toujours le même que celui de l'entreprise, notamment sur le plan économique et social.

Sécurité et sûreté au sein d'une entreprise passent par un renouvellement de nos modes de relations avec les pouvoirs publics pour fluidifier, adapter et anticiper nos échanges afin d'optimiser nos réactivités réciproques. ■

LA COMPLIANCE, UNE OPPORTUNITÉ POUR LES DIRECTIONS SÛRETÉ

XAVIER GUIZOT

Xavier Guizot

Directeur risks & compliance
du groupe CARREFOUR

Directeur risks & compliance du groupe CARREFOUR, Xavier Guizot est notamment en charge des cartographies des risques, de l'intelligence économique, de la gestion de crise, de la compliance, de l'éthique et de la sécurité-sûreté. De formation financière, il était auparavant directeur prévention des risques après avoir occupé pendant plusieurs années les fonctions de responsable de projets auprès du secrétaire général du groupe.

COMPLIANCE ?

Anglicisme souvent traduit par conformité, la « compliance » est une démarche / pratique assez récente en Europe qui s'est développée aux États-Unis depuis les années 2000 suite aux scandales financiers (Enron…).

La compliance se traduit par une multiplication des normes y compris hors du strict champ juridique, ce qu'on appelle la « soft law », des contrôles plus nombreux et un durcissement des sanctions. À travers ces pratiques, elle vise à renforcer le respect des procédures et cadres de référence par les collaborateurs tout en renforçant la résilience des organisations par une plus grande prévention.

Cela se traduit notamment par des « programmes de compliance » qui s'appliquent à de nombreux domaines correspondant à des risques auxquels est soumise l'entreprise (respect des lois, concurrence, corruption, confidentialité…).

Comme toute politique de prévention, le « programme de compliance » doit être le plus adapté possible aux réalités de l'entreprise, à sa culture, à son organisation et à ses problématiques. Il dépend également de l'activité de l'entreprise, avec une pression et des obligations réglementaires plus ou moins fortes selon les secteurs. À titre d'exemple, la problématique de conformité est ainsi plus sensible et développée dans les secteurs financiers.

La compliance est également un élément du dispositif de contrôle interne, un « rappel à la loi » alors que la performance et les résultats ne peuvent raisonnablement et durablement être atteints que dans le respect des réglementations. Dans cette démarche, la veille, l'information et la formation sont des éléments clés du dispositif dans une approche décloisonnée au service de l'entreprise.

Alors que le coût direct et indirect de ces programmes peut être parfois perçu comme un obstacle, le succès de la démarche dépendra notamment du caractère opérationnel et pédagogique de l'approche retenue.

COMPLIANCE ET SÛRETÉ

Pour le directeur sûreté, la compliance recouvre deux dimensions : les programmes de compliance de la fonction sûreté, c'est-à-dire le respect du cadre dans lequel le directeur sûreté va exercer ses fonctions, mais également le rôle du directeur sûreté dans la politique plus globale de compliance de l'entreprise.

- Pour la fonction sûreté proprement dite, si les standards globaux sont plutôt émergents et encore relativement peu développés, certains secteurs ou activités sont par nature soumis à des réglementations ou contraintes spécifiques (défense, énergie, aéronautique…) avec un cadre renforcé récemment pour les entreprises intervenant dans des « secteurs d'activités d'importance vitale » ou « critiques ». Si la problématique de compliance dépend ainsi du secteur d'activité, elle est également très variable selon les domaines d'intervention de la fonction sûreté qui sont soumis à des cadres réglementaires plus ou moins forts : vidéo protection, confidentialité, lutte contre la fraude interne, PCA, sécurité privée, sécurité des voyageurs et expatriés… Si plusieurs normes ISO spécifiques peuvent potentiellement concerner le directeur sûreté (27001 - Sécurité de l'information, 28000 - Sûreté de la chaîne logistique et du transport…), le périmètre et l'organisation de la fonction tout comme ses démarches de compliance peuvent également se concevoir dans une approche plus large de « Risk Management » formalisée dans l'ISO 26 000 et le COSO.
- Compte tenu de ses domaines d'intervention et de son positionnement, le directeur sûreté a également un rôle important à jouer dans l'accompagnement de la politique globale de compliance de l'entreprise en tant qu'acteur du contrôle interne.

Avec un comportement exemplaire, des actions au service de l'entreprise et sa vision transversale et décloisonnée, il peut selon les domaines, conseiller, accompagner ou contrôler les démarches de compliance des autres fonctions.

La compliance est une opportunité pour les directeurs sûreté de veiller à la conformité intelligente de leur organisation dans un contexte réglementaire évolutif. C'est également une démarche positive qui permet de valoriser la fonction de directeur sûreté par la démonstration de sa capacité à appréhender l'organisation d'un point de vue global avec une perspective d'expert au service de l'entreprise. La compliance n'est cependant pas une fin en soi mais un moyen de renforcer le dispositif qui ne doit pas faire oublier le bon sens, la vigilance permettant l'identification et l'anticipation dans une période d'incertitudes croissantes où les règles de demain ne sont pas encore écrites. ■


nationaux. Droits
tecteurs. Un ton,
PROTECTION (lat. *pr*
du mal. La protec
de lettres a rendu
sa protection, prer

Recommandations opérationnelles

- **Selon le secteur d'activité de son entreprise et son périmètre d'intervention, le directeur sûreté devrait ainsi construire un ou plusieurs *« programmes de compliance »* sûreté, par une identification des règlementations et cadres de référence auxquels l'ensemble des collaborateurs de la fonction sûreté sont soumis dans l'exercice de leurs fonctions, une évaluation de la conformité, la mise en place et le suivi de plans d'action et, le cas échéant, un contrôle confié à l'audit interne.**

- **On pourrait à titre d'exemple très facilement imaginer le *« programme de compliance »* pour la sécurité des voyageurs : une règlementation avec une jurisprudence, une évolution des contextes, des cadres de références à mettre en place, des programmes de formations et de sensibilisation, des indicateurs.**

- **L'efficacité de la démarche de compliance dépendra également de l'*« intensité et de la dynamique normatives »*. Nous appelons ainsi à la création d'un groupe de travail et de réflexion public/privé et interministériel sur les normes applicables en matière de sûreté, avec une mise en perspective comparée européenne et internationale. S'inscrivant dans une démarche de simplification et d'efficacité, cette initiative permettrait également d'améliorer la lisibilité et la cohérence des cadres de référence.**

LA SÛRETÉ AU DÉFI DE LA COMMUNICATION

ALAIN BELLEFACE

Alain Belleface

Responsable sûreté
du groupe VINCI

Est titulaire d'un master en management des risques et auditeur de l'Institut National des Hautes Études de la Sécurité et de la Justice. Il a travaillé pendant une quinzaine d'années au ministère de la Défense puis deux ans dans un cabinet de conseil spécialisé en sûreté internationale et gestion de crise. En 2008, il a rejoint VINCI comme adjoint au directeur sûreté du groupe.

L'entreprise est un monde ouvert d'échange, de partage et de communication. La légitimité des directions de sûreté et leur ancrage dans l'organisation interne comme une fonction support utile et aussi incontournable que d'autres plus « traditionnelles », passe nécessairement par la communication.

« Dire ce que l'on fait et faire ce que l'on dit », dans un souci de transparence, d'éthique et de normalisation du métier, est une nécessité pour asseoir la fonction sûreté et lui donner de l'envergure. Au contraire, le silence suscite l'interprétation, la suspicion, la rumeur, le fantasme, autant d'appréciations qui desservent la fonction.

La communication des directions sûreté est tournée essentiellement vers l'interne, afin qu'elles soient identifiées pour faciliter la remontée d'informations et faire valoir leur expertise et leur capacité d'action auprès du management ainsi que sur le terrain, au plus près du business. Elle est également externe, facilitant et fluidifiant les échanges avec l'ensemble des interlocuteurs du secteur privé et des services de l'État, avec qui le dialogue doit être étroit et permanent.

UN TRAVAIL INDISPENSABLE SUR L'IMAGE

L'absence de communication comme le parcours professionnel des directeurs sûreté et de leurs équipes (majoritairement issus des services spécialisés de l'État) favorisent la mise à l'écart, la stigmatisation, voire la crainte. Force est de constater

que l'image véhiculée par les directions sûreté est souvent négative. Dans l'entreprise, elles sont vues comme des centres de coût, d'entrave, d'enquête voire d'ingérence. À l'extérieur, elles sont perçues comme des structures de recyclage et de pantouflage d'anciens fonctionnaires. Parce que ces interprétations sont erronées, l'accent doit être mis sur la communication.

Par leur formation professionnelle, les directeurs sûreté sont avant tout des techniciens qui disposent de compétences pluridisciplinaires. **Leurs parcours professionnels les conditionnent à gérer des situations d'urgence, dégradées ou de crise, autant d'événements où le temps de la communication n'est pas celui des opérations.** Ainsi, la communication est une compétence qu'ils ne maîtrisent pas pour la grande majorité d'entre eux, d'autant qu'ils ont servi dans le cadre de missions régaliennes pour lesquelles l'essentiel est codifié, planifié et où la discrétion, la réserve et la confidentialité sont souvent constitutives de leur fonction.

Enfin, pour ce qui concerne les directeurs venant de la filière dite « civile » ou interne à l'entreprise, la majorité d'entre eux est issue de formations techniques et scientifiques qui ne les ont pas davantage préparé à communiquer que leurs homologues issus de la fonction publique.

Sans pour autant se positionner à contresens de la communication interne, la direction sûreté doit se singulariser en se construisant une image et une identité propres afin d'être lisible, visible et attractive. Tous les outils et techniques professionnels doivent être utilisés. Ainsi, slogans, travail sur l'image, création d'une identité visuelle, utilisation de l'Intranet, élaboration de guides et booklets de bonnes pratiques, visibilité dans les lettres et journaux internes, campagnes thématiques, témoignages de salariés, sont autant d'outils qu'il convient d'utiliser pleinement pour être exhaustif et toucher toutes les catégories de personnels de l'entreprise.

PRÉVENTION ET COMMUNICATION : UNE ASSOCIATION INDISPENSABLE POUR CONVAINCRE

Une politique de sûreté efficace repose sur trois principes généraux, à savoir des mesures techniques, organisationnelles et comportementales. Si les deux premières sont prévisibles, prédictives et mesurables, la troisième, qui repose sur le facteur humain, est aléatoire, instable et non-maîtrisable. Pour limiter l'amplitude de cet aléa, il convient de porter l'effort, de manière incontournable, sur l'anticipation, la préparation et la prévention. C'est en communiquant auprès des personnels de l'entreprise et en diffusant une culture de la sûreté que cet objectif sera atteint.

L'efficacité d'un dispositif ponctuel ou d'une politique générale repose très largement sur l'adhésion des personnels qui y sont confrontés. En effet, la négligence crée l'opportunité pour le malveillant, et c'est en évacuant les certitudes que l'on entretient la vigilance.

La sûreté vient indiscutablement perturber la quiétude des salariés. Les procédures peuvent être perçues comme contraignantes au quotidien car, avant d'être salarié, un personnel de l'entreprise est un citoyen responsable qui, à titre privé, revendiquera d'avoir les bons gestes et les bons comportements.

Parce que la marge de manoeuvre pour convaincre est étroite, les directions sûreté doivent apprendre à faire passer les bons messages pour susciter l'adhésion naturelle à des principes et des bonnes pratiques. Le bon message doit être en phase avec la réalité de l'entreprise, ses métiers, son environnement, son marché et ses contextes concurrentiels et réglementaires.

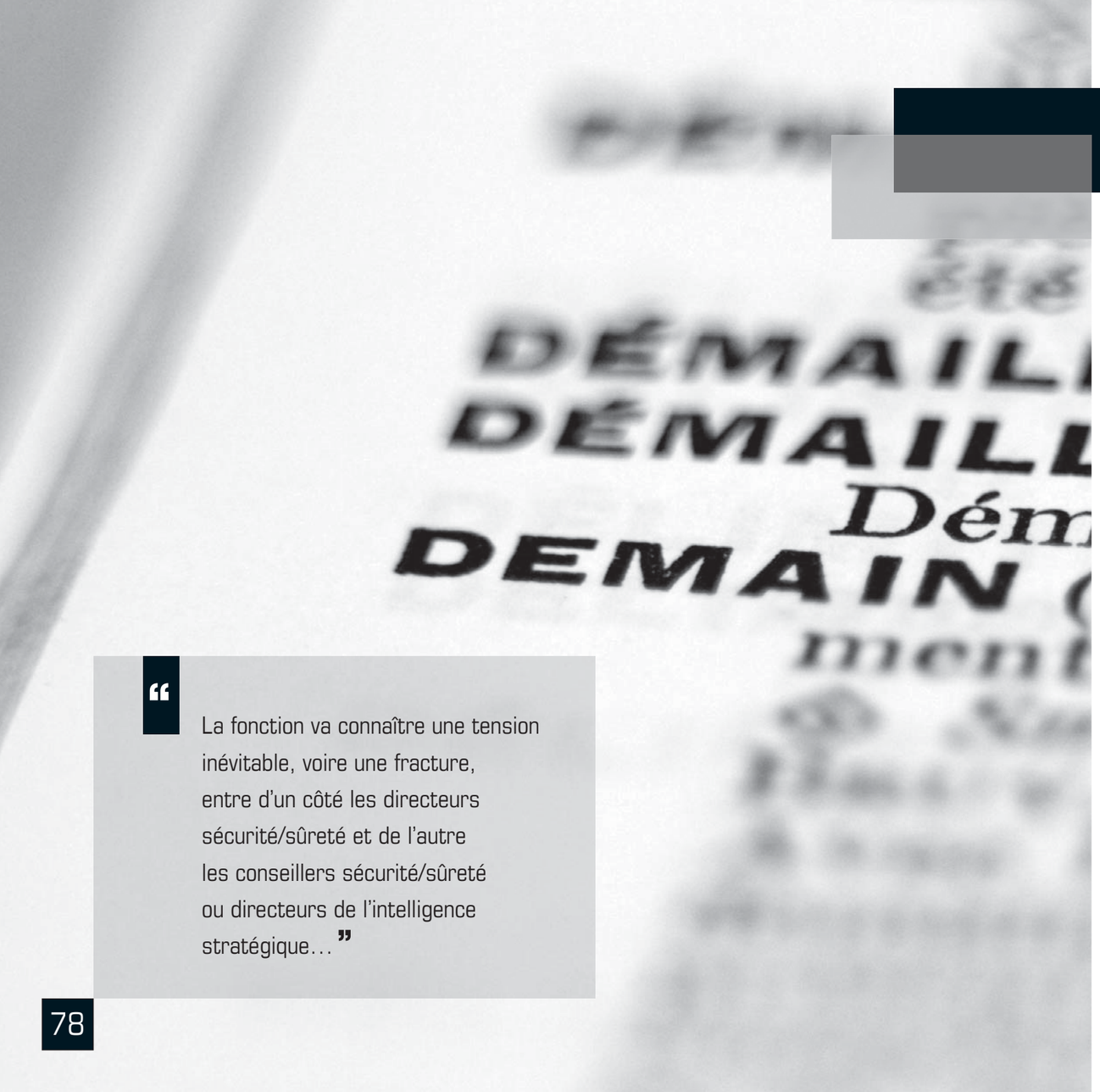
C'est à cette condition que le message sera reçu positivement par les salariés.

RÉPONDRE AUX EXIGENCES DE TRANSPARENCE

Enfin, au-delà de l'image et de la fonction prévention, les directions sûreté doivent se préparer à communiquer sur leurs activités à la demande des instances dirigeantes de l'entreprise.

Responsabilité des mandataires sociaux pour ce qui concerne la protection des personnels, perspectives de pénalisation de la violation des secrets d'affaires ou encore analyses de risques de plus en plus exhaustives, la tendance plaide en faveur d'une montée en puissance de la fonction sûreté. De plus en plus, le comité de direction, le comité exécutif voire le conseil d'administration seront amenés à solliciter des informations précises sur les actions réalisées par les directions sûreté. Dans un contexte de responsabilité sociale de plus en plus élargie qui suscite toujours un peu plus de communication et de transparence de la part des entreprises, la probabilité est forte qu'elles soient amenées à moyen terme à apporter des précisions sur les questions de sûreté dans leur rapport annuel. Cette communication devra être alors parfaitement maîtrisée au même titre que l'est aujourd'hui la communication financière.

Développer en propre, former les personnels, se faire accompagner par des prestataires et s'appuyer sur les compétences internes des directions de communication, tous les moyens sont à la disposition des directions de sûreté pour qu'elles puissent relever avec succès ce défi de la communication qui sera nécessairement le ressort pour faire aboutir les nombreux autres défis évoqués dans le présent livre blanc. ■



> La fonction va connaître une tension inévitable, voire une fracture, entre d'un côté les directeurs sécurité/sûreté et de l'autre les conseillers sécurité/sûreté ou directeurs de l'intelligence stratégique…

CONCLUSION

OLIVIER HASSID

Directeur général du CDSE

Olivier Hassid

Directeur général
du Club des Directeurs
de Sécurité des Entreprises

Docteur es sciences économiques, directeur général du CDSE, il a été directeur de la sécurité en collectivité locale en 2003 avant de rejoindre les services du premier ministre sur les questions de sécurité. A été ensuite l'adjoint du PDG de BRINKS avant de devenir directeur général du CDSE. Auteur de nombreux ouvrages en matière de sécurité et de management des risques. Il est également le directeur de la revue *Sécurité & Stratégie*.

Quel sera le directeur sécurité/sûreté de demain ? Quelles seront ses missions et à qui devra-t-il rendre des comptes ?

Notre propos conclusif n'est pas de suggérer un modèle idéal car il n'y en a pas. En fonction de l'histoire de l'entreprise, de la personnalité des dirigeants, de la nature des menaces auxquelles cette même entreprise est confrontée, le profil du directeur sécurité/sûreté et son travail évolueront considérablement. Cette première observation faite, il est néanmoins possible de tirer quelques tendances de fond.

Premièrement, la fonction est appelée à grandir au sein des entreprises. Malgré certaines affaires qui peuvent peser sur l'image de cette activité, les entreprises auront de plus en plus besoin d'équipes traitant du domaine de la sécurité/sûreté. L'expansion des activités des entreprises à l'échelle

mondiale en même temps que la virtualisation grandissante de l'économie soumettent ces dernières à un risque accru vis-à-vis des différents actifs de l'entreprise. Pensons aux risques de kidnapping, de fuites de données, de fraudes ou encore de pressions à l'encontre du personnel… Face à ces menaces, les entreprises, à la recherche de relais de croissance à l'international dans des pays à risque, n'auront d'autre choix que d'intégrer la sûreté au projet d'investissement.

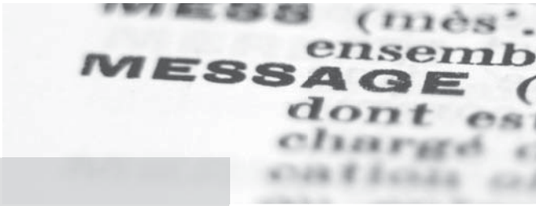
Deuxièmement, la fonction va connaître une tension inévitable, voire une fracture, entre d'un côté les directeurs sécurité/sûreté et de l'autre les conseillers sécurité/sûreté ou directeurs de l'intelligence stratégique (ou « VP Insight[1] »). En effet, il n'est pas impensable que les entreprises recourent à deux types de profils distincts. Tout d'abord un directeur sécurité/sûreté qui assure avec son équipe la sécurité des personnes, des biens et des données. Ensuite, un conseiller sécurité/sûreté en charge de la veille et de l'accompagnement des projets internationaux. Or, il n'est pas sûr que cela soit la même personne qui soit en mesure de réaliser ce travail. L'un sera plus opérationnel et organisationnel tandis que l'autre sera plus proche de la stratégie de l'entreprise et du groupe très restreint de ses décideurs pour y apporter une vision, le premier étant en charge de la sécurité et le second de la sûreté pour reprendre la distinction établie par le Président en introduction. Le premier réalisera ou fera réaliser des audits de sûreté ou des formations de sensibilisation en matière de protection des salariés partant à l'international alors que le second réalisera des *due diligences* et sera en charge de l'intelligence économique, contribuera à des négociations, des acquisitions. À moins que l'on parvienne à résoudre dans le futur l'équation, à travers des personnalités hybrides, qui connaissent à la fois extrêmement bien le business et des personnalités qui ont su développer des compétences pointues en matière de renseignement et de sécurité. Ces deux fonctions peuvent être également hiérarchiquement articulées.
Un « bicéphalisme ordonné » favoriserait un enrichissement de la fonction sûreté en entreprise. « Un bicéphalisme désordonné » créerait des zones de clivage, des pertes d'énergie managériale, de l'incompréhension et de la friction.

Troisièmement, la fonction sera-t-elle pourvue de civils venant directement du business ou d'anciens militaires ou policiers ? Dans le cadre d'une étude récente publiée dans *Sécurité & Stratégie*, le chercheur Frédéric Ocqueteau constate pour l'heure que la fonction se militarise, les militaires bénéficiant *« d'une réputation inentamée de savoir comment collecter du renseignement stratégique aux meilleures sources et au bon moment[2] »*. Mais il est certain que la partie n'est pas terminée. Nous devrions certainement avoir dans le futur un panachage de plus en plus complexe. On voit en effet émerger comme directeur sécurité/sûreté de nouveaux profils, des informaticiens, des ingénieurs ou encore des financiers. Il est par exemple certain qu'avec le développement d'une société numérique, un certain nombre de postes seront occupés par des informaticiens ou des experts de la sécurité informatique. De même, la financiarisation de l'économie laisse à penser que les directeurs pourront également venir des mondes assurantiel et bancaire. Il ne faut pas négliger les profils issus du *core business* de l'entreprise qui ont déjà identifié les risques et les parades à mettre en œuvre pour sa sécurité. Dès lors, pour certains secteurs d'activité, la dimension « compréhension des ressorts et mécanismes » peut primer sur toute autre dimension technique et même sur des savoirs-faire strictement liés à la sécurité.

Enfin, la fonction dépendra dans une large mesure des formations mises en œuvre. En France, pas moins d'une trentaine de formations universitaires existent en matière de sécurité/sûreté. Les *security directors* de demain émergeront en partie de ces formations qui allient justement Management, Criminologie et Droit. Ces nouveaux profils répondront alors peut-être à cette nécessité de profils hybrides à la fois vaccinés aux problèmes de ROI et de sécurité économique, et incollables en matière de prévention situationnelle. ■

1. Se référer à l'article de Bernard Galéa, « Sécurité économique », page 59 dans le présent livre blanc

2. Ocqueteau, « Profils et trajectoires des directeurs sûreté », Sécurité & Stratégie, Mars 2011-Juin 2011



1 rue de Stockholm
75008 Paris
Tél. 01 44 70 70 85
Fax 01 44 70 72 13
contact@cdse.fr
www.cdse.fr