LIVRE BLANC

2022

DE LA FONCTION SÉCURITÉ-SÛRETÉ EN ENTREPRISE

CDSE

CLUB DES **DIRECTEURS** DE **SÉCURITÉ** DES ENTREPRISES

INTRO > DUCTION

STÉPHANE VOLANT

PRÉSIDENT DU CDSE

Dès 2011, le Club des directeurs de sécurité des entreprises (CDSE) posait les fondamentaux de la fonction sécurité-sûreté en entreprise avec son premier Livre blanc, accompagnant ainsi une révolution en cours dans les organisations. Ces fondamentaux, nous les retrouvons dans ce nouvel opus, avec un regard neuf mais conforté par plus de dix ans de pratique de la gestion des crises et d'expérience quotidienne des aléas de la sécurité des entreprises. Pour les directeurs sécurité-sûreté membres du CDSE, ces « bonne pratiques » constituent les bases, les « invariants », gages d'une **sécurité-sûreté stratégique, intégrée à la gouvernance de l'entreprise car efficiente et transversale, au service du business.**

Ces fondamentaux de la sécurité-sûreté, il faudra néanmoins très certainement les rappeler dans le troisième Livre blanc du CDSE et probablement même dans le quatrième car, malgré une révolution, des évolutions restent à mener. Un certain nombre d'entreprises, parmi les fleurons de l'économie française, n'ont en effet pas encore saisi l'importance de ces sujets et ne se sont toujours pas dotées d'une direction sécurité-sûreté. D'autres estiment prendre en compte ces questions sérieusement mais devraient cependant y consacrer encore plus de moyens. Ainsi, parcourir le Livre blanc du CDSE 2022 revient autant à mesurer le chemin parcouru qu'à constater les efforts qu'il reste à fournir. En attestent **les 18 recommandations structurantes pour une fonction sécurité-sûreté stratégique dans l'entreprise et pleinement intégrée au *continuum* de sécurité** présentées en fin de document.

Au rang du chemin parcouru, ce Livre blanc est le produit de la fusion des idées issues du cœur du réacteur du CDSE : **les 14 commissions et groupes de travail qui favorisent le partage d'expériences et l'émergence de solutions pour tous les sujets traités par les directions sécurité.** De la protection des personnes et des biens matériels et immatériels, à l'intelligence économique, en passant par la sécurité à l'international, la gestion des crises et la continuité des activités, mais aussi la fraude et la compliance, la supply chain… La diversité des problématiques discutées tout au long de l'année au CDSE et opérées par les directions sécurité-sûreté au quotidien dans leurs entreprises témoigne du rôle grandissant de cette fonction, au cœur de la politique de sécurité globale de l'entreprise.

Certaines de ces thématiques étaient absentes du Livre blanc 2011 mais apparaissent aujourd'hui comme incontournables. La gestion des **radicalisations**, par exemple, revêt une importance considérable dans les organisations. Les directions sécurité-sûreté prennent aujourd'hui toute leur part dans la sensibilisation à ce phénomène et proposent des outils ou procédures pour traiter les comportements déviants et protéger ainsi l'entreprise. C'est pourquoi le CDSE travaille étroitement avec le secrétariat général du comité interministériel de prévention de la délinquance et de la radicalisation (SG-CIPDR).

En 2011, on ne parlait pas encore de **cybersécurité.** En 2022, la question des technologies et du cyber est omniprésente, tant dans la vie privée que dans l'entreprise. Et les directeurs sécurité n'ont jamais été autant impliqués sur ces questions. L'attaque cyber est ainsi une menace avérée et les directeurs sécurité-sûreté savent que la protection de l'entreprise passe d'abord par une sécurité numérique maîtrisée. Ils travaillent donc désormais en bonne intelligence avec leurs collègues DSI (directeurs des systèmes d'information) et RSSI (responsables de la sécurité des systèmes d'information). Ces professionnels de la crise s'emploient au quotidien à toujours mieux sensibiliser l'ensemble des collaborateurs et préparer en permanence l'entreprise aux pires scénarios, **à penser et imaginer l'impensable, à manager l'incertitude.** C'est pourquoi l'ANSSI (Agence nationale de la sécurité des systèmes d'information) a souhaité se rapprocher du CDSE afin de publier récemment son guide « *Crise d'origine cyber : les clés d'une gestion opérationnelle* ». Là aussi, il s'agit d'une belle preuve du chemin parcouru par la fonction sécurité-sûreté et le CDSE depuis onze ans.

En 2022, le directeur sécurité-sûreté n'est plus seul. La sécurité-sûreté est une matière active et la fiche de poste de celui qui en a la charge évoluera toujours. Les moyens alloués à la direction sécurité-sûreté ne sont pas fichés et appartiennent à chaque entreprise selon son histoire et son secteur d'activité. Néanmoins, **le directeur sécurité-sûreté peut désormais s'appuyer sur une véritable filière métier constituée de femmes et d'hommes aux parcours et aux compétences multiples.** Une étude menée par le CDSE depuis 2017 nous donne aujourd'hui une photographie plus précise de la physionomie générale de ces directions, ainsi que des progrès à accomplir en termes de professionnalisation et d'attractivité. La féminisation de la filière, par exemple, est en marche même si beaucoup reste à faire en la matière. Néanmoins, sept directrices sécurité-sûreté, présidentes de commission du CDSE ou expertes, ont contribué à ce Livre blanc. Elles n'étaient que deux en 2011. Elles seront encore plus nombreuses en 2032 !

Et puis en 2022, la dépense en sécurité n'est plus simplement considérée comme un coût par l'Entreprise, mais davantage comme un « coût évité », un investissement à la rentabilité certaine, une valeur et un avantage concurrentiel, au même titre que les exigences liées à la responsabilité sociétale des entreprises (RSE). Ainsi, en protégeant leurs emprises, leurs salariés et leurs clients, les directeurs sécurité-sûreté contribuent à la sécurité nationale. La présence des ministres de l'Intérieur successifs à chaque édition du colloque annuel du CDSE en atteste. Et Gérald Darmanin ne s'y est pas trompé, lors de l'édition 2021, en qualifiant l'Entreprise et la sécurité privée qu'elle emploie comme *« la troisième force de sécurité de notre pays ».* C'est pourquoi, comme en 2011, le CDSE recommande dans ce Livre blanc **la création d'un « cercle de confiance » instituant les directeurs de sécurité comme interlocuteurs privilégiés des forces régaliennes et de l'État dans l'Entreprise et permettant un partage d'informations bâti sur le secret professionnel.** Une telle mesure serait de nature à donner définitivement corps au *continuum* de sécurité, pour une sécurité nationale toujours plus optimale.

Vous l'aurez compris, notre reconnaissance est légitimement acquise aux « grands anciens » du CDSE, pionniers de la fonction de directeur de la sécurité-sûreté des entreprises. Et les membres actuels du Club, coauteurs de ce Livre blanc sont fiers de vous présenter, dans les pages qui suivent, le fruit de leur travail et de leurs réflexions…

LIVRE **BLANC**
de la fonction sécurité-sûreté en entreprise . CDSE
Paris . Mai 2022

Directeur de la publication
Marc-Antoine Bindler

Contributeurs
Gabrielle Berthelot, Jean-Paul Bonnet, Serge Collignon, Christian Crémel, Antoine Creux, Edmond d'Arvieu, Clémentine de Lambilly, Bernard Galéa, Jean Garcin, Christophe Gomart, Arnaud Kalika, Jean-Louis Kibort, Aurélien Lambert, Fabien Laurençon, Fabienne Louvet, Pierre-Arthur Mazeau, Jean Maurin, Claire Niclause, Jean-Yves Oger, Émile Perez, Anne Picot-Periac, Michel Pozzo di Borgo, Rudolphe Proust, Joëlle Rietjens,Annick Rimlinger, Pierre Tramier

Création graphique
Aurélie Alder. San Emeterio
reflexiongraphique.fr

SOMMAIRE

III. NOUVEAUX ENJEUX & PERSPECTIVES DE LA SÉCURITÉ — P. 115

18 RECOMMANDATIONS STRUCTURANTES — P. 153

POUR UNE FONCTION SÉCURITÉ-SÛRETÉ STRATÉGIQUE DANS L'ENTREPRISE
ET PLEINEMENT INTÉGRÉE AU CONTINUUM DE SÉCURITÉ

I. DÉFINITION DE LA FONCTION SÛRETÉ

LA SÛRETÉ[1] DANS LA STRATÉGIE DES ENTREPRISES : RÉALITÉ OU FICTION ?

Bernard GALÉA

Vice-Président Sûreté et Intelligence Économique du groupe DANONE et administrateur du CDSE

Si l'Entreprise dispose d'une relative maîtrise de ses risques endogènes, c'est à dire ceux générés par son activité propre (accidents du travail, de process…), elle est de plus en plus confrontée à des risques exogènes diffus.

Dans un monde en plein bouleversement où l'incertitude se développe, les organisations font face à des défis nouveaux et multiformes. Nous vivons de manière quasi simultanée des conflits persistants, en Syrie, au Sahel, en Afghanistan, en Ukraine, une croissance sensible des mouvements de radicalisation et de dérives sectaires, des crises sanitaires sans précédent, des catastrophes naturelles, des tensions commerciales exacerbées entre pays, etc.

Ces diverses crises ont eu, ont et continueront d'avoir des conséquences géopolitiques et géoéconomiques qui contraignent les entreprises à repenser leur stratégie et à modifier leur approche de la sûreté.

Aujourd'hui, le cadre de la mission de la fonction Sûreté est de protéger l'Entreprise, ses hommes et ses femmes, ses biens, contre toutes formes de menaces malveillantes, qu'elles soient d'origine humaine, logique ou économique : il s'agit désormais d'un concept d'approche globale.

Au lendemain du 11 septembre 2001, la sécurité physique est soudainement devenue la priorité. Tous les dirigeants craignaient que d'autres attaques terroristes ne viennent impacter leurs personnels ou installations. Plus de vingt ans plus tard, en 2022, à l'ère du « new normal », l'explosion de la digitalisation, de l'Intelligence Artificielle, des fraudes financières, l'avènement du télétravail, des attaques cyber conjuguées aux instabilités politiques et aux conséquences encore incertaines de la crise générée par la COVID-19 obligent les directeurs de la Sûreté et leurs équipes à être plus agiles. Car ces derniers doivent couvrir un spectre toujours plus large. Et,de la même façon, ils sont amenés à favoriser a minima la convergence avec d'autres fonctions comme celles des directeurs de la Sécurité des Systèmes d'Informations, des risques HSE (hygiène, sécurité et environnement), de la Gestion des Risques, Crises et Continuité d'activité.

DE LA MAÎTRISE DES RISQUES : ENTREPRENDRE C'EST PRENDRE DES RISQUES

La stratégie d'entreprise comprend principalement trois piliers : le modèle économique, la concurrence et l'espace sur lequel elle peut déployer son marché.

Par une gestion globale des risques et des crises, la fonction Sûreté aide à bâtir les fondations des trois piliers et contribue à l'élaboration puis à la réalisation du plan stratégique en protégeant l'organisation.

En amont de tout processus décisionnel, elle participe à une analyse des risques (géopolitiques, sécuritaires, concurrentiels, de réputation, de prédation, de déstabilisation, de contrefaçon, d'incidents sur la « supply chain », etc.) afin de pouvoir les anticiper. La capacité de collecter, trier et analyser des informations permettant de comprendre l'environnement, en discerner les menaces et penser les moyens de protection adéquats devient une expertise critique pour protéger de manière pertinente les organisations.

[1] Sûreté : pour cet article terme générique regroupant Sûreté et Sécurité.

En amont de tout processus décisionnel, elle participe à une analyse des risques (géopolitiques, sécuritaires, concurrentiels, de réputation, de prédation, de déstabilisation, de contrefaçon, d'incidents sur la « supply chain », etc.) afin de pouvoir les anticiper. La capacité de collecter, trier et analyser des informations permettant de comprendre l'environnement, en discerner les menaces et penser les moyens de protection adéquats devient une expertise critique pour protéger de manière pertinente les organisations.

Dans sa phase de déploiement, elle doit prévenir les risques et, en cas de survenance, participer aux dispositifs de gestion de crise et de continuité d'activité pour permettre à l'entreprise de poursuivre ses objectifs stratégiques en s'adaptant à son nouvel environnement.

Plus que jamais, la sûreté est le nécessaire accompagnement des prises de risques du décideur. Le directeur de la Sûreté est devenu un partenaire business qui vise à sécuriser les pensées et les prises de décisions des conseils d'administration et des comités exécutifs en réduisant les incertitudes.

DE LA CONFIANCE : ENTREPRENDRE C'EST ÊTRE SOCIALEMENT RESPONSABLE

La **Responsabilité Sociétale/Sociale des Entreprises (RSE)** est définie par la Commission européenne comme l'intégration par les organisations de préoccupations sociales et environnementales à leurs activités commerciales et leurs relations avec les parties prenantes. En d'autres termes, la RSE c'est la contribution des entreprises aux enjeux du développement durable.

Depuis l'entrée en vigueur de la loi PACTE du 22 mai 2019, de nouvelles dispositions sont entrées en vigueur pour renforcer la RSE :

> L'objet social de toutes sociétés intègre la considération des enjeux sociaux et environnementaux ;
> Les sociétés qui le souhaitent peuvent se doter d'une raison d'être dans leurs statuts ;
> Le statut d'entreprise à mission a été créé.

L'intégration des données sur les risques et la performance extra-financières est donc devenue un enjeu stratégique pour l'Entreprise, tant pour attirer les talents et les fidéliser que pour communiquer auprès des parties prenantes (actionnaires, consommateurs, salariés, organismes étatiques…).

Aussi, le nouveau document d'enregistrement universel (appelé également URD pour Universal Registration Document) défini par un règlement européen entré en vigueur en 2019, comprend désormais des informations précises sur les risques de sûreté. Par exemple, les indicateurs sur la protection des voyageurs d'affaires, des employés locaux et des expatriés sont très prisés.

Au-delà de répondre à une obligation légale de l'employeur (« Duty of care », article 121-2 du Code pénal et article L 4121-1 du Code du travail) ils permettent de mesurer la maturité des organisations dans leurs analyses de risques, non plus seulement financiers mais sécuritaires dans les pays où les opérations et marchés sont déployés.

Ainsi, comme le soulignait déjà en 2018 Madame Nicole Notat, présidente de Vigeo Eiris et ex-secrétaire générale de la CFDT, lors du colloque annuel du CDSE organisé à l'OCDE : *« Au-delà des enjeux humains, économiques et financiers vitaux pour la performance durable des entreprises, la sûreté s'impose désormais comme un élément central de la responsabilité sociale jusqu'à en devenir un avantage concurrentiel ».*

DE LA GOUVERNANCE : ENTREPRENDRE C'EST RENDRE L'ENTREPRISE PÉRENNE

Positionné au plus haut niveau de l'organisation, le directeur de la Sûreté doit être rattaché à la direction générale et/ou à un membre du comité exécutif. Ce rattachement garantit l'alignement de la sûreté avec la stratégie du business et permet de mieux anticiper les risques.

La fonction Sûreté, transverse par essence, est à la croisée des gouvernances de performance (création de valeur) et de conformité (maîtrise des risques) qui forment les deux piliers de la gouvernance d'une entreprise.

Bien souvent perçue comme un centre de coûts, la sûreté est a contrario un support à la création de valeurs et elle concourt à éviter certaines pertes financières en anticipant des pièges, en renforçant les mesures de mitigation ou en participant avec les équipes de la Compliance ou de l'Audit interne à la mise en œuvre opérationnelle des règles d'éthique, de conduite des affaires (loi Sapin2, etc.) en vue de rendre l'entreprise pérenne et résiliente.

Toutefois, les risques anticipés et gérés par les directions de la sûreté sont souvent invisibles dans les cartographies des risques des organisations.

En effet, l'analyse des risques repose principalement sur une approche financière pilotée par les directions contrôle interne/audit/risques régis par une batterie de processus de type ERM, COSO, ISO..., etc.

Or, les risques sûreté sont peu normés, par nature imprévisibles et leurs impacts financiers difficilement mesurables ce qui peut expliquer les difficultés auxquelles sont confrontés les entreprises pour budgéter cette fonction.

La Sûreté s'inscrit donc dans le temps long de l'Entreprise, toutefois sa maturité n'est pas homogène entre les organisations.

Pour certaines, cela relève encore de la fiction. La fonction sûreté n'est pas correctement positionnée, dimensionnée et ne dispose pas d'un budget proportionné aux risques. Pour d'autres, le directeur sûreté est devenu un cadre dirigeant à part entière.

Ainsi, si certaines entreprises choisissent d'adopter une tactique qui leur permettra de gagner peut-être le prochain match... Celles qui ont intégré la sûreté dans leur stratégie seront, elles, en mesure de remporter le championnat. ■

RECOM > MANDATIONS

- **> Continuer à « évangéliser » les Comex et les DRH à la fonction Sûreté dans les entreprises**
- **> Mettre en place une stratégie éducative pour sensibiliser les futurs dirigeants aux rôles et fonctions de la Sûreté (ENA, Sciences PO, HEC, écoles de commerce...)**
- **> Veiller à bien positionner la fonction au sein des organisations**
- **> Mettre en place, au profit des directeurs sûreté et de leurs équipes, des formations continues non pas technique mais de « management générale des entreprises »**

LE DIRECTEUR SÛRETÉ : UNE FONCTION STRATÉGIQUE AU CŒUR D'UN LARGE ÉCOSYSTÈME D'ACTEURS & DE COMPÉTENCES

FABIENNE LOUVET

Présidente de la commission « Carrières-Emploi-Formation » du CDSE
Directrice Métiers et Organisation de la Sécurité, Renault

Depuis les années 2000, face à la diversification des menaces et des risques (cyber, terrorisme, géopolitique, sanitaire…) et leurs interdépendances dans une économie globalisée, découplée, hyperconnectée, la fonction Sécurité et Sûreté corporate (SSC) en entreprise a pris un essor considérable.
En France, la plupart des grandes entreprises comptent désormais une direction SSC et chacun perçoit, à plus forte raison depuis 2020 à l'aune de la crise de la COVID-19, le caractère de plus en plus incontournable de cette fonction.

Pour autant, il n'existe pas de direction SCC type : les missions, les organisations, les tailles de ces directions sont très hétérogènes et sont relatives aux caractéristiques intrinsèques de chaque entreprise, de son secteur d'activité, de son exposition aux risques et de son histoire.

Afin de faire émerger un positionnement collectif de la filière, de ses métiers aujourd'hui et des évolutions nécessaires demain au service de la « sécurité globale[1] » des entreprises, le Club des directeurs de sécurité des entreprise (CDSE) mène depuis 2017 une étude suivie sur les métiers de la filière sécurité-sûreté corporate, pilotée par sa commission « Carrière - Emploi - Formation ». Cette analyse approfondie vise ainsi à répondre à un questionnement multiple :

- Quelle est la physionomie de la filière ?
- Quels sont les différents métiers de la sécurité-sûreté en entreprise ?
- Quelle est la réalité du positionnement de ces fonctions, de leurs niveaux d'expertises et d'intervention ?
- Des parcours et perspectives de carrière de ces professionnels ?
- Quel est le degré d'attractivité de la filière et comment celle-ci doit progresser pour répondre aux enjeux de demain ?

Les travaux se sont déroulés en deux phases avec l'assistance de cabinets de conseil sélectionnés pour leur expertise et leur professionnalisme : EY, spécialisé en organisation et études prospectives, et Arthur Hunt, spécialisé en Ressources Humaines (recrutement, parcours de carrières et pratiques de rémunération).

La première phase, publiée en 2019, a permis de dresser la physionomie actuelle de la filière, de disposer d'analyses sur les organisations et de renforcer le positionnement de ces activités au niveau stratégique dans les entreprises. L'étude et la structuration des métiers par les compétences a par ailleurs abouti à l'élaboration d'un document inédit sous la forme d'un référentiel des métiers SSC, modulaire, adaptable à la diversité des organisations qui comprend, sans prétendre à l'exhaustivité, 12 fiches métier repères.

En 2021, la deuxième phase est venue affiner ces travaux fondateurs et approfondir les niveaux de contribution, les pratiques de rémunération en vigueur ainsi que les parcours et les perspectives de carrière à tous les échelons de la filière.

[1] La sécurité globale couvre la prévention et la protection des personnes, du patrimoine matériel et immatériel de l'entreprise contre toutes les atteintes accidentelles et malveillantes, ainsi que les activités de veille, de gestion de crise, de continuité d'activité et la sécurité économique. En fonction des entreprises, les directions SSC couvrent tout ou en partie de ces périmètres d'activité.

Cette étude des emplois, activités et compétences associées est devenu un outil de référence dans l'écosystème de la filière, pour accompagner l'évolution de ses acteurs. L'ensemble des livrables constitue ainsi un cadre directement opérationnel pour les directeurs sécurité-sûreté, en particulier pour échanger avec leur direction des Ressources Humaines. Jean Maurin, directeur de la Prévention et de la Protection du Groupe Renault, souligne que « *cette étude du CDSE nous est très utile, car elle décrit de manière très complète les métiers sécurité-sûreté. Elle peut servir de référence de base lorsque des travaux sont menés au sein de l'entreprise sur l'organisation ou la réorganisation de la direction sécurité-sûreté.* »

Voici les grands enseignements de l'étude du CDSE sur les métiers de la filière sécurité-sûreté en entreprise.

UNE FILIÈRE STRATÉGIQUE QUI ÉVOLUE VERS UN RÔLE DE CRÉATION DE VALEUR

Il s'agit du premier enseignement de l'étude, la direction SCC est **un interlocuteur privilégié des gouvernances et un acteur stratégique de l'entreprise.** Bien que la fonction soit encore méconnue, celle-ci se révèle stratégique, au cœur des enjeux de l'entreprise et de son fonctionnement : **dans 74 % des entreprises, la direction sécurité-sûreté corporate est rattachée à la direction générale (DG) ou au secrétariat général.** Elle évolue d'un positionnement d'anticipation, de prévention et de protection, perçue comme un centre de coûts, vers un rôle de création de valeur, en véritable Business Partner des directions générales. Le directeur SSC s'efforce donc de transformer cette perception en stratégie de création de valeur.

En effet, la finalité première de cette filière métiers est de contribuer à la performance de l'entreprise en augmentant sa résilience par rapport aux risques et aux menaces qui pèsent sur l'entreprise. À ce titre, sa capacité de prise de recul et d'analyse systémique de la valeur stratégique des éléments à sécuriser est déterminante. La sécurité-sûreté corporate se positionne ainsi de plus en plus comme un avantage concurrentiel, jusqu'à faire partie de la promesse de marque dans des secteurs tels que le tourisme, les parcs de loisirs, les transports publics, la culture et l'agroalimentaire.

L'étude montre en outre que **la fonction SSC s'affirme comme une fonction transverse par essence avec un périmètre « d'entreprise étendue »** qui se traduit par une grande ouverture en interne et en externe. En interne, elle interagit avec toutes les fonctions et tous les métiers de l'entreprise pour intégrer la sécurité-sûreté dans leurs processus, ce qui suppose des relations structurées avec la quasi-totalité des directions de l'entreprise et la co-construction de processus transverses. En externe, elle met en place de nombreuses interactions avec les clients et les fournisseurs, mais aussi avec les institutions et les administrations.

« La caractéristique principale d'une direction SSC est d'être à la fois stratégique et transverse, relève Geoffrey Fournier, director of Health, Safety, Security and Environment du groupe Flex'N' Gate, *cela nécessite une certaine polyvalence. En effet, elle traite d'une multitude de sujets à haute valeur ajoutée en temps contraints, ce qui la rend particulièrement attrayante au quotidien.»* Pour mener à bien ses missions, la direction SSC a besoin d'une connaissance approfondie de l'entreprise (ses métiers, ses marchés, ses clients, ses interlocuteurs), de son fonctionnement et de tisser des réseaux de parties prenantes. Elle doit en outre disposer d'une connaissance fine du fonctionnement et des codes de l'administration.

UNE FILIÈRE MÉTIERS ATTRACTIVE, MULTI-COMPÉTENCES, D'EXPERTISE ET AU LEADERSHIP AFFIRMÉ

La fonction SCC couvre des qualifications très larges, avec quatorze lignes de compétences identifiées, huit postes d'expert déjà définis et des besoins toujours en hausse. Les Directions SSC recourent donc à des experts de plus en plus pointus, mais avec un besoin de compétences comportementales affirmées, notamment de leadership, permettant un décloisonnement et un rayonnement au sein de l'ensemble de l'écosystème.

LES MÉTIERS DE LA SÉCURITÉ-SÛRETÉ

Gouvernance - Pilotage

- Responsable de pôle Sécurité - Sûreté corporate
- Directeur - Directrice Sécurité - Sûreté corporate
- Adjoint Sécurité - Sûreté corporate

Expertise - Conseil - Déploiement

- Gestion de crise et continuité d'activité
- Déplacements professionnels et mobilité internationales
- Intelligence - Sécurité économique
- Protection de l'information
- Sécurité systèmes d'information
- Responsable Sécurité des événements
- Lutte contre la fraude
- Protection des actifs matériels

Veille - Analyse - Suivi

- Analyse Sécurité - Sûreté corporate

ACTIVITÉS OPÉRATIONNELLES (PAYS, FILIALES...)

- Responsable Sécurité - Sûreté d'entité

L'étude démontre que **la filière est particulièrement attractive pour les professionnels issus du régalien et les cadres issus de l'entreprise.** *« C'est une filière attractive par sa vision globale de l'entreprise, par sa forte contribution à l'atteinte de ses objectifs et par ses rémunérations sensiblement supérieures au marché »*, analyse Yann de Kersauson, Director Executive Search du cabinet de conseil en Ressources humaines Arthur Hunt. *« Concernant les directeurs sécurité-sûreté corporate, cette valorisation se justifie par leur expérience, leur expertise et leur capacité de recul pour conseiller et accompagner dans la prise de décision au plus haut niveau de l'entreprise. De surcroît, Ils doivent faire preuve d'une très grande disponibilité. Dans leur mission, ils ont aussi une capacité de prescription qui va jusqu'au droit de veto. Et, selon les situations, ils peuvent engager la responsabilité de l'entreprise. »*

Globalement, **le niveau de rémunération est supérieur de 4 % à 15 % au marché** (toutes filières de métiers, à grading équivalent).

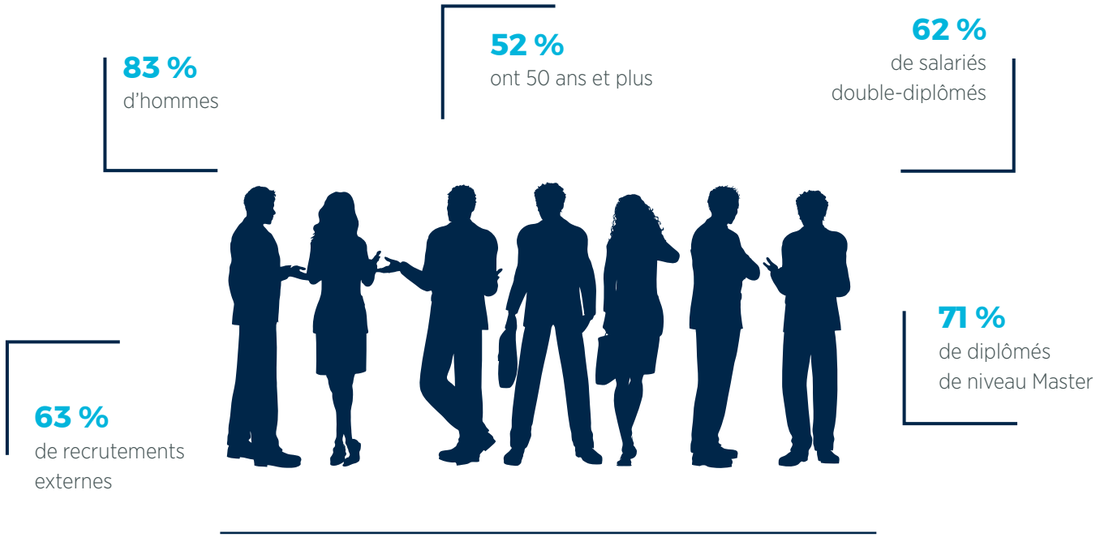
En 2021, 91 % des directeurs SCC sont des professionnels issus d'une carrière dans le régalien. On attend d'un directeur SSC de l'expérience, de la maturité et du leadership, comme l'explique Jean Maurin (Renault) (Cf. encadré p. 26).

La sécurité-sûreté corporate réclame d'avoir le sens de l'intérêt général, d'être passionné mais aussi d'avoir un esprit très curieux et critique, une bonne culture générale à l'international, une éthique, une déontologie, d'aimer l'action car on est proche du terrain, et de pouvoir intervenir dans des postures très variées : management transverse ou hiérarchique, prescripteur, donneur d'ordre, contributeur, capacité d'opposer un véto etc...

Le sens de l'anticipation et des responsabilités, la force de conviction, les capacités d'adaptation aux enjeux de l'entreprise, de conseil et de prescription, de prise de décision rapide sous la pression, la discrétion sur les sujets sensibles, le sens de l'écoute, la capacité à travailler en équipe... sont autant de qualités attendues des directions SSC.

UN BESOIN DE DIPLÔMES & DE FORMATIONS RECONNUES

Autre point saillant, si les femmes sont peu représentées dans les postes de management, comme dans le monde régalien, elles sont en revanche majoritaires dans les postes d'entrées dans la filière, où elles représentent 57 % des analystes en sécurité-sûreté. Une dynamique de féminisation est donc en cours et va prendre encore du temps, car l'expérience est un prérequis pour progresser dans la filière.



PHYSIONOMIE DE LA FILIÈRE SSC

« La montée en compétences et la spécialisation croissante qui caractérise la filière SSC pose de nombreux défis aux nouvelles générations, témoigne Natasha Lery, Analyste Cyber Threat Intelligence au sein de la direction sécurité du groupe Orange. La filière SSC est amenée à attirer de nouveaux talents dans des domaines de pointe tels que la cybersécurité. Face à de nouveaux enjeux sécuritaires, la filière SSC présente des challenges intellectuels et professionnels en constante redéfinition, qui sont passionnants. »

Le constat dressé par l'étude montre que l'expérience prévaut à un cursus académique. Le passage par le régalien et les institutions fait office de parcours de formation et de gage de crédibilité aux postes de management. Pour progresser et se professionnaliser toujours plus et éviter le phénomène de « plafond de verre », la filière doit développer des formations diplômantes et reconnues et favoriser des parcours de carrière intégrant des mobilités externes à la filière (dont public-privé).

Cette dynamique engagée sur la visibilité de la filière, les perspectives d'évolution et les parcours de carrière devrait contribuer à fidéliser et attirer des talents.

Avec de beaux challenges à relever pour les jeunes générations ! ■

> **Pour plus d'informations, nous vous encourageons à vous approprier les principaux livrables de cette étude disponibles sur le site du CDSE > cdse.fr :** le référentiel métiers ainsi que l'enquête des rémunérations et des parcours professionnels.

LEADERSHIP DU DIRECTEUR
SÉCURITÉ-SÛRETÉ CORPORATE

La vision de Jean Maurin, directeur de la Prévention et de la Protection du Groupe Renault

« Leadership, management, gouvernance, pilotage, direction… Beaucoup de mots, dont l'étude des nuances est une mine pour ceux qui conseillent, enseignent, témoignent, postent, vont de leurs citations, tant dans les écoles de commerce, qu'à l'université, lors de colloques ou via les réseaux sociaux professionnels. Ces mots naviguant dans le domaine de la sémantique tentent en fait de dépeindre les différentes facettes de l'art d'exercer son autorité pour la réussite d'une cause commune.

Fédérer un collectif humain et mobiliser des ressources pour atteindre des objectifs précis n'a rien d'exceptionnel, c'est le lot de tout responsable, qui s'appuie sur des fondamentaux solides, reste pragmatique et fait preuve d'intelligence de situation.

En quoi le directeur sécurité-sûreté corporate serait-il ou devrait-il être différent pour assumer son autorité ? À mes yeux, il n'est pas différent de tout autre chef, mais doit porter une attention particulière aux points suivants :

DESCENDRE DANS L'ARÈNE

En se mêlant, ne serait-ce qu'un peu, à la réalité des épreuves quotidiennes de ceux qui exécutent les missions de sécurité et de sûreté dans les sites. C'est un principe de vie générale : on a tout intérêt à descendre dans l'arène de la réalité et à connaître les missions de la base si on veut les comprendre au mieux. Comprendre le fonctionnement d'un site (usine…) permet de connaître ses forces et ses faiblesses et aussi celles de l'entreprise, les rouages plus ou moins huilés entre ses différents services, son environnement tant interne qu'externe. Cette connaissance de la « vie série » permet aussi de percevoir le bon sens de terrain qui anime les équipes, et de mettre de la chair sur des principes, des règlements, des prescriptions. Ce contact, fondé sur l'écoute et la vérité des prix, doit conduire alors à une confiance et un respect réciproques, garants d'une efficacité redoutable en cas de crise, et d'un bon sens partagé lors des prises de décision.

FAIRE PREUVE D'AUDACE

En recherchant toujours à agir par anticipation, à être réactif, à s'adapter en permanence aux évolutions. Pour cela, combattre « la machine à pas faire », en inculquant le culte de la mission et le partage de l'information pour l'atteinte du bien commun. Les personnes qui refusent de bousculer leurs habitudes le font soit par flegme, soit pour ne pas quitter leur zone de confort, soit parce qu'elles ne voient pas la nécessité d'évoluer car elles ne comprennent pas l'urgence de l'adaptation au milieu en pleine évolution. Faire preuve d'audace, c'est d'abord convaincre ses équipes du bien-fondé de la mission confiée.

Faire développer en chacun ses qualités. Sens de la mission, sens de l'engagement, volonté de former, sens de la collectivité, fidélité. Toutes ces qualités ne peuvent être développées que si chacun a la conviction d'appartenir à la même famille qui agit pour le bien commun de l'entreprise. On ne choisit pas ses collègues de travail, comme on ne choisit pas ses parents et ses frères et sœurs, mais l'appartenance à la même famille permet de grandir, d'apprendre, de s'entraider, d'être élevé, de se surpasser, de surmonter ensemble toutes les épreuves, et en fin de compte de vivre pour une cause qui dépasse chacun et le fait participer à un grand récit : la sûreté et la sécurité des personnes et des biens, toutes deux garantes tout simplement de la vie et de l'épanouissement de la famille « entreprise ».

LE DIRECTEUR SÉCURITÉ-SÛRETÉ CORPORATE N'AGIT PAS SEUL

Au contact de ses collaborateurs, comprendre d'abord la vie de l'entreprise et ses enjeux l'aidera à remplir la mission commune, en famille, et à relever avec calme et détermination les défis que l'imprévu posera. »

RECOM > MANDATIONS

> Poursuivre la professionnalisation des équipes en renforçant les parcours de formation technique propres à la filière pour répondre aux besoins croissants d'expertise

> Renforcer la capacité de leadership, notamment en incluant des modules de formation sur les compétences comportementales

> Concevoir des parcours de carrière intégrant des mobilités internes et externes à la filière dans l'entreprise ainsi qu'avec les institutions

> Élaborer des cursus de formation dédiés aux cadres de la sûreté pour améliorer leur employabilité et faciliter leur mobilité

> Développer les métiers pépinières, les rendre attractifs auprès des jeunes

RECOM > MANDATIONS GÉNÉRALES

> Renforcer la professionnalisation de la filière métiers SSC par des cursus de formation dédiés et des parcours de carrière intégrant des mobilités hors de la filière dans l'entreprise et avec les institutions

> Intégrer les processus de sécurité-sûreté au système de management de l'entreprise

À QUELLES QUALITÉS MANAGÉRIALES RECONNAÎT-ON UN BON DIRECTEUR SÛRETÉ D'ENTREPRISE ?

CHRISTOPHE GOMART

Directeur de la sûreté, des risques et de la gestion de crise du groupe Unibail-Rodamco-Westfield

Si l'on pose la question aux présidents directeurs généraux ou directeurs généraux des entreprises qui les emploient, ces derniers répondront qu'en les recrutant, ils souhaitaient des directeurs sûreté qui soient des professionnels de la sûreté et des managers dotés de toutes les qualités de leadership et humaines telles que l'audace, la ténacité, le sens de l'organisation, la sociabilité, l'esprit de décision, l'esprit d'équipe et, si possible… la mise à disposition d'un réseau sécuritaire public. En un mot, la perle rare : un être parfait, grand, beau et fort, autant dire la quadrature du cercle. Cette perle rare peut bien évidemment être une femme ou un homme.

Mais interrogeons-nous sur les qualités spécifiques demandées qui font les bons directeurs sûreté d'entreprise. Il est nécessaire de préciser en début d'analyse que le rôle et le périmètre de leurs responsabilités sont à géométrie (très) variables selon les entreprises. Quand l'un sera strictement en charge de la sûreté et de la sécurité, l'autre traitera aussi de cybersécurité et un troisième englobera la gestion des risques voire l'intelligence économique, sans oublier le dernier qui couvre la sûreté globale de l'entreprise, physique et logique. Il est donc difficile de tenter de définir les qualités en fonction du périmètre de responsabilités.

LE DIRECTEUR SÛRETÉ, UN MANAGER COMME UN AUTRE…

Les qualités de leadership et les qualités humaines (« soft skills ») d'un directeur sûreté en entreprise ne sont-elles pas demandées à tout manager, ou bien s'agit-il de qualités spécifiques ?

Un directeur sûreté est, en effet avant tout, un manager en charge d'une équipe plus ou moins étoffée. Comme à tout manager on lui demande d'être un leader qui pilote une équipe, l'oriente, la dirige dans le but d'atteindre les objectifs fixés dans le cadre du plan stratégique de l'entreprise. Pour cela, il montre l'exemple.

L'exemplarité est la qualité indispensable d'un manager mais surtout celle d'un leader. Faites ce que je fais et non pas uniquement faites ce que je dis. Le bon manager est celui qui unit les talents constituant son équipe pour avancer et gagner ensemble, en sachant que le manager disparaît derrière son équipe. Il est celui qui met en valeur et non celui qui se met en valeur. Le succès de son équipe est celui de son équipe et non le sien, même si son action a été incontournable et indispensable. Le directeur sûreté, comme tous les bons managers, est celui qui ose, celui qui sait faire preuve d'audace à bon escient. Il sait aussi pousser ses équipiers ou collaborateurs à oser. Car si l'on n'ose pas, on n'avance pas et on ne progresse pas. Il est celui qui agit à l'opposé de celui qui attend qu'une solution se dégage d'elle-même à la façon d'Henri Queuille : *« Il n'est pas de problème dont une absence de solution ne finisse par venir à bout ».* Il est celui qui oriente vers une solution et ensuite décide de l'appliquer quand bien même l'idée initiale émane de l'un de ses subordonnés. C'est un chef qui définit une stratégie et sait où il va.

… AVEC DES QUALITÉS SPÉCIFIQUES

Un dirigeant d'entreprise attend de son directeur sûreté, qu'il définisse bien sûr une politique sûreté pour l'entreprise ou le Groupe et qu'il la mette en œuvre. Mais il attend surtout de sa part des qualités indispensables à sa fonction. La première d'entre elles est sans doute sa

capacité à s'adapter à toute nouvelle situation, à une situation changeante et évolutive. **La capacité d'adaptation permet de tirer parti des opportunités, de réagir aux conséquences et de s'adapter aux dommages potentiels.** Réagir rapidement aux changements d'idées, d'attentes, de tendances, de stratégies et autres processus inhérents à toute vie d'entreprise doit être le souci quotidien de tout directeur sûreté. Pour cela, il doit être capable de prendre du recul tout en sachant mettre les mains dans le cambouis lorsque c'est nécessaire. À la fois homme de réflexion et un homme d'action, c'est un homme de terrain. D'ailleurs peu de responsables de niveau « groupe » dans les entreprises connaissent aussi bien le terrain et en ont des retours concrets. C'est en cela que, si l'on regarde les profils des directeurs sûreté, une forte proportion d'entre eux est issue des rangs de la police, de la gendarmerie nationale ou de l'armée française. Leurs qualités sont celles de personnes ayant appris au travers de leurs responsabilités précédentes à agir en temps de crise. Attention, avoir appartenu à l'un de ces milieux n'est pas une condition indispensable pour faire un bon directeur sûreté. S'il s'agit d'une plus-value évidente sur le plan de l'expérience, en termes de prise de décision en mode dégradé et en temps contraint… de plus en plus de directeurs sûreté qui ne sont pas issus des rangs policiers ou militaires arrivent dans les entreprises où ils font un travail remarquable. **Leur force réside bien dans cette capacité d'adaptation à un milieu sécuritaire dont ils ne sont pas issus et qui était jusqu'à une période récente préemptée.**

Cette capacité d'adaptation va de pair avec l'intelligence de situation. Cette qualité permet au directeur sûreté d'avoir une réaction proportionnée à la situation. Grâce à elle, il agit en connaissance de cause en tenant compte de l'environnement, du contexte et des personnes impliqués afin d'être efficace dans sa réaction. Ce n'est pas une qualité innée. Elle s'acquiert en faisant preuve de compréhension rapide des enjeux et des mécanismes invisibles qui régissent les comportements, mais aussi d'empathie.

LE DIRECTEUR SÛRETÉ DOIT ÊTRE CONNU ET RECONNU

Le directeur sûreté ne doit surtout pas rester dans l'ombre au sein de l'entreprise, il doit **être connu et surtout reconnu.** Cette condition est liée à sa capacité à être compris et entendu. Pour cela bien évidemment son expertise en matière de sûreté globale est une condition sine qua non. Mais ce qui compte, c'est sa parfaite connaissance des rouages de l'entreprise et donc son intégration en son sein. Il doit devenir ce que l'on appelle un **« business partner »**. Il est celui qui protège le fonctionnement de l'entreprise et le facilite et pourquoi pas l'accélère autant que possible. Il doit pour cela **faire preuve de créativité**. Une autre de ses qualités devra être **la résilience**, car cette connaissance et cette intégration peuvent prendre du temps, du temps pour connaître, du temps pour comprendre et du temps pour convaincre.

Au-delà d'incontournables « hard skills », on reconnaît un bon directeur sûreté en entreprise à ses qualités de leadership et à ses qualités humaines. Ses qualités sont liées à l'essence même de son métier qui est l'incertitude.

Incertitude face à la menace, incertitude face au comportement des prestataires de sécurité, incertitude face au comportement des employés de l'entreprise en cas d'incident, incertitude face à l'implication des dirigeants de l'entreprise… Pour y faire face, la définition d'une stratégie est la première des conditions. La sûreté étant intimement liée à la crise, le directeur sûreté devra être celui qui, en dépit de la crise, eXntraîne les autres et les fait se dépasser. **Pour cela, il aura besoin d'anticipation, d'adaptation, de compréhension des enjeux, d'humilité, de force d'âme et bien sûr de retour d'expérience.** Enfin, **résolument innovant**, il va de l'avant en prenant en compte les nouvelles technologies et le digital. Car il sait que la sûreté est devenue un différentiateur au profit de la croissance de l'entreprise. ■

RECOM > MANDATIONS

> Manager, le directeur sûreté doit être exemplaire

> Homme de réflexion et homme d'action, le directeur sûreté doit faire preuve de capacité d'adaptation, de prise de recul et d'intelligence de situation

> Le directeur sûreté ne doit surtout pas rester dans l'ombre au sein de l'entreprise, il doit être connu et surtout reconnu

> Business partner, le directeur sûreté doit parfaitement connaître les rouages de l'entreprise et faire preuve de résilience et de créativité

LA CRÉATION D'UNE DIRECTION DE LA SÛRETÉ EN 2022 : L'EXEMPLE RÉCENT DE PERNOD RICARD

SERGE COLLIGNON
Directeur sûreté du groupe Pernod Ricard

Pragmatisme, ouverture et agilité sont les maîtres mots lors de la création d'une direction de la Sûreté au sein d'une entreprise, surtout lorsqu'il s'agit d'un grand groupe international comme Pernod Ricard, leader dans son secteur.

J'ai rejoint le siège de Pernod Ricard en 2018, qui était alors l'un des derniers groupes du CAC 40 à ne pas disposer d'une direction de la Sûreté. Ces questions n'étaient pour autant pas absentes des préoccupations de la direction générale de ce fleuron de l'économie tricolore, qui a toujours veillé au strict respect de ses obligations en la matière. De fait, une société comme Pernod Ricard, numéro deux mondial des vins et spiritueux, avec près de 19.000 collaborateurs dans plus de 86 pays, est nécessairement confrontée régulièrement à des problèmes de Sûreté. Néanmoins, entreprise familiale et décentralisée, ces fonctions sont très présentes dans l'organisation de Pernod Ricard mais le groupe ne disposait d'une vision centrale, corporate.

De fait le responsable de la Sûreté qui met en place cette nouvelle fonction au sein d'un groupe de cette envergure n'endosse pas le costume d'un révolutionnaire. Il doit se mettre au service des autres départements, en rencontrer tous les responsables et commencer à cartographier patiemment toutes les mesures ou politiques qui sont déjà effectives comme celles qui doivent l'être à l'avenir.

Le siège, qui représente moins de 3 % des effectifs, est chargé de définir la stratégie. Les plus de 80 filiales directes dans le monde sont constituées de six grandes sociétés de marques en charge de fabriquer nos produits (Chivas Brothers à Londres, Irish Distillers à Dublin, the Absolut Company en Suède, Winemaker en Australie, Havana Club à Cuba et Martell/Mumm/Perrier Jouët en France), qui seront ensuite distribués par nos sociétés de marché des États-Unis au Japon, en passant par le Mozambique. Du fait de cette grande diversité culturelle et géographique et en l'absence de Directeur de la Sûreté pour le Groupe et de règles communes, il existe de grandes disparités dans les solutions et les pratiques qui avaient été mises en place (ou non) dans toutes ces filiales.

FAIRE ÉMERGER LA FONCTION, SE FAIRE CONNAÎTRE ET RECONNAÎTRE

Le directeur de la Sûreté se doit d'expliquer clairement l'importance de ces enjeux et d'incarner ses différentes composantes, souvent éclatées entre différents départements, parfois perçues uniquement comme des contraintes avec une forme d'ambiguïté entre les notions de Sûreté et de Sécurité. L'ambition de la nouvelle direction de la sûreté est donc de rationaliser ces politiques, de mieux les expliciter afin d'instiller cette culture de la sécurité. En effet, une entreprise du secteur agro-alimentaire, qui n'est pas une OIV, peut faussement considérer qu'elle est immune à certains enjeux comme le vol de données. Or, un grand groupe coté comme Pernod Ricard qui dispose de joyaux dans son portefeuille de marques et enregistre de solides performances ne peut que susciter les curiosités, y compris malveillantes. Il doit donc protéger ses intérêts.

Faire émerger la fonction et se faire connaître constitue ainsi le premier enjeu. À cet égard, le rattachement de la fonction à un membre du Bureau Exécutif, en la personne du Directeur des Ressources humaines Cédric Ramat, et la proximité du General Management ont été déterminants pour rencontrer rapidement les principaux dirigeants du groupe lors de leur passage au siège. Si la crise sanitaire du COVID a par la suite constitué un catalyseur, elle a aussi accéléré l'intégration d'une Direction de la Sûreté en contribuant directement à la sécurisation des approvisionnements en masques.

Car le deuxième enjeu primordial sera de se faire reconnaître et d'apporter une plus-value sous la forme d'une aide ou d'un soutien concret aux problématiques rencontrées par les filiales. C'est là assurément un positionnement au profit du « client » (*« consummer centric »* selon la terminologie interne à Pernod Ricard). Cela nécessite une agilité certaine pour identifier et collecter les besoins en tenant comptes des spécificités locales. Disponibilité et réactivité sont dès lors primordiales dans la prise de décision. En contrepartie, l'une de mes très grandes satisfactions au quotidien réside dans la diversité des échanges puisque j'interagis avec la quasi-totalité des entités du groupe et sur une formidable variété de sujets.

Afin de ne pas se perdre dans autant d'enjeux, il faut distinguer le temps long du temps court, distinguer ce qui est important de ce qui est urgent : répartir son action entre la création du poste et la réponse aux urgences en veillant notamment à combler les carences dès qu'elles sont identifiées, et ce sans oublier de suivre les crises dans le temps.

RECONSIDÉRER SON RÔLE ET SON DOMAINE DE COMPÉTENCE EN PERMANENCE

Construire sa fiche de mission est à ce titre une opportunité exceptionnelle et une expérience passionnante qui impose de reconsidérer en permanence son rôle au sein de l'entreprise et son domaine de compétence. Après seulement deux ans, mon périmètre a considérablement évolué par rapport à la feuille de route que j'avais proposée au moment de mon recrutement. L'actualité s'est imposée à moi autant qu'à tous mes homologues dans le monde ; la crise du

COVID a nécessairement bouleversé les priorités initiales comme il a profondément reconfiguré l'environnement dans lequel j'évolue. Preuve en est la nécessité « nouvelle » de répondre prioritairement au Duty of care en contribuant à la santé et à la sécurité de nos voyageurs et expatriés. Par ailleurs, alors que ma fonction ne couvrait initialement que la Sûreté, elle a été étendue depuis l'été 2021 au Health & Safety, pour tous les sites et filiales non industrielles.

La politique santé et sécurité de Pernod Ricard constitue l'une des premières priorités identifiées, avec pour ambition de figurer parmi les meilleures du secteur. L'intégration et la prise en compte des problématiques H&S (pour une partie conséquente du groupe) et auxquelles je n'étais pas formé, constituent en soi un challenge qui a demandé un investissement personnel conséquent. Grâce au soutien interne dont j'ai pu bénéficier et en dépit du surcroît d'activité généré, cet élargissement de mon scope m'a permis de renforcer les actions que j'avais engagées au titre de la Sûreté et de créer des synergies entre Sûreté et Sécurité. À titre d'illustration, les règles qui s'imposent notamment aux voyageurs et aux expatriés comme à leur gestion, figurent désormais dans le socle commun minimal en matière de politique Health & Safety.

Dans les missions d'un directeur de la Sûreté à l'écoute des besoins réels de sa société, rien n'est ainsi figé. La clef de la réussite réside à mon sens dans la capacité à adapter sa feuille de route, ce qui apporte nécessairement son lot de petites frustrations, mais surtout de nouvelles opportunités et de nouveaux challenges à relever.

Je vais prochainement bénéficier d'un renfort pour mener à bien les missions qui m'ont été confiées, avec deux réseaux à animer et à former, les réseaux des « référents Sûreté » et les réseaux des points de contacts et des « coordinateurs Santé et Sécurité ». Avec de nouvelles procédures de sûreté des sites à rédiger et à implémenter, avec la veille économique à développer, l'intégration des nouveaux risques, la révision des modèles de gestion de crises, les synergies à développer avec la direction de la cybersécurité, la valorisation des réseaux, l'amélioration de la sécurisation du siège et des événements..., les enjeux sont nombreux et variés. Dans un monde où le risque est de plus en plus présent et polymorphe, mis à rude épreuve par la crise sanitaire, la direction de la sûreté doit faire partie intégrante de la gouvernance d'une entreprise de dimension internationale. ■

RECOM > MANDATIONS GÉNÉRALES

- **> La direction de la sûreté doit faire partie intégrante de la gouvernance de l'entreprise**
- **> Rationaliser les politiques de sécurité existantes, mieux les expliciter afin d'instiller une culture de la sécurité**
- **> Se mettre au service de tous les départements de l'entreprise**
- **> Faire émerger la fonction pour se faire connaître puis reconnaître en apportant une plus-value concrète aux filiales**
- **> Faire preuve de pragmatisme, ouverture et agilité : reconsidérer en permanence son rôle au sein de l'entreprise et son domaine de compétence**
- **> Répartir son action entre la création du poste et la réponse aux urgences, suivre les crises dans le temps**

LA NÉCESSAIRE COPRODUCTION DE SÉCURITÉ

ÉMILE PEREZ

Directeur de la sécurité et de l'intelligence économique du groupe EDF
Vice-président du CDSE en charge de l'International

Dans toute société, comme dans toute entreprise, quelles que soient sa taille et sa nature, la fonction sécurité est primordiale.
La sécurité (ou sûreté sur les acceptions des termes) est en effet **la protection du patrimoine de l'entreprise contre tout acte de malveillance.**

Et le patrimoine d'une entreprise est toujours des plus diversifiés : son patrimoine humain, tout d'abord, sa plus grande richesse, les femmes et les hommes qui composent la force vive de l'entreprise ; son patrimoine immobilier ; son patrimoine immatériel, son savoir-faire, ses informations… ; sa production, son activité commerciale et financière…

FACE À LA MENACE…

Il s'agit de protéger tout cela **contre les risques et les menaces** de toutes natures et de tous impacts, d'où qu'ils viennent. L'entreprise peut être la cible d'attaques de la part d'individus, de concurrents, d'organisations terroristes, criminelles ou de gouvernements. Et aujourd'hui plus que jamais, l'expression de cette menace peut prendre le caractère plus dangereux ou pernicieux, **des attaques cyber**, elles-mêmes d'origine criminelle, terroriste ou étatique.

Ce n'est pas qu'un scénario de cinéma, c'est la vie de tous les jours.

L'entreprise reste une cible potentielle, ou un lieu d'expression de ces phénomènes de radicalisations ou de criminalisation, avec toutes les conséquences que cela peut avoir en termes d'image et de coût social ou financier.

Bref, cette menace est globale. Mais la traduction de l'activité malveillante, criminelle ou terroriste est toujours locale. C'est ce que j'appelle la **GLOCALISATION**. Cela tombe toujours quelque part en France ou dans le monde. Et cela peut impacter les intérêts de l'entreprise, nos intérêts, où qu'ils se trouvent. Dès lors, il faut **être prêt en permanence et partout** où notre entreprise est représentée. Notamment à l'international, quand nos agents, expatriés ou en mission, sont éloignés de leur base.

Et n'oublions jamais, qu'il en est de même pour le service public de la sécurité porté par différents services de l'État.

La sécurité que nous mettons alors tous en œuvre, dans le respect des lois et règlements et également de nos prérogatives propres, doit nous permettre **d'anticiper et de prévenir** ces risques et ces menaces.

La sécurité doit, elle-aussi, être glocale : globale pour couvrir parfaitement tous nos intérêts, tout notre patrimoine face à toutes les menaces ; locale pour être parfaitement adaptée au niveau du terrain. Sinon, nous risquons de paralyser notre propre activité.

En plus des nécessaires actions de sensibilisation ou de formation en interne pour y développer une véritable culture de sécurité, il convient dès lors de renforcer la coopération étroite entre l'entreprise et chacun des services concernés de l'État, ou de partenaires privés, tant aux niveaux international, national que local.

LA NÉCESSAIRE COPRODUCTION INTERNE…

Face aux risques et menaces pouvant affecter les intérêts de l'entreprise, il est impératif de conforter, voire de faire évoluer, les dispositifs de prévention, de dissuasion ou d'intervention. L'entreprise seule ne peut y parvenir. Il s'agit ici de développer, tant en interne qu'en externe, un véritable **maillage** « sécuritaire » de l'entreprise, de renforcer ses aptitudes de **réseautage** pour démultiplier ses capacités et de systématiquement organiser le **partage** de l'information permettant les décisions adaptées.

Pour que dans ce domaine, la relation entreprise-État soit efficiente, encore faut-il qu'en interne de l'entreprise, la culture de sécurité soit vraiment partagée. Il convient ici de tous se mobiliser, et ce n'est pas toujours chose facile…

En interne, au niveau de l'entreprise, la signature et la mise en application d'une **politique de sécurité du patrimoine face à la malveillance en général** permet de faire progressivement évoluer la « culture sécuritaire » partagée au sein de chacune des entités et des filiales. La désignation d'un **responsable ou un correspondant de la sécurité du patrimoine** pour chacune de celles-ci facilite les conditions d'un maillage serré permettant de déceler, le plus en amont possible, risques et menaces sécuritaires.

En termes de prévention des crises, toute entreprise doit bien se doter, avec une politique globale de gestion et de contrôle des risques ou une politique de gestion de crise permettant une maîtrise des situations. Reste à conforter un dispositif de réseaux (veille, alerte, conseil, risques nouveaux et signaux faibles) et de partage de l'information.

La relation étroite avec les directions Métiers est primordiale comme le montre bien le développement de manière coordonnée de **programmes sécuritaires partagés.**

Sur la base d'un dispositif d'alerte et de déclenchement bien préparé, avec des systèmes de permanence et de remontée des alertes, une articulation avec les pouvoirs publics et les cellules de crises à différents niveaux et la mise en œuvre des Plans de continuité et de reprise d'activité (pandémie, systèmes d'informations, continuité électrique…, VIGIPIRATE), l'entreprise se doit de développer, pour l'ensemble des directions concernées, une **cellule stratégique de crise** sur des domaines des plus divers.

D'une manière générale, dans les trois phases, de prévention, de dissuasion ou d'intervention, le **principe de défense en profondeur** est plus que jamais de mise. Il s'agit ici d'exploiter plusieurs techniques de sécurité afin de réduire le risque lorsqu'un composant particulier de sécurité est compromis ou défaillant. Cela rendra plus complexes des actes préparatoires ou des tentatives de commission d'actes malveillants, criminels ou terroristes. Dans ce domaine également, la coproduction partenariale est fondamentale, comme le démontre au quotidien l'action de certaines unités étatiques au sein d'installations sensibles.

Enfin, pour mieux se préparer à l'intervention, la mise en œuvre d'exercices de simulation et d'inspections internes ou externes est des plus primordiales. Ils permettent de bien déterminer les conditions d'intervention des unités concernées et les mesures d'amélioration à prendre en termes de sécurité.

Au sein de l'entreprise, la prise en compte de la sécurité ou de la sûreté reste donc une **affaire de coproduction interne intelligente,** dans le respect des prérogatives et des obligations de chacun, y compris de celles du directeur de la sécurité.

ET EXTERNE…

Au-delà de l'entreprise, il est tout aussi nécessaire de marier les forces alors que nous sommes tous démunis, en situation de faiblesse face à certains risques ou à certaines menaces. Nous devons d'autant plus le faire que l'État lui-même ne peut plus tout… et que le monopole étatique de sécurité est en crise.

Quelle que soit la taille de l'entreprise, reste impérative la nécessité d'une **véritable coproduction externe de sécurité t**ant avec les partenaires étatiques que les prestataires privés de sécurité, d'intelligence stratégique ou économique. Dans cette même logique de maillage, l'échange et le partage entre pairs est primordial pour les entreprises, qui se sont mobilisées depuis longtemps pour créer des liens entre elles, profitant souvent du profil particulier de beaucoup de leurs directeurs de sécurité ou de sûreté, anciens des services et autres ministères. C'est ainsi qu'est né le Club des directeurs de sécurité des entreprises (CDSE) en 1995, et c'est ainsi qu'il perdure et évolue.

La nécessaire coproduction Entreprise-État passe d'abord par la complémentarité des mesures prises. S'il revient à l'entreprise de prendre en compte la conception et l'exploitation de ses installations (configuration des installations, conduite, maintenance, protection des sites, gardiennage…), de remplir son devoir d'information aux pouvoirs publics, ou d'avoir une connaissance précise des matières détenues par exemple ; restent du domaine de l'État la prévention du terrorisme, le renseignement, l'interdiction de survol des sites sensibles, la surveillance rapprochée des sites, l'intervention en cas d'intrusion…

Ici encore, **le partage des informations est essentiel,** et pas seulement au niveau central. C'est ce que l'on doit s'évertuer à formaliser ainsi qu'à développer **entre les entreprises et les différents acteurs étatiques :** ministères de tutelle le cas échéant, Intérieur, Armées, Europe et Affaires étrangères - MEAE, Secrétariat général de la défense et de la sécurité nationale - SGDSN, ANSSI, COSSEN en fonction des secteurs d'activité.

La bonne connaissance des rouages étatiques est donc des plus utiles, car elle conditionnera la qualité des relations avec les services de l'État dans tous les aspects de la protection du patrimoine. Dès lors, il ne sera pas rare d'échanger avec la sécurité publique de la Police nationale, la Préfecture de Police ou la Gendarmerie, avec les représentants des services de renseignement intérieur ou extérieur, le centre de crise et de soutien du MEAE, les services des ambassades et autres consulats, ou la direction de la coopération internationale (de sécurité)…

Pour renforcer **la confiance réciproque,** il conviendra de bien décliner ces modalités d'échanges face à cette menace « glocale », au niveau local (en France comme à l'étranger).

Dans le respect des lois et règlements, au travers de criblages, d'échanges de terrain, il sera alors plus constructif de **partager l'information de façon précoce** pour mieux détecter et contrer toute menace pouvant affecter la collectivité au sein ou en dehors de l'entreprise.

En effet, le développement systématique de cette coproduction, tant pour l'entreprise que pour les services de l'État, permettra de toujours mieux contrer la menace, et notamment la menace terroriste, qu'elle soit interne ou externe.

Progressivement, les uns et les autres ont compris la possibilité et la nécessité faire coïncider leurs objectifs dans **une relation gagnant-gagnant** où l'entrepreneur, voire l'administration, s'engage à accepter un certain niveau d'incertitude et le chercheur à s'assurer du réalisme des solutions proposées.

D'où une réflexion forte lancée en 2008 dans le domaine de la formation et de la recherche stratégiques. Sous l'égide du **SGDSN**, la coordination et la mutualisation sont désormais de mise entre les ministères et les grandes entreprises, et l'ont été au travers du **Conseil Supérieur de la Formation et de la Recherche Stratégiques – CSFRS** qui associait notamment ce que font des structures comme l'IHEDN ou l'INHES-J (devenu l'IHEMI).

Dans le prolongement de ces recommandations et du *« Livre blanc sur la défense et la sécurité »*, les organes de la filière industrielle de sécurité dont le **Comité de Filière de l'Industrie de Sécurité (COFIS) et le Conseil des Industries de la Confiance et de la Sécurité - CICS,** ont été constitués simultanément en 2013, pour finalement donner naissance en 2018, sous l'égide du ministère de l'Industrie, au **Comité Stratégique de la Filière (CSF) des Industries de sécurité.** Cette instance est un bon exemple de coproduction puisqu'elle regroupe au sein de sa gouvernance les offreurs (grands industriels, PME, start-up), les clients-utilisateurs, représentés notamment par le CDSE, et l'État. Mais tout cela reste fragile, tous ne percevant pas la **nécessité d'inscrire dans la durée, ce pari du partage entreprise-État.**

AUTOUR D'UNE CONFIANCE PARTAGÉE

En 2018, sous l'impulsion du Premier ministre Edouard Phillipe, le ministère de l'Intérieur lançait une vaste réflexion sur le « continuum de sécurité », confiée aux députés de la majorité Alice Thourot et Jean-Michel Fauvergue (également ancien chef du RAID). Ces travaux se sont concrétisés en plusieurs phases : d'abord le rapport Thourot/Fauvergue remis au Premier ministre en septembre 2018, puis un Livre blanc de la sécurité intérieure publié en novembre 2020, une proposition de loi Thourot/Fauvergue et enfin une loi *« pour une sécurité globale préservant les libertés »* promulguées en mai 2021. Le CDSE a été associé à chaque étape de cette réflexion et a ainsi pu porter **13 propositions** (Cf. encadré), dont un bon nombre - sur la profession d'agent de sécurité privée notamment - ont été reprises dans la loi.

Les 13 propositions du CDSE dans le cadre de la réflexion sur le continuum de sécurité

> Pour un continuum de sécurité animé par l'échange d'informations

1. Faciliter les échanges d'informations public/privé dans un « cercle de confiance »

> Pour un usage encadré et décomplexé des nouvelles technologies de sécurité

2. Doter la biométrie et la reconnaissance faciale de règles d'emploi sous le contrôle strict de la CNIL
3. Réviser les normes techniques de la vidéosurveillance/vidéoprotection et faciliter l'interopérabilité de réseaux
4. Instaurer un criblage des entreprises digitales candidates à des marchés sensibles
5. Faire émerger une solution de cloud « souverain » ou de « confiance » compétitive

> Pour une profession d'agent de sécurité privée qualifiée et renforcée

6. Instaurer une garantie financière pour les entreprises de sécurité privée
7. Instaurer une limitation de la sous-traitance à un niveau dans les prestations de sécurité privée
8. Publication systématique des sanctions prononcées par le CNAPS pour les entreprises et les dirigeants
9. Instaurer un uniforme unique et de qualité pour les agents de sécurité privée
10. Instaurer une protection juridique des agents de sécurité
11. Renforcer la professionnalisation de la filière et la qualité de la formation
12. Intégrer la sécurité incendie au sein du livre VI du code de la sécurité intérieure
13. Intégrer les activités des entreprises de services de sécurité et de défense au sein du livre VI du code de la sécurité intérieure

La proposition n°1 portait sur la constitution d'un cercle de confiance permettant de faciliter les échanges d'informations entre le public le privé :

1. Faciliter les échanges d'informations public/privé dans un « cercle de confiance »

Depuis décembre 2018, chaque samedi de manifestation du mouvement dit des « Gilets jaunes », le CDSE est informé en temps réel de l'évolution des événements par le cabinet du préfet de police de Paris. Il s'agit d'un lien précieux pour les entreprises qui peuvent se prémunir au mieux des actes de malveillance qui peuvent accompagner ce mouvement.

Afin de donner corps au *continuum* de sécurité, aux évolutions des métiers de la sécurité au sein des entreprises, et à la reconnaissance des directeurs de sécurité comme interlocuteur privilégié, l'État pourrait favoriser ce type d'échange d'informations opérationnelles avec les entreprises en l'étendant à l'échelle du territoire national et à des sujets plus sensibles grâce à la constitution d'un « cercle de confiance ». Celui-ci serait constitué de « référents entreprise » soumis à une procédure d'habilitation préalable ou à un criblage.

Si cette proposition a été retenue dans les préconisations du rapport Thourot/Fauvergue[1], puis dans les conclusions du *Livre blanc de la sécurité intérieure*[2], elle n'a cependant pas trouvé de concrétisation dans la loi. On peut ainsi regretter une occasion manquée, d'autant qu'il ne s'agit pas là d'une préconisation nouvelle pour les directeurs de sécurité en entreprise : celle-ci figurait déjà dans le premier Livre blanc du CDSE, en 2011.

L'ensemble des mesures et des actions de protection que nous mettons en place au sein de l'entreprise vise un double objectif : **protéger et développer.** Protéger notre patrimoine (à commencer par l'humain donc) et continuer à développer notre activité d'entreprise sans rupture profonde.

[1] *« D'un continuum de sécurité vers une sécurité globale »*, Rapport de la mission parlementaire Thourot/Fauvergue, septembre 2018, page 58 : *« Proposition 14 : revaloriser le rôle et le positionnement des directeurs de la sécurité dans les entreprises :*
- *créer un statut de correspondant sécurité (CS) au sein des entreprises ;*
- *faire agréer par le CNAPS les candidats à un poste de correspondant sécurité ;*
- *ouvrir la possibilité d'habiliter les titulaires de ces fonctions au confidentiel-défense. […] »*

[2] *« Livre blanc de la sécurité intérieure »*, novembre 2020, page 155 : *« Les directeurs de sécurité des entreprises sont des parties prenantes au continuum de sécurité […] ; « Proposition : renforcer la reconnaissance du rôle des directeurs de sécurité en entreprise dans le continuum et les intégrer dans l'animation du continuum par la mise en place d'une relation de confiance mutuelle partageant le secret. […] »*

Avec l'ensemble des acteurs, nous le voyons, les choses avancent, mais comme souvent en matière de coopération : par empilement au gré des réponses immédiates à apporter aux crises ou aux failles successives. C'est le cas en matière de coopération internationale, c'est le cas pour la coproduction nationale que nous souhaitons tous renforcer dans le respect des prérogatives de chacun, mais aussi dans l'intérêt de tous.

Vision globale et stratégie inclusive doivent encore être renforcées. Car ici, la seule véritable question pour nous tous demeure :

Quelle est la menace la plus importante pour l'entreprise comme pour la société dans son ensemble : l'intensification de la coopération, de cette nécessaire coproduction interne comme externe, ou l'intensification des actes de terrorisme, de criminalité ou de simple malveillance ? ■

RECOM > MANDATIONS

CONDITIONS DE LA RÉUSSITE & PROPOSITIONS SPÉCIFIQUES

Trois conditions générales

Parmi les conditions de la réussite, figure cette nécessaire coproduction que j'ai évoquée tout au long de mon propos. Tant pour sa mise en œuvre que dans ses résultats, il convient de toujours marteler ce triptyque maillage, réseautage, partage.

- **1. Un maillage fort des territoires, des domaines de chacun, des problématiques pour être en capacité de mieux déceler de façon précoce menaces et risques**
- **2. Un réseautage maîtrisé qui nous permettra de démultiplier nos propres capacités en permettant à chacun de compter sur et pour ceux qui sont ainsi reliés**
- **3. Un partage largement ouvert de nos savoirs, savoir-faire et savoir-être, de nos informations pertinentes.**

Une proposition spécifique du CDSE formulée depuis 2011

- **4. Faciliter les échanges d'informations public/privé dans un «cercle de confiance»**

II. FONDAMENTAUX & MISSIONS DE LA FONCTION SÛRETÉ

LE DIRECTEUR SÉCURITÉ FACE À L'INTERNATIONAL : LA VISION D'ARNAUD KALIKA (MERIDIAM)

ARNAUD KALIKA

Directeur de la sécurité de Meridiam et président de la commission « International » du CDSE

S'il fallait trouver un point de convergence entre les attentats du Bataclan le 13 novembre 2015, la crise en Chine méridionale, l'annexion de la Crimée puis l'invasion de l'Ukraine par la Russie, les charniers éthiopiens, la guerre du Haut-Karabakh et la pandémie de la Covid-19, ce serait peut-être le retour au réel. Même si ces drames avaient tous fait l'objet d'anticipation dans les documentations respectives de l'ensemble des services de renseignement de la planète, la sidération couplée à la surprise d'un réel d'une extrême violence a désarçonné les plus aguerris. Un réel implacable qui nous saute aux yeux et à propos duquel nous savons parfaitement qu'il peut advenir tout en restant trop souvent aveugle à ses signaux faibles. Le directeur de la sécurité est l'acteur du réel. Il est là pour bousculer les plus frileux face aux menaces qui viennent, afin d'anticiper et de préparer des solutions.

L'enracinement du fait terroriste parmi des entrepreneurs de violence toujours plus créatifs est une évidence qui constitue le fil d'airain de l'insécurité au XXIe siècle. Les simplifications du monde savamment distillées dans le sillage de la dissolution de l'URSS ont fait long feu : nous savons tous que ce que nous vivons est bien différent de ce qu'une poignée d'intellectuels de salon ont pu vendre au travers de « la fin de l'Histoire » ou encore du « choc des civilisations ». Le monde a quitté la camisole des concepts pour faire corps avec le concret braudélien. Une réalité difficile qui met à l'épreuve le directeur de la sécurité. Il ne peut plus simplement être le faire-valoir isolé d'un CEO en quête de notoriété ; il doit plonger les mains dans le cambouis pour devenir en quelque sorte l'assurance vie du développement économique de l'entreprise, de la sécurité des expatriés en passant par le risque réputationnel et la protection de son patrimoine matériel et immatériel.

RISQUE GÉOPOLITIQUE & DÉVELOPPEMENT ÉCONOMIQUE : LE MARIAGE FORCÉ

Dans l'écosystème de l'entreprise, il y a ceux qui considèrent que la signature d'un deal prime sur le reste, reléguant les fonctions supports dont fait partie la « sécurité » à un rôle de figurant, voire de « fou du Roi ». La case est cependant cochée pour la norme ISO puisque le directeur de la sécurité a été, à un moment, dans la boucle. Une telle vision du développement place le directeur de la sécurité comme un simple centre de coût, un empêcheur de tourner en rond qu'il convient de « neutraliser » administrativement.

Bien entendu, une telle approche est une erreur primaire qui ressemble à la faute du débutant aux échecs qui tombe dans le piège du « mat du berger ». À l'heure de l'anthropocène, de la finance durable et des marchés responsables, les seules entreprises qui survivront seront celles qui épouseront la vision du long-terme et positionneront la sécurité comme pivot du développement.

Ce directeur de la sécurité « pivot » bénécifie d'une vision à 360 degrés pour mieux dérisquer sur le long terme. Dans son portefeuille international, le risque géopolitique est son cœur de cible. En effet, personne ne peut plus aujourd'hui investir sur le long terme dans des géographies même anodines comme la Finlande ou le Chili sans prendre en compte ce risque. À charge pour chaque entreprise et son directeur de la sécurité de bâtir, en fonction d'intérêts propres, une matrice et des procédures produisant des indicateurs objectifs projet par projet ; chaque critère de notation enclenchera une forme d'action à la fois en anticipation et en réaction.

Le risque géopolitique ne peut pas être industrialisé ; il convient de le traiter de façon artisanale en adéquation avec la vision stratégique de l'entreprise.

Ainsi, se lancer dans un projet économique au Maroc impose au préalable l'examen minutieux de la géopolitique du Royaume, procédant de l'analyse de ses menaces intérieures et extérieures, voire d'une cartographie des acteurs qui comptent par rapport au marché envisagé. Une analyse qui peut être internalisée (c'est généralement mieux mais cela implique l'embauche d'un directeur de la sécurité éveillé à ce type de sujets) ou externalisée. Les résultats des analyses sont partagés en réunion de management du projet, le directeur de la sécurité devant nécessairement être intégré à tous les développements. Le partage de l'information est stratégique parce qu'en géopolitique personne n'est propriétaire d'une tendance ou d'un signal faible.

Plus aucun CEO ne peut se permettre d'attaquer un marché sans passer par l'antichambre de la sécurité qui doit dérisquer son développement. Il s'agit, certes, d'un « mariage forcé » en raison d'une pression de l'insécurité globalisée, mais surtout d'un mariage auquel ne pas consentir équivaudrait à un aveuglement.

LES OUTILS DE L'INTERNATIONAL AU SERVICE DES EXPATRIÉS

Investir le champ international implique d'une part de s'équiper, et d'autre part de se constituer un réseau d'experts. Autant d'éléments qui en apparence semblent abstraits, mais qui en pratique peuvent permettre d'anticiper des crises et des désagréments pour les expatriés.

> **S'ÉQUIPER EN GÉOPOLITIQUE :** le directeur de la sécurité ne peut pas se permettre d'être l'otage des grands quotidiens, des agences de presse ou des youtubeurs de tous poils. Il doit anticiper et en savoir plus que les autres. S'équiper en géopolitique, c'est donc d'abord faire un travail sur soi pour s'extraire de tous préjugés. En géopolitique, il n'y a pas de place pour les égos, encore moins pour les théories du « souverain bien ». En la matière, il n'existe malheureusement aucune solution miracle, ni prestidigitation. Il faut lire un maximum en prenant des notes, noircir des « petits cahiers », plonger dans l'histoire, l'ethnologie, croiser les perceptions, arpenter le terrain… C'est ensuite savoir trier le bon grain de l'ivraie parmi les informations qui nous arrivent à portée de smartphone. Ne pas se laisser ligoter par les nœuds de l'infosphère et des réseaux sociaux où chaque tweet chasse l'autre. Souvent ingrat, cette partie du travail du directeur de la sécurité implique de pouvoir s'isoler, appuyer sur le bouton « arrêt sur image » et réfléchir avant de livrer ses vues au niveau stratégique, voire au CEO. Sur ce plan, constituer une équipe d'analystes internes à la direction sécurité-sûreté issus d'horizons variés (universitaires, sciences politiques, diplomatiques, intelligence économique), aux savoir-faire multiples et spécifiques (OSINT…) peut s'avérer stratégique.

> **SE CONSTITUER UN RÉSEAU D'EXPERTS :** trop souvent, les directeurs de la sécurité s'orientent vers les sociétés d'intelligence et autres cabinets de renseignement privés pour avoir des informations de nature géopolitique alors que la seule expertise de qualité dans ce domaine réside dans les « think tanks », les universités et les correspondants du réseau diplomatique français. Il ne faut rien s'interdire parce que les « think tanks » touchent l'académique, avec lequel le directeur de la sécurité doit tisser des liens. Le « think tank » est le réservoir d'experts dont l'entreprise a souvent besoin mais dont elle se prive par méconnaissance ou préjugés. Quant au réseau diplomatique, le Centre de Crise et de Soutien du Quai D'orsay (CDCS) est au service des entreprises, un appui indispensable à toute gestion du risque international. Lorsque je me rends dans une nouvelle géographique, mon premier réflexe est, sur la partie géopolitique, de prendre rendez-vous avec les différents recteurs d'universités du pays en question pour connaître leur ressenti sur la situation générale et très souvent, je sors de ces entretiens avec une mine d'informations. Il en est de même pour le réseau diplomatique, qu'il faut aller rencontrer sur place, pour y partager des perceptions, des craintes… Marche après marche, le réseau se constitue et s'entretient, parfois en synergie avec d'autres divisions de l'entreprise (Affaires publiques, Relations institutionnelles…).

L'ensemble des informations recueillies constitue le socle à partir duquel le directeur de la sécurité peut commencer à travailler avec ses partenaires pour la protection des expatriés. Dès lors que j'ai les clefs géopolitiques de la région de déploiement de mes expatriés, je peux envisager sereinement les plans possibles de sécurité pour l'ensemble des mes filiales. ■

RECOM > MANDATIONS

> **S'emparer sur sujet international pour l'intégrer aux besoins et à la stratégie de l'entreprise.**
Dans beaucoup de structures, l'international est considéré comme un sujet lointain, qui touche les ressources humaines dans la gestion des expatriés. Les unités « business développement » ne partagent pas les informations avec la sécurité et ne voient la sécurité que comme le pompier d'un possible incendie, qui n'arrivera peut-être jamais… et quand il arrive, il est déjà trop tard. Il s'agit donc de casser cette mécanique d'isolement de la fonction sécurité pour l'impliquer dans l'ensemble des projets de l'entreprise.

> **Développer un cycle de sensibilisation ciblée.**
Dans l'international, tout le monde pense avoir la vérité. Tout le monde a son idée sur la Chine, l'Inde, la Russie, l'Afrique… la France même… mais, au final, cela ne débouche sur rien. Effectuer régulièrement, tous les trimestres, une séance de sensibilisation par rapport à nos développements en cours est un excellent moyen de rassembler ce qui est épars.

> **S'impliquer personnellement dans le sujet international.**
Pour se positionner en anticipation de crises, le directeur de la sécurité doit prendre l'initiative de s'autosaisir des sujets et montrer qu'il est un créateur de valeur.

> **Prendre attache avec le CDCS.**
Il serait illusoire de vouloir faire sans le Centre de Crise et de Soutien du Quai d'Orsay (CDCS) ou sans le réseau diplomatique, parce que la marque « France » chasse en meute. Afin d'être reçu par nos diplomates, il importe de partager l'information, d'instaurer un dialogue dans les deux sens.

> **S'abonner à des outils de veille pays.**
Le directeur de la sécurité doit travailler le contour thématique et géographique de sa veille pays, en fonction des intérêts de son entreprise. Ces outils peuvent bien entendu être sous-traités.

LE MANAGEMENT DE CRISE NE PEUT PLUS ATTENDRE

COMMISSION « GESTION DE CRISE & CONTINUITÉ D'ACTIVITÉ » DU CDSE

*Cet article a été rédigé au titre de la commission « Gestion de crise et Continuité d'activité » du CDSE par **Gabrielle BERTHELOT** (Kering), **Anne PICOT-PERIAC** (Atos) et **Joelle RIETJENS** (EDF), sous la direction de **Jean-Yves OGER**, directeur adjoint de la Prévention et de la Protection du groupe Renault, et président de la commission.*

Les entreprises estiment être confrontées à davantage de crises aujourd'hui qu'il y a dix ans, relève une étude récente[1]. Avec la diversification des menaces et des risques (cyber, terrorisme, géopolitique, sanitaire…), l'art de protéger les entreprises est devenu un enjeu majeur. La plupart des grandes entreprises ont aujourd'hui une organisation dédiée à la gestion de crise animée par une équipe de professionnels. La crise Covid a accéléré cette tendance.

Ces onze dernières années nous ont également montré qu'il était indispensable de **« penser l'impensable[2] »**. Les grandes crises récentes ont très souvent surpris par leur nature et leurs conséquences. En 2009-2010, la crise H1N1 avait eu des conséquences limitées pour nos organisations. En 2022, les impacts de la crise Covid sont majeurs, et touchent toutes les dimensions de l'entreprise (RH, supply chain…)

L'approche par les risques mais aussi une meilleure intégration de la veille et de l'analyse des signaux faibles sont des clés de réussite pour mieux anticiper les crises de demain.

Pour répondre à ces enjeux, nos métiers sont devenus des fonctions stratégiques de l'entreprise. Les directions de sûreté jouent un rôle majeur dans l'animation des dispositifs de crise. Elles ont dans leur ADN les capacités d'anticipation, de réactivité et d'organisation indispensables à la gestion de crise. Notre activité doit être encore plus transversales pour rayonner dans l'ensemble de l'écosystème et développer notamment des compétences comportementales nécessaires pour accompagner les directions générales dans le management des crises.

Les événements d'ampleur auxquels ont été confrontées les organisations depuis 2010 n'ont fait que confirmer les fondamentaux - déjà identifiés - d'un dispositif de crise efficace. **Des facteurs clés de succès qu'il est indispensable de continuer à renforcer :**

> **LEADERSHIP/ENGAGEMENT DE LA DIRECTION.** La capacité de réponse immédiate en cas de crise et/ou la capacité à maintenir l'activité opérationnelle en toute circonstance est aujourd'hui un impératif pour toutes les entreprises. Nécessairement, ces enjeux doivent être intégrés dans les plans stratégiques d'entreprise et portés au plus haut niveau. L'implication des dirigeants, que ce soit dans la préparation ou la gestion des situations de crises réelles est une condition préalable indispensable de réussite, de mobilisation et d'engagement des équipes.

> **PROFESSIONNALISATION/EXERCICES/RETOURS D'EXPÉRIENCE.** La formation des équipes et les exercices sont la clé de voute d'un pilotage de crise performant. Or les dispositifs de préparation et d'entrainement restent encore souvent trop marginaux. Ils ont besoin d'être renforcés, intégrés à la formation de tous les managers, en y incluant les dirigeants, et doivent proposer des scénarios d'exercices ambitieux. À ce titre, les retours d'expérience sont fondamentaux. Ils permettent de repenser l'organisation, les modes de décision et surtout de s'appuyer sur la mémoire collective des événements, pour pouvoir faire bouger les lignes à grande vitesse en situation de crise.

[1] *« La gestion de crise des entreprises résilientes »*, Deloitte, 2021.

[2] Cf. article « *Penser & imaginer l'impensable, manager l'incertitude* » P. 127

> **MISE À JOUR DES RÉFÉRENTIELS.** Dès la conception de son dispositif de crise, l'organisation doit intégrer le principe de maintenance des éléments de référence qui vont servir en cas de crise. Le référentiel c'est à la fois ce qui va servir de support à la gestion de crise mais aussi ce qui va permettre de mesurer l'impact potentiel sur l'organisation et à appuyer les décisions : politiques, checklist, contacts utiles, plan de communication, plan de continuité d'activités, plan de reprise d'activités, cartographie des risques, liste des menaces et vulnérabilités, inventaire et localisation des produits et des actifs de l'entreprise, sauvegarde externe du système d'information…

> **DIFFUSER UNE CULTURE DE GESTION DE CRISE.** Les structures les plus résilientes sont aussi les plus agiles, celles qui savent s'adapter aux contraintes, les prendre en compte et, pourquoi pas, créer des opportunités. Dans cet objectif, chaque collaborateur de l'organisation a son rôle à jouer, chacun à son niveau. Il est donc primordial d'investir dans la sensibilisation de l'ensemble des équipes, au-delà des acteurs du management de crise, et l'étendre à tout l'écosystème de l'organisation (interne et externe). Cependant, la composante interculturelle ne doit pas être sous-estimée, car si certaines décisions issues du corporate peuvent paraître légitimes et justifiées en temps de crise, elles pourront ensuite compliquer considérablement les relations de l'organisation avec le pays dans lequel elle opère, ou ses équipes locales.

> **VEILLE.** Les crises sont devenues de plus en plus complexes et globales. Percevoir les signaux faibles, développer l'analyse sur les risques identifiés aideront les entreprises à mieux anticiper les crises. Les exemples récents du Covid ou la pénurie des semi-conducteurs illustrent parfaitement le besoin de mettre en place très amont un dispositif de veille robuste pour faciliter la prise de décision.

> **CAPACITÉ À ANTICIPER EN CRISE.** La complexité de notre monde et les relations d'interdépendance entre les grands systèmes rendent difficile la prévision à la fois des sources potentielles de crise et leur dynamique d'amplification. Mais plus l'imprévisibilité des événements est forte et plus le besoin d'anticiper les impacts possibles sur les organisations s'accroît. Aussi, la mise en place de cellules d'anticipation répond aujourd'hui à un besoin vital des organisations pour appuyer le pilotage stratégique en crise.

> **COORDINATION PUBLIC/PRIVÉ, POUR UNE SIMPLIFICATION DES ÉCHANGES.** La complexification des interdépendances, et la montée en compétence des organisations de crise renforce les besoins d'échanges entre acteurs. En crise, l'information est clé ! Pour répondre à la multiplicité des acteurs économiques concernés, il importe que des canaux privilégiés et unifiés d'échange d'information entre services de l'État et entreprises soient définis, dans une logique de « guichet unique » : ceci permettrait efficacité, fiabilité, équité dans l'accès et le partage d'information.

> **CLARIFIER LES PÉRIMÈTRES.** Dans les normes 9001 ou 27001, il est question de « savoir adresser les parties prenantes ». Avoir une bonne visibilité en interne et en externe des entités qui peuvent aider, freiner ou au contraire perturber la reprise d'activité et le retour à la normale doit permettre d'anticiper les réactions. Suivant l'organisation il peut y avoir un niveau local (site, pays, région géographique, divisions de marché, département…) et un niveau global. En face de chaque partie prenante, il faut définir qui dans l'organisation de crise a la charge de mener les actions et d'alimenter la relation. La question n'est pas *« qui fait quoi ? »* mais *« qui adresse qui ? ».*

> **CAPITALISER SUR LES OUTILS DIGITAUX.** De plus en plus d'outils digitaux sont développés pour faire gagner un temps précieux aux équipes de crise et augmenter leur efficacité ainsi que la traçabilité des actions menées. La crise COVID a été un accélérateur de la transformation vers des espaces de crise virtuels ou hybrides. En revanche, il faut prendre en considération le temps nécessaire à l'implémentation, au paramétrage, la formation, le coût de l'ensemble, et l'adhésion des équipes surtout si ces outils sont dédiés aux seules situations de crise. Une attention particulière doit être portée quant à la dépendance à ces outils, car ils peuvent devenir un risque pour l'organisation en cas de dysfonctionnement, fuite de données, souveraineté…

> **DES CRISES MONDIALES ET SYSTÉMIQUES.** La pandémie de Covid-19 a donné un aperçu d'une crise mondiale, systémique et multidimensionnelle. La diversité des acteurs concernés et leurs interconnexions complexifient la réponse et chaque décision entraîne des répercussions sur d'autres acteurs. Il devient impératif de se préparer collectivement à affronter ces futurs événements d'ampleur. Cela permet de mieux connaitre les capacités ainsi que les limites de chacun, et éventuellement de créer des effets de synergie.

Face à la complexité des crises, la réponse est désormais nécessairement collective : toutes les entreprises, tous secteurs d'activité confondus, ont un rôle essentiel à jouer. Par cette démarche de structuration et de rationalisation du dispositif de crise, mais également de sensibilisation de leurs salariés, clients, partenaires, par des coopérations public/privé plus étroites, les entreprises peuvent être de précieuses contributrices de la diffusion d'une culture de la crise auprès des populations. Par cette action, les organisations peuvent également renforcer leurs relations avec les pouvoirs publics dans les pays dans lesquelles elles opèrent. Car elles participent in fine à la résilience de la société civile. ■

RECOM > MANDATIONS GÉNÉRALES

> **Renforcer le travail de préparation aux crises par l'analyse des risques et le développement d'un dispositif de veille**

> **Nommer un responsable du management de crise et continuité d'activité au sein de chaque entité**

> **Diffuser la culture de crise au sein de l'ensemble de l'écosystème élargi de l'entreprise**

> **Se former et s'entraîner à la crise collectivement (avec tous les acteurs internes et externes concernés)**

> **Utiliser des outils numériques en crise implique de prévoir des solutions alternatives de contournement, avec une attention particulière à la sécurisation des données**

> **Élargir la coopération public/privé et considérer tous les acteurs économiques/secteurs d'activité comme indispensables à la résilience de la Nation**

POUR UN DONNEUR D'ORDRE RESPONSABLE & UNE SÉCURITÉ PRIVÉE DE QUALITÉ, ACTEURS INDISPENSABLES DU CONTINUUM DE SÉCURITÉ

COMMISSION « SÉCURITÉ PRIVÉE » DU CDSE

*Cet article a été rédigé au titre de la commission « Sécurité privée » du CDSE par **Claire NICLAUSE**, responsable Sécurité privée de la RATP, et **Chrisitian CREMEL**, directeur sûreté du groupe Bouygues et président de la commission.*

L'Entreprise demeure confrontée à une évolution constante des menaces. Elle doit protéger ses emprises, ses produits ou sa réputation face à des risques multiples et répondre aux attentes de sécurité, tant de ses salariés que de ses clients. Longtemps considérée comme un coût par l'Entreprise, la dépense en sécurité gagne aujourd'hui à être perçue par le prisme du « coût évité », comme un investissement à la rentabilité certaine, une valeur et un avantage concurrentiel, au même titre que les exigences liées à la responsabilité sociétale des entreprises (RSE).

Afin de répondre à cette responsabilité en sécurité et assurer le bon déroulement de leurs activités économiques, les entreprises et leurs directeurs de sécurité (DSE) éprouvent un besoin croissant en prestations de sécurité privée. En 2020, 79 % du chiffre d'affaires des entreprises prestataires de sécurité privée a été assuré par la commande privée, contre 21 % pour la commande publique[1]. À ce titre, en tant que principaux « donneurs d'ordre » des prestataires de sécurité, l'Entreprise et ses directeurs de sécurité constituent un maillon incontournable du *continuum* de sécurité.

« MIEUX-DISANT » CONTRE « MOINS-DISANT » : LE RÔLE DU DSE DANS L'ACHAT DE SÉCURITÉ PRIVÉE

Le rôle des directions sécurité-sûreté se trouve essentiel dans l'achat de prestations de sécurité. Par son expertise et son expérience, le directeur sécurité-sûreté apparaît en mesure de peser sur les choix de son entreprise dans toutes les phases de l'appel d'offres amenant au choix du prestataire. Il doit cependant travailler en liaison directe avec les services « Achats », dont la tentation pourrait être de se tourner vers le « moins-disant », là où il se montre absolument nécessaire de privilégier le « mieux-disant ».

Dans son Cahier technique intitulé *« La prestation de gardiennage : le guide du donneur d'ordre »* (Les Cahiers techniques du CDSE, janvier 2020), le CDSE recommande de respecter un juste équilibre entre les exigences qualitatives portées par les opérationnels et les contraintes budgétaires. Si toutes les parties prenantes concourent à la réussite de l'appel d'offres, le binôme des fonctions « Achats » et « Sécurité-Sûreté » semble probablement le mieux placé pour piloter ce processus. Cela ne signifie pas que les critères de coût sont prépondérants, mais que la synergie entre la compétence métier et la compétence process achats demeure essentielle pour le bon déroulement de l'appel d'offres :

> **Dans la phase de préparation de l'appel d'offres,** il s'agit de constituer une équipe projet équilibrée entre les différentes fonctions corporate, afin de définir très précisément les besoins du donneur d'ordre. La fonction « Sécurité-Sûreté », par sa connaissance du secteur, facilite l'analyse quantitative et qualitative des acteurs du marché.

> **Dans la phase d'identification des offres recevables sur le plan technique,** après publication de l'appel d'offres, la direction sécurité-sûreté doit se prononcer clairement sur les restrictions, voire les exclusions à l'égard de certains soumissionnaires dont la qualité n'apparaît pas au niveau requis. Cette étape permet d'éviter une négociation financière non-pertinente. Il convient ici d'écarter une offre anormalement basse, c'est-à-dire nettement décalée par rapport aux autres.

[1] Enquête de branche prévention-sécurité 2021 sur les données de 2020 (Xerfi Spécific)

> **Dans la phase d'attribution du contrat,** la seule base du tarif, « le moins-disant », est fortement déconseillée, car elle génère plusieurs risques à des niveaux élevés en termes de qualité de la prestation : contrôle interne au prestataire, management local, non-paiement des charges sociales et patronales, travail dissimulé, travail illégal ou non-conforme aux législations en vigueur, formation insuffisante du personnel, défaillance du prestataire… À noter que lors des contrôles menés par le Conseil national des activités privées de sécurité (CNAPS), *« les constats susceptibles de constituer des infractions pénales (emplois dissimulés…) font l'objet d'un signalement au procureur de la République sur le fondement de l'article 40 du Code de procédure pénale »*. Dans ce cadre, « la co-responsabilité du donneur d'ordre peut être pénalement retenue »[2] .

> **Dans la phase de négociation financière,** la fonction « Achats » prend la main pour négocier avec des soumissionnaires tous valides sur le plan technique. Elle peut ainsi retenir le prestataire au « mieux-disant ».

La Loi du 25 mai 2021 « *pour une sécurité globale préservant les libertés* » instaure un encadrement de la sous-traitance pour les activités de sécurité privée : une prestation ne peut être intégralement sous-traitée et le sous-traitant de premier rang ne peut lui-même sous-traiter que s'il justifie de l'absence de savoir-faire, de manque de moyens/capacités techniques, ou d'une insuffisance ponctuelle d'effectif. Cette justification doit être validée par l'entrepreneur principal. Puis, le donneur d'ordre doit vérifier que l'entrepreneur principal a bien validé ce motif de recours à la sous-traitance. Le sous-traitant de second rang ne peut sous-traiter sous aucun motif.

Sur ce plan, le CDSE recommande au donneur d'ordre de contraindre l'entrepreneur principal à lui fournir une attestation écrite confirmant que ce dernier a bien validé le motif du recours à la sous-traitance. De façon plus générale, le CDSE préconise de proscrire le recours à la sous-traitance, compte tenu des risques qu'elle comporte (qualité des prestations, conformité, relation entre donneur d'ordre et prestataire…). Si ce procédé s'avère toutefois nécessaire (ponctuellement et par dérogation), il convient de bien l'encadrer pour en conserver le contrôle.

Pour toutes ces raisons, et afin de pérenniser les relations gagnant-gagnant avec les prestataires de sécurité privée, les donneurs d'ordre ont besoin de bâtir une relation plus fluide avec le Conseil national des activités privées de sécurité (CNAPS), afin de travailler de concert et solliciter la mission de conseil de l'établissement public de régulation du secteur.

LES ATTENTES DES DONNEURS D'ORDRE EN MATIÈRE DE QUALITÉ DE LA PRESTATION

L'Entreprise, pour répondre à l'ensemble de ses défis en matière de sécurité, doit pouvoir s'appuyer sur des sociétés de sécurité privée qui se montrent au rendez-vous de la qualité de la prestation. Tandis que la France se trouve à l'aune de deux grands événements d'ampleur internationale avec la Coupe du monde de Rugby 2023 et les Jeux olympiques et paralympiques de Paris 2024, le CDSE considère qu'il devient plus que jamais nécessaire de renforcer la professionnalisation de la filière et la qualité de la formation des agents. En outre, les besoins des entreprises évoluent constamment et sont à prendre en considération, notamment quant à la montée de formes de protestations violentes (activismes et mouvements sociaux) nécessitant un savoir-faire en matière de gestion de foule et d'analyse comportementale.

La loi « *pour une sécurité globale préservant les libertés* » a d'ores et déjà durci les conditions d'accès à la profession et prévoit de réformer par ordonnance, d'ici à 2023, les modalités de formation, d'examen et d'obtention des certifications professionnelles ainsi que le contrôle des activités de formation en sécurité privée. Il s'agit là d'une occasion à ne pas manquer pour revaloriser les compétences des agents de sécurité privée par une formation initiale redéfinie en concertation avec la branche professionnelle des entreprises de prévention et sécurité (organisations patronales et syndicats de salariés) autour d'un socle commun robuste et des blocs de compétences additionnels en adéquation avec les missions concrètes des agents sur le terrain et les besoins des clients.

Cette réforme doit en outre faire émerger un véritable encadrement intermédiaire possédant les qualifications opérationnelles et les qualités humaines nécessaires à l'exercice de cette fonction. Une telle restructuration de la filière autour des compétences, savoir-faire, missions et encadrement sont le véritable gage de prestations de surveillance humaine de qualité, impliquant des rémunérations réévaluées en conséquence pour une filière qui gagnerait en attractivité.

[2] www.cnaps.interieur.gouv.fr/Vos-demarches/Vous-souhaitez-acheter-une-prestation-de-securite-privee

CONFORTER LE RÔLE DE L'ENTREPRISE & DE LA SÉCURITÉ PRIVÉE DANS LE CONTINUUM

La sécurité privée et l'Entreprise constituent *« la troisième force de sécurité de notre pays »* affirmait le ministre de l'Intérieur, Gérald Darmanin, jeudi 16 décembre 2021, lors du colloque annuel du CDSE. Néanmoins, la sécurité privée souffre toujours en France d'un déficit d'image qui reste à combler. À cet égard, plusieurs avancées notables - appelées par le CDSE dans ses différentes contributions aux réflexions nationales sur le continuum - sont à mettre au crédit de la loi *« pour une sécurité globale préservant les libertés »* : ce texte instaure une protection juridique des agents de sécurité, des éléments d'identification sur leur tenue, ou l'autorisation exceptionnelle de missions sur la voie publique contre les actes terroristes qui pourraient viser les biens dont ils ont la garde. Un dernier point particulièrement structurant pour le continuum resterait à préciser, notamment dans la perspective de la Coupe du monde de Rugby et des JOP 2024, à savoir l'élaboration d'une véritable doctrine d'emploi de la sécurité privée quant à ses interactions avec les forces de l'ordre dans la gestion des foules lors de grands événements.

Sur le plan économique, la limitation de la sous-traitance citée plus haut vient apporter un premier gage en matière de pratiques plus vertueuses dans le secteur. Celle-ci permet de réduire le risque de dumping inhérent au phénomène de la sous-traitance en cascade. Néanmoins, un effort supplémentaire en matière de régulation économique reste nécessaire : **l'instauration d'un mécanisme de type garantie financière.** Cette mesure, qui fait consensus entre donneurs d'ordre et prestataires depuis 2018 (GES[3] et CDSE), permettrait de s'assurer des capacités financières des entreprises de sécurité privée et de la volonté de leurs dirigeants de s'inscrire durablement et de manière responsable dans ce marché. La Coupe du monde de rugby 2023 et les JOP de Paris 2024 nécessitent que le secteur de la sécurité privée soit plus solide sur le plan économique et moins atomisé, préalable essentiel à la montée en compétence des agents et à une meilleure qualité de service, comme le pointait la Cour des comptes dans son rapport public annuel 2018 [4]. Un tel mécanisme a fait ses preuves pour d'autres secteurs réglementés (agences de voyages, agences immobilières, sociétés de travail temporaire…) et permettrait d'installer définitivement la sécurité privée comme un acteur incontestable du *continuum* de sécurité.

Les agents de sécurité privée en tant que primo-intervenants constituent des capteurs précieux de signaux faibles et de matérialisation de la menace. Ces derniers rendent compte au donneur d'ordre, au directeur sécurité-sûreté, qui, le cas échéant, assure la remontée d'information à la puissance régalienne. Il apparaît nécessaire de favoriser un tel partage d'informations, et de permettre en retour au public de transmettre au privé dans une relation de confiance. Les directeurs sécurité-sûreté d'entreprise constituent à ce titre un vecteur essentiel, un pivot entre le privé et le public. C'est pourquoi le CDSE plaide depuis 2011 pour la création d'un **« cercle de confiance »** instituant les directeurs de sécurité comme interlocuteurs privilégiés des forces régaliennes et de l'État dans l'Entreprise. Un **« référent sécurité »** qui aurait été soumis à une procédure d'habilitation préalable ou à un criblage permettant un partage d'informations, tant sur le plan de l'ordre public que de sujets plus sensibles. Une telle mesure serait de nature à donner définitivement corps au *continuum* de sécurité. ■

[3] Communiqué commun SNES, USP (depuis fusionnés au sein du Groupement des entreprises de sécurité - GES) et CDSE en faveur d'une régulation économique renouvelée permettant un fonctionnement pérenne du marché de la sécurité privée (15 octobre 2018).

[4] Cour des comptes - Rapport public annuel 2018 (Février 2018) - Chapitre 2, *« Les activités privées de sécurité : une contribution croissante à la sécurité publique, une régulation insuffisante »*

RECOM > MANDATIONS

À L'ÉGARD DES POUVOIRS PUBLICS

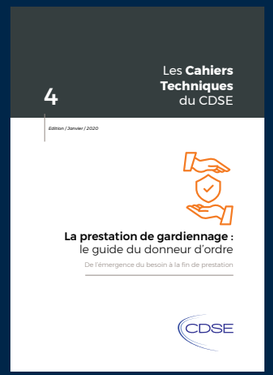
> Réformer la formation professionnelle en sécurité privée :

- En revalorisant les compétences des agents de sécurité privée par une formation initiale redéfinie en concertation avec la branche professionnelle des entreprises de prévention et sécurité (organisations patronales et syndicats de salariés)
- En bâtissant un socle commun robuste et des blocs de compétences additionnels en adéquation avec les missions concrètes des agents sur le terrain et les besoins des clients
- En faisant émerger un véritable métier d'encadrant en sécurité privée

> Instaurer un mécanisme de type garantie financière pour les entreprises de sécurité privée

> Faciliter les échanges entre les donneurs d'ordre et le CNAPS, notamment dans le cadre de la mission de conseil de l'établissement public de régulation du secteur

> Créer un « cercle de confiance » public-privé instituant les directeurs de sécurité comme acteurs incontournables du continuum de sécurité et interlocuteurs privilégiés des forces régaliennes et de l'État dans l'Entreprise



Pour consulter le cahier technique du CDSE *« La prestation de gardiennage : le guide du donneur d'ordre »*

- **Vous êtes membre du CDSE :** dans votre espace adhérent « Mon CDSE » > onglet « Boîte à outils » > « Les publications du CDSE » > « Les cahiers techniques du CDSE »
- **Vous n'êtes pas membre du CDSE :** contact@cdse.fr

LE DIRECTEUR SÛRETÉ & LES ENJEUX DE CYBERSÉCURITÉ DE L'ENTREPRISE

JEAN-PAUL BONNET

Chief security officer du groupe Safran
Président de la commission « Cybersécurité & protection de l'information » du CDSE

Tout a déjà été dit ou presque sur la sécurité du monde numérisé et pour avoir une chance de capter l'attention, il est préférable d'utiliser le terme « cybersécurité », même si le terme de cyber sûreté serait plus approprié.
À des niveaux certes différents, la résilience des entreprises membres du CDSE dépend globalement, si ce n'est presque totalement de la sécurité du monde numérique : la cybersécurité. Au même titre qu'elle dépend d'une bonne gestion de ses ressources, de la compétence de ses forces commerciales, de la qualité de ses produits et services…

Pourquoi donc est-il besoin de revenir sur le sujet encore et encore ? Peut-être parce que certaines évidences doivent être rappelées régulièrement dans **un domaine qui évolue à une vitesse telle que personne ne peut prétendre maîtriser l'ensemble du sujet**. Y compris les experts les plus en pointe. Suffit-il alors d'énoncer que des moyens humains, organisationnels et techniques permettent de faire face au sujet ? C'est un début de réponse mais il n'est pas suffisant.

LA SEULE BONNE ORGANISATION EST CELLE QUI FONCTIONNE

Il est préférable de s'abstenir d'affirmer de façon péremptoire que le modèle idéal d'organisation à mettre en place au sein de l'entreprise pour traiter le sujet est universel. **La seule bonne organisation est celle qui fonctionne** en fonction des ressources disponibles, du secteur d'activité, de l'histoire et de l'expérience de l'entreprise et de ses dirigeants. **Prétendre définir une organisation type, où la sécurité des systèmes d'information de l'entreprise doit être sous la responsabilité du directeur Sûreté ou pas, est illusoire.** Au mieux, certains modèles peuvent être décrits, avec leurs avantages et inconvénients, **à charge pour les dirigeants de retenir celui qui leur semble le plus approprié.** Et d'être capables de se reposer la question régulièrement sur la répartition des missions entre les différentes lignes de défense de l'entreprise face à ce risque.

Certains ont qualifié notre monde de volatile, incertain, complexe, ambigu. C'est bien cette vision qui doit animer l'action d'un directeur Sûreté, notamment dans le domaine de la cybersécurité. Qu'elle soit **qualifiée de globale ou de systémique,** sa démarche lui permet d'aborder avec un esprit ouvert et agile des interdépendances et relations complexes, de valoriser la somme des expertises spécifiques qui, isolément, sont vite limitées. La priorité est-elle de savoir qui reporte à qui ? **La priorité est de s'assurer que les objectifs de sécurisation de l'entreprise ont été définis dans leur ensemble, que les menaces sont identifiées et les risques formellement acceptés par des dirigeants conscients des actions engagées ou à initier pour rester au niveau de risque tolérable établi.**

De cette boucle vertueuse découle le processus qui permet de définir d'une part **les politiques spécifiques** de sécurité de chaque domaine et d'autre part **le contrôle de leur mise en œuvre de façon indépendante.**

Chaque expert trouve sa place dans ce dispositif, quel que soit le schéma d'organisation retenu. **Le directeur sûreté en est un acteur majeur.**

Il ne s'agit pas de prédéfinir qui sera le bouc émissaire en cas d'incident majeur. Il s'agit de s'assurer que tous les rôles sont tenus et les missions réparties. De nombreux exemples récents ont confirmé qu'une crise systémique implique une réponse systémique. Cela s'adapte parfaitement à la sécurisation des entreprises dont les processus numérisés les exposent aux attaques sur une surface de plus en plus étendue alors que leur capacité à se défendre dépend largement de leur écosystème et de leurs partenaires.

UNE CYBERGUERRE EST BIEN EN COURS

Le sentiment d'impuissance qui a pu s'emparer de certaines victimes d'attaques majeures sur leurs systèmes d'informations doit inciter à remettre en avant **les fondamentaux d'une démarche globale dont les phases sont bien détaillées dans les standards internationaux qui font référence** (famille des standards ISO27K, Directive NIS, NIST CYbersecurity framework…). **Elle tend à garantir l'essentiel de la sécurité des actifs tant matériels qu'immatériels dont la convergence est illustrée par l'omni-présence de l'Internet** des objets dans la vie quotidienne, professionnelle ou personnelle. La sensibilisation et la formation aux actes réflexes ou gestes barrières de cybersécurité doivent donc commencer dès le plus jeune âge. **Au cours de la vie professionnelle, les rappels réguliers et adaptés aux activités de chacun sont à organiser par les experts compétents.**

Il est néanmoins peu discutable que les victimes sont et seront nombreuses sur le champ de bataille digital. Faut-il accepter ou refuser ce vocabulaire guerrier ? Qu'elle soit larvée, à nouveau froide, asymétrique ou irrégulière, **une cyberguerre est bien en cours.** Le terme marketing ne change pas le constat, ce cyberespace créé par l'homme, enrichi par l'homme est également détourné de ses objectifs initiaux par l'homme pour y mener ses combats. Et l'entreprise opère en permanence sur ce théâtre d'opérations numérique, parfois dans un déni de réalité encore surprenant, notamment sur le thème de la cybercriminalité organisée liée à des États membres de l'ONU ou celui de l'espionnage industrialisé, y compris entre proches alliés. L'entreprise court donc en permanence le risque d'être **un dommage collatéral d'un combat auquel elle ne prend pas part directement** mais au milieu duquel elle évolue et s'expose avec plus ou moins de protections, par naïveté ou déni.

DERRIÈRE LE CYBER, IL Y A SURTOUT L'HUMAIN

Car tout est vraiment une histoire de comportements humains. Tant du côté de la défense que de l'attaque. La compétence technique offensive ne vient que servir de levier à une intention humaine. Laquelle bénéficiera de l'inattention ou de l'incompétence technique défensive d'un autre être humain.

Le bénéfice de la révolution numérique et de tous les progrès qu'elle apporte est donc à portée de main **si les concepts de sécurité, notamment numériques, sont intégrés dès le début de toute démarche au sein de l'entreprise,** s'ils sont inclus dans les calculs de profitabilité, tant dans le choix des solutions de cybersécurité utilisées que dans la définition des processus et des comportements humains associés, comme une évidence indissociable de la réussite du cycle de vie de cette activité. **Si la sécurité est intégrée a posteriori, elle représente alors une contrainte et un surcoût dérangeants donc contournés voire rejetés.**

La souveraineté de l'entreprise a un prix, celui de sa capacité à limiter l'ingérence numérique malveillante dans l'atteinte de ses objectifs. Et comme les interdépendances sont de plus en plus grandes entre acteurs d'un même écosystème, en renforçant sa posture de cybersécurité, chaque entreprise contribue à renforcer celle de ses partenaires et de son environnement, dans une démarche responsable. Quelle entreprise préciserait dans sa raison d'être qu'elle entend contribuer à l'élaboration d'un monde moins sécurisé, en étant le maillon faible de son environnement ? Quelle entreprise ne se soucierait pas de savoir si ses partenaires extérieurs qui se connectent à ses systèmes d'information ont au préalable sécurisé leurs propres systèmes ? ■

RECOM > MANDATIONS

> Adopter une démarche systémique

> S'assurer que les objectifs de sécurisation de l'entreprise ont été définis par des dirigeants conscients des actions engagées ou à initier pour rester au niveau de risque tolérable établi

> Définir les politiques et mettre en place un dispositif indépendant de contrôle de leur mise en œuvre

> Former et sensibiliser sans arrêt

> Tout est affaire de comportements humains, pas de techniques

> Chaque individu/entreprise contribue à la cybersécurité de son écosystème et dépend des autres

L'INTELLIGENCE ÉCONOMIQUE, VECTEUR DE LA VALORISATION DES ACTIFS

COMMISSION INTELLIGENCE ÉCONOMIQUE DU CDSE

*Cet article a été rédigé au titre de la commission « Intelligence Économique du CDSE » par **Fabien LAURENÇON** (chercheur associé à l'Institut de Recherche Stratégique de l'École Militaire - IRSEM), sous la direction de **Jean-Louis KIBORT**, directeur de la Sûreté du groupe L'Oréal et président de la commission.*

L'intelligence économique (IE) se conçoit comme un maillon clé de la pérennisation des organisations. Depuis 2020, la crise de la COVID-19 a initié une réflexion en profondeur sur le concept de souveraineté tandis qu'il apparaît que le monde entre dans une nouvelle guerre froide, qui oppose notamment la Chine et les États-Unis. Pour les entreprises, il s'agit de remettre en valeur des actifs matériels et intangibles jusque-là considérés comme périphériques, donc délocalisables, et de questionner les risques et opportunités de nos interdépendances.

Partant de ce constat, la commission IE du CDSE a orienté ses travaux autour du besoin crucial consistant à « repenser la notion de valeur ». Dans cette mesure, quels sont les modes alternatifs de valorisation d'une entreprise ? Comment les mettre en œuvre par l'IE ? Comment protéger cette création de valeur ?

ÉLARGIR LES LEVIERS DE VALORISATION

La valeur d'un actif, qu'il soit immatériel (brevet par exemple) ou matériel (site de production, laboratoire), reste encore largement appréhendée sous l'angle financier et d'une stratégie court terme. Plutôt que de revendre automatiquement un brevet ou un portefeuille de brevets en sommeil, ou de céder un site, il est aujourd'hui crucial de réfléchir à différentes stratégies de long terme permettant de dégager d'autres externalités positives. En mars 2021, la fin annoncée par l'État des mesures dites du « quoiqu'il en coûte[1] », amène les entreprises, dans une logique stratégique, à réfléchir à d'autres modes de partenariats substituables aux solutions de financement (Prêt garanti par l'État, Programme d'investissements d'avenir…). L'IE, dans une vision long terme appuyée par son pilier « influence », a pour mission de renforcer la valorisation réputationnelle (mettre en valeur l'image de marque[2]) de l'organisation et de ses actifs.

L'IE peut donc aider à repenser la valeur sociétale et politique des entreprises et de leurs ressources. La crise du transport maritime (pénurie de certains équipements stratégiques, hausse du coût des matières premières et leurs répercussions…) a servi d'accélérateur dans la prise de conscience des limites de nos modes de consommation et du coût du global de ces pratiques. Quand elle est possible, la création de valeur locale, territoriale ou nationale - qui s'impose comme une attente de fond des consommateurs - doit être privilégiée. Le comportement du consommateur est une variable centrale, qui est la cible de l'IE.

PROTÉGER LES CONNAISSANCES & LES VECTEURS HUMAINS DE L'INNOVATION

La crise a mis en valeur, à tous les niveaux, l'action décisive du facteur humain : personnels médicaux, chercheurs mobilisés sur les programmes accélérés de développement de vaccins, métiers de la grande distribution.

Dans le cas des chercheurs, une priorité doit être donnée à la protection, le suivi et la promotion des hauts potentiels. L'IE joue ici pleinement sa fonction en détectant les hauts potentiels, qu'ils soient dans la R&D&I publique ou privée, en accompagnant leur protection contre toutes les formes d'ingérence (débauchage, espionnage, manipulation, déstabilisation…) par des tiers, aux côtés des services des Ressources humaines et des experts de la sécurité des systèmes d'information. Les incubateurs et écosystèmes d'innovation, qui constituent l'étape clé suivante, celle du passage de la découverte scientifique à son industrialisation, doivent être protégés de la même manière, qu'ils soient employés d'une grande entreprise de cybersécurité ou d'une filiale privée sous délégation de service public spécialisée dans l'innovation de santé, en allant au-delà des outils juridiques existants (brevets, propriété intellectuelle, qui présentent des avantages comme des limites.

La guerre économique est d'abord une guerre des intelligences ainsi qu'une course à la connaissance scientifique et à l'innovation de rupture. Il est ainsi envisageable d'aborder les mesures de protection et d'aide selon **trois cercles concentriques de valorisation** et différents types d'actifs (biens, services, connaissances/savoir-faire, recherche dont la recherche fondamentale), qui appellent trois niveaux de sécurité économique :

> **CERCLE 1 : actifs stratégiques, indispensables à la survie du pays.**

Maîtrise complète de la filière par des entreprises implantées sur le territoire national et à capitaux contrôlés par l'État dans lesquelles les décisions opérationnelles ne peuvent être prises que par une personne de nationalité française habilitée par l'État (dissuasion nucléaire, cyber…). La mobilisation des services dédiés de l'État s'opère avec le concours de l'IE des entreprises pour protéger ces actifs. L'indépendance est définie comme la capacité de conserver sa liberté et son autonomie de décision : le secteur électronucléaire, les composants électroniques et verrous technologiques (semi-conducteurs, maîtrise de l'Internet…), la cryptologie, certains fleurons industriels ou encore certaines activités du luxe et de la culture, qui font la renommée de la France, figurent parmi ces secteurs clés.

[1] L'ensemble des mesures économiques de soutien aux entreprises et organisations déployées par l'État pendant la crise de la Covid-19.

[2] On a vu les dégâts en Australie du travail de sape et de dénigrement méthodique mené pendant cinq ans par l'opposition intérieure (une partie de la classe politique locale) et les concurrents allemands (TKMS) et suédois (Saab) à l'encontre du programme Attack, en dépit de l'excellence technologique de la proposition française et de la force du partenariat stratégique proposé au niveau bilatéral.

> **CERCLE 2 : actifs fondamentaux indispensables à la continuité d'activités du pays et de ses habitants à moyen et long terme (OIV - Organismes d'importance vitale et OSE - Opérateurs de services essentiels).**
L'activité de ces entreprises (production d'hydrogène, électronique grand public, agro-alimentaire, transports, médicaments, espace…) devraient être localisée dans un des pays de l'UE avec un contrôle par un de ces pays sur ses décisions opérationnelles et ses capitaux. Il est donc nécessaire de promouvoir une règlementation européenne permettant cette approche et une valorisation du continuum R&D&I. Ces entreprises qui permettent de construire l'indépendance nationale dans l'interdépendance européenne. À ce titre doivent être valorisés, dans une logique de construction d'une Base industrielle, scientifique et technologique européenne[4] (BISTE), des biens, services et domaines de science mentionnés plus haut (également l'agriculture et la sécurité alimentaire), sur la base de l'acceptation de l'interdépendance mutuelle ou croisée entre économies des États membres.

> **CERCLE 3 : actifs non stratégiques, non OIV ou OSE, qui peuvent être localisés hors UE, mais dont la relocalisation peut générer de retombées positives pour le territoire ou l'État, ou pour le renforcement des cercles 1 et 2.**
Pour les entreprises membres du CDSE, cette interdépendance est une réalité depuis longtemps. Il s'agit de garder la possibilité de rapidement pouvoir produire ou reconstituer une capacité de production sur le territoire de l'UE. L'État et l'entreprise peuvent céder la maîtrise technique mais en conservant la maîtrise des savoir-faire et des méthodes. L'enjeu ici est garder de leviers de contrôle capitalistique, PI (propriété intellectuelle) ou autres dans un délai compatible avec l'impact d'un embargo qui nous serait imposé par un État agressif sur ces domaines ou pour lesquels l'État français ou l'entreprise seraient prêts à renoncer.

Ces secteurs sont peu couverts ou mal connus des services de l'État, qui ne disposent pas toujours de l'expertise nécessaire (par exemple sur les sujets d'IA, quantique et d'hydrogène **[cercle 1]**, de smart cities **[cercle 2]** ou de la chimie **[cercle 3]**. La mise à disposition d'experts des entreprises et de la recherche au profit de l'État (par exemple dans les instances de normalisation) pourrait être un autre axe de valorisation. Ce qui est intéressant dans un brevet, ne tient pas du produit de sa cession et d'un gain financier immédiat mais limité, mais bien des retombées à moyen et long terme sur un territoire donné à travers la création d'emplois, les recettes fiscales et le maintien négocié d'une activité scientifique sur le territoire.

C'est à l'État de fixer ses priorités pour les trois grilles de lecture, en interaction avec l'UE à son niveau **[cercle 2 et cercle 3]**, et bien sûr aux entreprises pour ces trois niveaux d'actifs, en interaction avec Bruxelles et l'État dont elle est originaire. Le cas des stratégies cloud, cyber ou hydrogène sont des leviers pour favoriser un marché européen.

Seule la Commission européenne peut financer un programme sur dix ans pour une filière spécifique, comme pour une autonomie sur les puces électroniques. Mais la France, pour des raisons de dissuasion, aurait peut-être besoin d'une maîtrise complémentaire qui serait alors financée par elle seule sur des sous-segments précis (lasers de forte puissance, recherche génomique, protection NRBC) dans une stratégie de verrous technologiques et scientifiques.

Dans ce dernier cas, une stratégie de sécurité économique à l'échelle de l'Union européenne, qui ouvre un champ vertigineux de sujets, pourrait s'appuyer sur deux piliers :

- Une harmonisation des pratiques de sécurité économique (par exemple la PPST - Protection du potentiel scientifique et technique de la nation) entre ministères des États membres pour renforcer les mécanismes de contrôle à l'entrée (sur le mode des IEF[5]). Cette approche est aujourd'hui théorique, mais l'évolution de la Commission européenne est un signal positif[6].
- Des échanges de bonnes pratiques entre fédérations professionnelles : depuis 2018, le CDSE a initié plusieurs contacts avec son homologue allemand de l'ASW (Akademie für Sicherheit und Wirtschaft). D'autres contacts pourraient être approfondis avec l'Italie et l'Espagne. La commission IE pourrait jouer un rôle moteur dans le rapprochement des acteurs de la sûreté-sécurité en Europe, complémentaire de l'action des États[7].

[4] La notion rejoint l'appel de la présidente de la Commission en faveur d'une souveraineté européenne de défense.

[5] Dispositif de contrôle des « Investissements étrangers en France ».

[6] Au sein du CDSE, une approche inter-commissions en partenariat avec la commission « Fraude & Compliance » mériterait d'être étudiée.

[7] Tout en restant attentif quant à l'introduction de nouvelles règles et normes par un État au profit de ses acteurs.

CONCLUSION

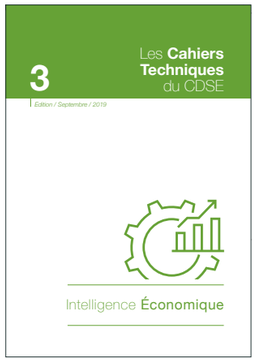
L'IE a toute sa place dans le déploiement de cet arsenal de souveraineté, dont elle n'est qu'un maillon parmi d'autres fonctions de l'organisation.

Face à un environnement d'affaires toujours en mouvement et qui se durcit, la souveraineté est garante de la résilience de l'État comme des entreprises.

Cette **résilience** n'est pas synonyme de passivité. Il importe de penser également nos moyens de « rétorsion » : quelles sont les faiblesses chez nos adversaires ? Dans le cadre de cette **stratégie offensive**, ne nous interdisons pas de cartographier les faiblesses et forces de nos concurrents, chacun dans son domaine et avec les ressources qui lui sont propres : à l'État ses moyens régaliens, avec ses services spécialisés, aux entreprises de définir leurs vulnérabilités propres, dans leur secteur, face à leurs concurrents.

Cette connaissance de nos atouts et faiblesses n'est pas statique, elle doit s'adapter à des écosystèmes en constante mutation, pour la recherche, l'entreprise et l'État qui sont appelés à travailler ensemble.

Cette coordination/coopération entre les acteurs institutionnels et privés est la clé de notre **souveraineté,** et du **rayonnement** de notre pays. ■



Pour consulter le cahier technique du CDSE *« Intelligence économique »*

- **Vous êtes membre du CDSE :**
  dans votre espace adhérent
  « Mon CDSE » > onglet « Boîte à outils »
  > « Les publications du CDSE »
  > « Les cahiers techniques du CDSE »
- **Vous n'êtes pas membre du CDSE :**
  contact@cdse.fr

RECOM > MANDATIONS GÉNÉRALES

> **Identifier les leviers de valorisation des actifs de l'entreprise et de l'État par l'IE** dans une vision à plus long terme au détriment d'une valorisation à court terme. Pour cela, les entreprises doivent avoir connaissance des priorités de l'État, ces dernières devant éviter la concurrence entre elles au profit d'une harmonisation des chaînes de valeur

> **L'intégrité des chaînes de valeur permet de sécuriser les segments stratégiques.** C'est pourquoi il est nécessaire d'identifier les éléments sensibles qui peuvent se situer dans les différents cercles d'intérêts. Il est essentiel que l'État puisse s'appuyer sur des experts de la recherche et des entreprises pour obtenir une vision intégrant tous les verrous scientifiques et techniques de cette chaîne de valeur

> **Protéger les connaissances et les vecteurs humains de l'innovation :** les chercheurs, entrepreneurs, intrapreneurs en demandant à l'État de fixer les priorités dans les trois cercles en termes de sécurité, en partant du principe que l'IE ne peut pas tout protéger, qu'elle soit portée par l'État (politique de sécurité économique) ou par l'entreprise (direction de la sûreté)

> **Agir pour une stratégie de sécurité économique à l'échelle de l'Union européenne :** conduire des actions d'influence auprès de l'Europe pour partager les priorités avec une harmonisation au rang des États membres et l'Europe : l'enjeu est de bâtir une R&D appliquée et théorique c'est-à-dire un écosystème européen allant de la recherche à l'industrie (*continuum*)

LUTTE CONTRE LA FRAUDE & COMPLIANCE : DEUX LEVIERS DE CROISSANCE POUR LE DIRECTEUR DE LA SÉCURITÉ-SÛRETÉ CORPORATE

RUDOLPHE PROUST

Directeur sûreté du groupe Altarea
Président de la commission « Fraude & Compliance » du CDSE

Dans un contexte économique d'échanges complexes et internationaux, de plus en plus digitalisés, les entreprises doivent faire face à des atteintes frauduleuses toujours plus sophistiquées, tant depuis leur environnement extérieur plus ou moins proche, que de la part de leurs propres collaborateurs, partenaires ou clients.

La prévention passe ainsi par la mise en place d'un corpus de règles adaptées et de process solides, ou encore par une résilience accrue reposant sur un traitement adéquat et rapide des incidents frauduleux. Ce sont les éléments clés de l'efficacité de la lutte contre ces atteintes et de la minimisation des impacts tant matériels qu'immatériels sur nos groupes.

De même, le contexte réglementaire est de plus en plus contraignant pour les entreprises (contrôles et sanctions). Grâce à sa vision transverse, le directeur de la sécurité-sûreté corporate participe à la mission de mise en conformité de l'entreprise, en assurant la recherche et la réponse à toute déviance et en répondant aux incidents frauduleux. Il est force de proposition pour des mesures correctives adaptées aux côtés des services opérationnels, des services juridiques ou encore des instances disciplinaires.

La lutte contre la Fraude et son corollaire, la Compliance, ont donc comme objectifs de mettre en place une prévention efficace, assurer une réactivité opérationnelle dans le traitement des fraudes et permettre une adaptation permanente à des fins d'anticipation et de prise en compte des risques par la mise en place des structures et des process internes adéquats.

La fonction de directeur de la sécurité-sûreté corporate trouve ainsi toute sa place dans l'organisation des entreprises, aux côtés d'autres acteurs selon les organisations propres à chaque culture de groupes ou à des réglementations spécifiques (directeurs juridiques ou risques, contrôle et audit internes…). Compte tenu de ses domaines de compétences et d'intervention, de son positionnement au sein des structures, le directeur de la sécurité-sûreté a un rôle central à jouer dans la mise en place des moyens tant organisationnels qu'opérationnels pour garantir la conformité de l'entreprise et assurer la confiance pour les dirigeants et collaborateurs ainsi que pour tous les partenaires quels qu'ils soient.

POUR UN CONTINUUM DE LA LUTTE ANTI-FRAUDE

Le directeur de la sûreté est un maillon important du *continuum* de sécurité, qui entretient des liens avec différentes entités régaliennes, sous l'égide du ministère de l'Intérieur notamment. Néanmoins, la lutte anti-fraude pourrait nécessiter la création d'un groupe de travail commun entre les services étatiques répressifs et une organisation regroupant les directeurs de sécurité-sûreté des grandes entreprises, telle que le CDSE. Une telle instance public-privé permettrait ainsi d'améliorer la prise en compte du traitement des fraudes subies par les entreprises (absence de dépôt de plainte systématique pour cause de temps passé, absence de connaissance de services de police et gendarmerie en charge des plaintes pour les tentatives ou préjudices subies par des personnes morales et non physiques…), et améliorer le retour sur les fraudes subies et le partage d'information (nécessité absolue pour mise en place des mesures correctives immédiates, mise en place de mesures préventives pour les autres entreprises…).

Dans cette même logique, les directeurs de sécurité-sûreté pourraient intervenir, lors d'échanges ou de formation, auprès des personnels chargés des prises de plaintes et enquêtes afin de faire connaitre les enjeux et les contraintes des entreprises dans le traitement de la fraude.

LE DIRECTEUR SÉCURITÉ-SÛRETÉ & LA COMPLIANCE

La direction sécurité-sûreté corporate s'attache à promouvoir toutes mesures de nature à garantir l'indépendance des personnes traitants les sujets Éthique et Compliance. Le directeur sécurité-sûreté participe à formaliser les règles qui permettent de traiter la majorité des cas (code et procédures) et impulser une culture Éthique et Compliance pour changer en profondeur les pratiques (ne pas s'arrêter au déploiement de nouvelles procédures). Pour cela, il devra s'assurer du portage de cette culture par les dirigeants (exemplarité et « Tone on Top »), définir un plan de formation pour tous les collaborateurs ainsi que pour les populations sensibles et faire vivre cette culture au travers de sensibilisation et de communications récurrentes ou auprès des nouveaux arrivants dès leur accueil. Il doit être un appui à la remontée des questions ou des manquements via la voie hiérarchique ou tout autre chaîne de compliance (Officiers compliance, déontologue…). Et ainsi, encourager les collaborateurs à ne pas rester seul face à une situation délicate. Pour cela, l'entreprise doit mettre en place un canal d'alerte, pour les cas qui ne pourraient être remontés par la voie hiérarchique, afin de permettre à l'entreprise ou l'organisation de traiter en interne ces situations.

Le directeur sécurité-sûreté doit prendre une part de la responsabilité de l'évaluation de l'ensemble des tiers avec lesquels l'entreprise ou l'organisation travaille, dans le but de protéger la réputation de celle-ci et éviter des risques de sanction financière ou autre. Dans ce cadre, procéder à un contrôle « à blanc » en vue d'un contrôle par une autorité, peut être une initiative efficace. Il s'agit ici d'identifier les points de contrôle à reproduire sur le dispositif de contrôle interne et, au besoin, de mettre en place les actions correctives.

Enfin, de façon à exercer en toute sérénité ses responsabilités en la matière, le directeur de la sécurité-sûreté corporate doit exercer le traitement des alertes dans un cadre formalisé. C'est notamment le cas pour les process d'enquête interne cadre, dont les modalités et les limites sont précises.

Il peut en outre s'avérer utile de mesurer la culture d'éthique de l'entreprise via un baromètre portant notamment sur la notoriété et le niveau de confiance dans le système d'alerte.

POUR UNE VISION PLUS GLOBALE DE LA LUTTE CONTRE LA FRAUDE & DE LA COMPLIANCE

L'efficacité de la protection des entreprises contre les fraudes internes comme externes dépendra de l'engagement et du déploiement d'une culture de l'ensemble des parties prenantes en affaires (dirigeants, collaborateurs, prestataires, fournisseurs, clients). Nous appelons à une meilleure représentation de la fonction de directeur de sécurité-sûreté corporate dans les groupes de travail au sein des instances étatiques (Bercy, ministère de l'Intérieur, ministère de la Justice…) et instances de régulation (autorités publiques, autorités administratives…). L'intérêt est de « désîloter » cette responsabilité dans les entreprises et d'intégrer les compétences d'un directeur sécurité-sûreté corporate dans le traitement de la Fraude et de la Compliance.

RECOM > MANDATIONS

> Création d'un groupe de travail mixte entre services étatiques répressifs et directeurs de la sécurité-sûreté corporate (CDSE) pour améliorer la prise en compte du traitement des fraudes subies par les entreprises

> Participation des directeurs sécurité-sûreté corporate (CDSE) aux formations des personnels étatiques en charges des plaintes et enquêtes sur les enjeux et les contraintes des entreprises en matière de fraude

> Promotion de toutes les mesures garantissant l'indépendance de traitement des sujets Éthiques et Compliance dans l'entreprise et de toutes les mesures de développement d'une culture de compliance dans l'entreprise

> Participation à toutes les initiatives permettant le contrôle de l'efficacité du dispositif ainsi que la mesure de la confiance éthique des collaborateurs

> Intégration des directeurs de sécurité-sûreté corporate (CDSE) aux côtes des autres directions (juridiques, risques, audit…) en tant que représentants des intérêts de l'entreprise dans le domaine de la compliance auprès des instances de régulation

SÉCURITÉ DES PRODUITS, TRAFICS & SUPPLY CHAIN : POUR UNE STRATÉGIE DE LUTTE GLOBALE

EDMOND D'ARVIEU

Chief security officer du groupe Sanofi
Président du groupe de travail « Sûreté du cycle de vie des produits et lutte contre la contrefaçon » du CDSE

Contrefaçon, trafics illicites, détournements et vols de produits affectent toutes les entreprises commercialisant à l'international des produits à forte valeur ajoutée ou véhiculant une image de marque reconnue. Ces activités criminelles en continuelle expansion sont de plus en plus orchestrées par des réseaux très organisés.

Ces trafics présentent de graves menaces pour la santé publique, notamment en ce qui concerne les médicaments, les cosmétiques, l'alimentation, le tabac ou les alcools. D'autres secteurs comme l'industrie du jouet, électrique, chimique ou des transports sont également impactés, les produits contrefaits entraînant des risques de pollution environnementale, de choc électriques, d'incendie, ou d'accidents. Selon l'OMS, le seul trafic de médicaments falsifiés provoque, chaque année, la mort de 100.0000 à 1 million de personnes[1].

[1] Communiqué publié sur le site de l'OMS, https://www.who.int/fr/news/item/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified, novembre 2017.

Pour l'Union Européenne, la contrefaçon représente 6,8 % du total des importations, soit une valeur estimée de 121 milliards d'euros, ce qui se traduit donc par un manque de recettes fiscales de 19 milliards d'euros et la perte massive de 40 000 emplois par an[2]. S'agissant de la France, l'Organisation de coopération et de développement économique (OCDE) estime qu'elle en est, à l'échelle mondiale, la plus impactée après les États-Unis[3]. Pour les entreprises victimes, les pertes de parts de marché peuvent atteindre 60% sur certains produits, notamment dans les pays émergents.

Les risques légaux, d'image et de réputation peuvent également être désastreux si, face aux consommateurs pouvant être gravement impactés, les entreprises ne démontrent pas qu'elles s'organisent et agissent pour lutter contre ce fléau. Ceci impacte particulièrement les PME qui n'ont ni les ressources, ni les expertises pour exercer un contrôle de leurs produits tant sur leurs marchés physiques que digitaux.

Les organisations criminelles écoulent leurs productions en cherchant à infiltrer les circuits licites de distribution, notamment sur Internet via les réseaux sociaux. Bénéficiant de la porosité des marchés et des frontières ainsi que de l'insuffisance des contrôles des autorités parfois complices et corrompues, exploitant les différences de prix des produits, comblant le vide généré par les ruptures d'approvisionnement ou l'insuffisance de produits face aux pics de demandes, les produits périmés, détournés ou falsifiés envahissent les marchés ou atteignent directement les consommateurs.

Avant l'ère digitale, les trafics de produits étaient surtout présents dans les pays émergents. Mais avec le développement des plates-formes de vente numériques et la généralisation des achats en ligne encore amplifiée par le confinement imposé dans le contexte de la pandémie COVID 19, les produits illicites sont dorénavant accessibles à tous les particuliers y compris ceux des pays développés qui en sont devenus les premières victimes. Concernant la santé par exemple, plus de 90 % des pharmacies en ligne sont illégales et 50 % des produits écoulés sont falsifiés (source). C'est notamment le cas en France ou l'Internet est directement à l'origine de l'apparition de faux médicaments sur le territoire national. En effet, les circuits physiques de distribution de médicaments sont contrôlés de bout en bout par l'Agence nationale de sécurité du médicament et des produits de santé (ANSM), ce qui évite tout risque de contamination de la chîne logistique. Le développement du commerce en ligne complique la détection et la saisie grâce à la multiplication des commandes de petit volume expédiés par colis postaux.

Pour être efficace, une stratégie de lutte doit être globale, de bout en bout, opérationnelle, instrumentée, partagée et communiquée.

UNE STRATÉGIE DE LUTTE GLOBALE, DE BOUT EN BOUT…

UNE STRATÉGIE GLOBALE. Si une grande majorité des produits contrefaits circulant sur les marchés mondiaux provient d'Asie (60 à 80% selon les secteurs), les trafics illicites de produits authentiques ou contrefaits affectent considérablement d'autres régions comme le Moyen-Orient, l'Eurasie, l'Europe de l'Est et l'Amérique du Sud. Il est donc fondamental que les sociétés impactées puissent connaitre et suivre mondialement les ventes de leurs produits sur les marchés réels et sur Internet.

A contrario, certains produits (notamment alimentaires à haute valeur commerciale) sont contrefaits en Europe et ciblent le marché chinois.

UNE STRATÉGIE DE BOUT EN BOUT. Éviter le détournement, le vol ou l'infiltration des circuits de distribution légitimes par des produits contrefaits nécessite un contrôle continu et de bout en bout de l'ensemble du cycle de vie de produits. Il s'agit d'éviter une rupture de qualité et de continuité dans la livraison des produits aux clients finaux qui serait très préjudiciable pour l'entreprise. Si grâce à la stratégie de sécurisation mise en place les occurrences et impacts d'incidents sont réduits, l'entreprise peut obtenir des conditions favorables auprès des assureurs et réduire ou limiter ainsi les coûts parfois élevés de ses primes d'assurances.

À chaque étape (approvisionnement - production - transport - stockage - distribution - destruction), il convient de procéder à une analyse de risques adaptée aux menaces existantes pour élaborer les mesures de prévention et de contrôle visant à réduire au maximum les vulnérabilités identifiées.

Les procédures, équipements et audits standardisés permettent d'évaluer le niveau de maturité en sécurité des sites, de contrôler les accès normaux et réservés, de surveiller les aires de manipulation, de stockage, de chargement et de circulation des produits, des emballages et des labels de sûreté, de vérifier les flux entrants et sortants ainsi que, le cas échéant, les retours et destructions de produits.

[2] Rapport conjoint OCDE (Organisation de coopération et de développement économique)/ EUIPO (Office de l'UE pour la propriété intellectuelle), *« Trade in Counterfeit Pharmaceutical Products »*, mars 2020

[3] Rapport de l'OCDE, *« Trends in Trade in Counterfeit and Pirated Goods »*, mars 2019

À cet égard, l'association mondiale TAPA (Transported Asset protection Association) fournit des standards de mesures de sûreté et d'audits ainsi que des formations et qualifications concernant la sécurisation des transporteurs et des distributeurs qui font référence. En Europe, un protocole est mis en œuvre avec les forces de police chargées du suivi des vols de marchandises. Il permet ainsi de disposer d'un panorama exhaustif des lieux et types de vols, des modes opératoires et du coût des marchandises volées.

Aux côtés des services Achats et de la supply chain, **la direction de la sûreté doit être partie prenante des processus de sélection des fournisseurs logistiques, transporteurs ou distributeurs** avec lesquels l'entreprise est susceptible de contracter. Elle sera alors à même d'effectuer les due diligences adaptées pour vérifier l'intégrité et la conformité des sociétés postulantes ainsi que détecter d'éventuelles implications de personnes morales ou physiques dans des affaires suspectes passées. Des clauses de sûreté insérées dans les contrats peuvent ainsi prévoir la possibilité, selon les secteurs et lorsque cela est possible, d'effectuer des contrôles et des audits de distributeurs et prescrire les exigences attendues en matière de sûreté comme des certifications, les demandes d'accord en cas de recours à la sous-traitance, les règles d'annonce des transporteurs sur sites, les équipements de sûreté à installer et les mesures de prévention destinées à garantir l'intégrité de la supply chain.

Il est également primordial d'inclure des clauses de cybersécurité pour évaluer la cyber-résilience des fournisseurs, assurer la conformité avec les règles et normes en vigueur - notamment celles sur les données privées -, vérifier la présence de back-ups fiables pour les données critiques, coordonner les réponses en cas d'incident cyber et exiger d'être immédiatement alertés en cas d'attaque, de fuite de données ou de cryptage.

… OPÉRATIONNELLE & INSTRUMENTÉE

UNE STRATÉGIE OPÉRATIONNELLE. La stratégie de lutte opérationnelle s'articule autour de la détection, de l'analyse et des enquêtes.

La détection :

La « détection » vise à trouver des produits falsifiés dans les circuits de distribution réels ou virtuels et à identifier les trafics illicites. L'efficacité de la détection dépend de la qualité du processus de recherche, d'analyse et d'exploitation des informations. Pour cela il faut recourir en interne ou en externe à des analystes spécialisés disposant d'outils et d'accès aux banques de données pour identifier les organisations criminelles, connaitre les modus operandi, les zones de trafics, les acteurs et les produits d'intérêt.

Selon la nature des produits, il est intéressant de déterminer les zones et conditions propices à la contrefaçon et aux trafics. Les contextes de crise, de guerre, de pénurie, de pandémies sont particulièrement favorables car ils génèrent de fortes perturbations dans les services étatiques chargées du contrôle des importations et de la qualité des produits.

Un échange régulier d'informations en global et dans les régions avec les diverses entités commerciales de l'entreprise et les planificateurs de la supply chain aide également à mieux cibler les zones d'intérêt pour les criminels, en analysant, par exemple, les chiffres de vente afin de détecter des variations inexplicables d'une période à l'autre ou anticiper des ruptures de stocks.

En fonction de la criticité des produits et des marchés, des campagnes de vérification de terrain peuvent être organisées pour détecter la présence de produits falsifiés ou illicites.

Sur Internet, la détection vise à recenser les offres de produits sur les sites spécialisés, les plates-formes de vente et les réseaux sociaux les plus utilisés, dans toutes les langues, en

utilisant un mélange d'experts globaux et nationaux. Il convient alors de vérifier le caractère licite de l'offre et dans le cas contraire de recourir à des tests d'achats pour essayer d'identifier la provenance des produits, tout en agissant auprès des plates-formes concernées pour obtenir un retrait des offres en ligne.

L'analyse :

Obtenir des échantillons de produits suspects sur le terrain ou via Internet permet une analyse par des laboratoires internes ou spécialisés afin de caractériser la nature de la contrefaçon. Ceci est indispensable si le titulaire de droits veut intenter une action en justice ou témoigner en tant qu'expert lors du procès d'un réseau criminel qui serait démantelé par les autorités.

L'enquête :

La détection d'un produit contrefait ou illicite entraîne en principe l'ouverture d'une enquête. Il est essentiel de pouvoir identifier dans chaque pays d'intérêt des sociétés privées d'investigation efficaces, répondant aux critères de discrétion et de conformité pour procéder au repérage des circuits illicites, remonter les filières et élaborer les dossiers d'informations exploitables par les analystes de la direction sûreté.

Il convient également d'identifier les unités opérationnelles étatiques qui sont en charge et en mesure de procéder, en fonction des dossiers d'information transmis, aux opérations de démantèlement des sites de production et de filières de distribution. Ceci nécessite d'établir une relation de professionnalisme et de confiance avec ces unités par les correspondants des directions de sûreté locaux. À cet égard, il est particulièrement important de pouvoir utiliser les mêmes outils d'enquête et de traitement des informations que les services des États afin de pouvoir partager avec eux les données selon un format compréhensible et exploitable par leurs systèmes.

Sur Internet, il s'agit d'adresser aux unités compétentes les listes de sites illicites et les détections de vente illicites en ligne pour bénéficier, quand cela est possible, de l'apport des outils d'investigation et d'identification des experts nationaux et internationaux.

UNE STRATÉGIE INSTRUMENTÉE. Les technologies existantes peuvent apporter une aide précieuse pour renforcer l'étanchéité des circuits de distribution, l'intégrité des produits et assurer leur authentification.

Étanchéité :

Les transporteurs aériens, maritimes ou terrestres disposent actuellement de moyens technologiques très efficaces pour prévenir l'accès aux marchandises, comme des dispositifs de verrouillage, de détection d'ouverture, d'immobilisation forcée et de signalisation en cas d'anomalie de parcours.

Traçage :

Diverses solutions permettent de tracer les produits, palettes et conteneurs tout au long de leurs parcours et de pouvoir ainsi les localiser en cas de vols. À base de puces numériques communicantes, elles offrent également une panoplie de services logistiques intégrés, comme la surveillance continue de la température.

Authentification :

La digitalisation permet aujourd'hui d'offrir des solutions qui ne peuvent être copiées par les contrefacteurs, contrairement à celles de la génération précédente, à base d'hologrammes visibles ou invisibles ou de codages visibles.

Certains systèmes exploitent l'empreinte unique de la trame de papier utilisée sur des étiquettes ou des emballages. Une simple application numérique permet de photographier cette empreinte digitale et d'effectuer une comparaison avec l'image scannée lors du passage sur la ligne de production, permettant de savoir immédiatement si le produit est authentique ou pas.

L'utilisation de la blockchain pourrait également garantir le suivi continu de chaque produit tout au long de son cycle de vie.

… PARTAGÉE & COMMUNIQUÉE

L'ampleur de la contrefaçon, la complexité des circuits de distribution, la diversité géographique et les moyens limités des entreprises privées militent pour la mise en place d'une stratégie concertée d'échange d'informations et de lutte.

ENTRE INDUSTRIES AU SEIN D'UN MÊME SECTEUR. Les réseaux de criminels se livrant à la contrefaçon de produits ou aux trafics illicites ne ciblent pas une entreprise particulière mais plutôt une gamme de produits. Plusieurs entreprises peuvent être donc victimes simultanées d'un même réseau et avoir donc intérêt à coopérer dans ce domaine non compétitif. Il est très rentable de s'organiser ainsi sur le plan national et international pour formaliser une coopération qui peut prendre les formes suivantes :

- Échange d'informations sur les enquêteurs et les contacts auprès des autorités dans les pays ;
- Partage d'informations sur les menaces, les modes opératoires des réseaux criminels ;
- Mise en commun de ressources pour financer des campagnes de détection ou des enquêtes de terrain.

Le Pharmaceutical Security Institute (PSI) regroupe ainsi les quarante plus importantes sociétés pharmaceutiques internationales pour orchestrer des campagnes de détection communes sur des gammes de médicaments, comme cela a été le cas sur les traitements et vaccins de la COVID 19. Le PSI organise par ailleurs des campagnes régionales de sensibilisation auprès des services étatiques spécialisés et met en place des outils et bases de données d'enquête à l'usage des analystes des différents membres.

ENTRE INDUSTRIES AU SEIN D'UN MÊME PAYS. Dans la plupart des États industriels, des associations regroupant les entreprises d'un même pays tous secteurs confondus, comme l'UNIFAB (Union des fabricants pour la protection internationale de la propriété intellectuelle), ou des entreprises d'un secteur particulier, comme le G5 Santé pour l'industrie pharmaceutique, ont pour but d'aider leurs adhérents victimes d'atteinte à la propriété intellectuelle à faire valoir leurs droits auprès des pouvoirs publics. Ces associations peuvent informer les organisations de l'impact de la contrefaçon sur leurs activités, le grand public et les États, élaborer des positions concertées ainsi que susciter des initiatives légales ou réglementaires, coopérer avec les autorités pour accroître l'efficacité de la lutte contre les réseaux criminels.

ENTRE LE PUBLIC & LE PRIVÉ. L'État et l'entreprise partagent un intérêt commun fort à lutter contre la contrefaçon et les trafics illicites de produits :

- L'entreprise pour protéger ses parts de marché, sa croissance future, son image et sa réputation ;
- L'État pour préserver les emplois, les revenus fiscaux et, dans certains cas, la santé publique.

Pour être efficace sur le terrain, il est primordial que le public et le privé coopèrent de façon organisée, opérationnelle et continue.

L'entreprise apporte une connaissance unique de ses produits, caractéristiques et marchés lui permettant de procéder en amont aux opérations de détection et de caractérisation de la contrefaçon ou des trafics illicites. Elle peut également mobiliser ses ressources implantées dans de nombreuses zones géographiques et fournir ainsi aux services de l'État un éclairage particulier.

L'État peut mobiliser les différents services d'enquêtes concernés, utiliser des techniques d'investigation particulières, mobiliser la coopération internationale et poursuivre au pénal.

La coopération peut prendre plusieurs formes allant jusqu'à se caractériser par la signature d'un partenariat officiel, comme ente le G5 Santé et l'Office central de lutte contre les atteintes à l'environnement et à la santé publique (OCLAESP), sur les actions suivantes :

- Information mutuelle au travers de revues de cas régulières et échanges de données provenant des enquêtes ou de la surveillance cyber ;
- Formation des services spécialisés de douanes, de police, de lutte contre la fraude sur l'authentification des produits et la détection de contrefaçons ;
- Intervention opérationnelle des autorités après identification des réseaux pour arrêter les trafiquants et démanteler les sites de production ou exiger la fermeture des sites illicites en ligne ou le retrait des offres de produits contrefaits ou illicites sur les plates-formes et réseaux sociaux ;
- Porter plainte, fournir les témoignages et apporter l'expertise judiciaire pour soutenir l'action des pouvoirs publics au pénal. À ce propos, on ne peut que regretter le fait que la contrefaçon, dans de nombreux pays, soit encore perçue sous l'angle juridique telle une atteinte à la propriété intellectuelle, avec des impacts économiques et financiers certes importantes mais non vitales. Une perception de la contrefaçon qui serait plus largement considérée comme un risque grave de santé publique, qui provoque de graves maladies et de nombreux décès selon les produits concernés, et donc passibles d'une plainte au pénal serait plus pertinente. Ce constat a de nombreuses conséquences :
  - La lutte contre la contrefaçon, même de médicaments, ne fait pas partie des priorités des services des États qui, pour des raisons légitimes sur le plan fiscal ou de l'ordre public, sont plus centrés sur les luttes traditionnelles contre les trafics de narcotiques, de tabac, d'armes, d'êtres humains. De ce fait, les contrefacteurs savent que les risques d'être arrêtés sont faibles ;
  - Les contrefacteurs ne sont pas jugés comme des criminels et n'encourent bien souvent que des peines légères, tant au civil qu'au pénal, souvent avec sursis, ce qui est peu dissuasif. Ce sentiment d'immunité est exacerbé sur l'Internet, où les ventes peuvent s'opérer de façon anonyme et discrète en se jouant des frontières. Face à cette flexibilité, les services des États progressent mais les procédures administratives et judiciaires sont encore lourdes, peu efficaces et réactives. L'organisation des tribunaux et les pouvoirs des juges ont besoin d'être renforcés et spécialisés pour répondre de façon efficace à la complexité des trafics digitaux internationaux.

UNE STRATÉGIE COMMUNIQUÉE. Pour accroître l'efficacité de la lutte contre la contrefaçon et les trafics illicites, il est important de sensibiliser les victimes potentielles et de communiquer en interne et en externe sur la réalité de ces fléaux.

Sensibilisation interne

La sensibilisation vise à faire reconnaître la réalité des trafics existants auprès :

- Des instances dirigeantes pour obtenir leur soutien et les ressources nécessaires à la mise en œuvre d'une stratégie efficace ;
- Les fonctions impliquées dans le cycle de vie de produits afin de les convaincre de l'utilité de la mise en place des mesures de prévention des risques et de contrôle ;
- Les forces de vente qui sont les oreilles et les yeux de l'entreprise pour leur apprendre à rapporter sans délai toute suspicion de produit défectueux.

Sensibilisation externe

La sensibilisation externe joue un rôle la fois préventif & mobilisateur :

- Des victimes potentielles, afin d'éveiller leur vigilance par une prise de conscience sur les risques de la contrefaçon. En fonction du type de risques et de produits, des campagnes et supports plus particuliers peuvent viser certaines contrées ou population ciblées, les parents, les enfants, les voyageurs etc. Concernant les achats sur Internet, les populations les plus vulnérable sont les jeunes qui, souvent persuadés de faire des bonnes affaires, ne sont pas conscients des risques de contrefaçon ou les considèrent négligeables au vu de la différence de prix ;
- D'organisations ou associations nationales et internationales, afin de mobiliser les pouvoirs publics, de renforcer les dispositifs législatifs et les moyens d'intervention ;
- Des pouvoirs publics, afin de les inciter à renforcer leur législation et les moyens de lutte ;
- Aux services étatiques spécialisés de douanes et d'enquête, en les formant à reconnaître les caractéristiques des produits originaux et les technologies de prévention mises en œuvre.

Communication

Une communication régulière sous formes de colloques, d'interviews, de campagnes et d'articles est nécessaire pour éduquer le grand public sur les dangers de la contrefaçon, les risques des achats sur Internet ainsi que les éventuelles possibilités de vérifier la légalité du vendeur et l'authenticité du produit.

CONCLUSION

Devant la croissance continue des activités criminelles de contrefaçon et d'atteinte à l'intégrité de la supply chain, et considérant les risques dramatiques atteignant le grand public ainsi que les impacts sur les entreprises, il est crucial d'amplifier considérablement les moyens de lutte actuels, tant au niveau international que national, public ou privé.

L'efficacité passera par une législation plus sévère pour être réellement dissuasive, des dispositifs réactifs et contraignants, notamment sur Internet, pour limiter les canaux de distribution, et une coopération renforcée entre les titulaires de droits et les services étatiques. ■

[4] Rapport d'information du Comité d'évaluation et des contrôles des politiques publiques de l'Assemblée nationale présenté par les députés Christophe Blanchet et Pierre-Yves Bournazel en octobre 2020

RECOM > MANDATIONS GÉNÉRALES

> **Renforcer l'action de l'État dans la lutte anti-contrefaçon en mettant en œuvre les recommandations du rapport Blanchet-Bournazel sur l'évaluation de la lutte contre la contrefaçon[4]**

> **Renforcer l'arsenal judiciaire tant au civil, en accroissant de façon dissuasive les montants des dommages et intérêts pour les titulaires de droits, qu'au pénal en renforçant les peines, tant à l'égard des personnes morales ou physiques se livrant aux trafics illicites, qu'aux plates-formes virtuelles d'intermédiation**

> **Institutionnaliser et mieux fédérer le partenariat public-privé pour le rendre plus opérationnel en identifiant une structure ad hoc capitalisant sur l'expérience du Comité national anti-contrefaçon (CNAC)**

> **Améliorer l'efficacité de la lutte contre la contrefaçon en obtenant que les Douanes, puissent adresser les échantillons saisis aux entreprises titulaires de droits à des fins d'analyse scientifique pour caractériser le danger éventuel da santé publique et ainsi mobiliser les autorités pour assurer la protection des populations**

- Identifier un organisme international qui pourrait abriter et maintenir une base de données alimentée par les différents secteurs concernés permettant de signaler les incidents constatés avec les opérateurs de la supply chain

- Créer une rubrique « Contrefaçon » pour permettre de signaler les produits suspects sur la plateforme nationale PHAROS de signalement des contenus illicites en ligne sur Internet

- Sur le modèle du partenariat G5 Santé-OCLAESP, selon les secteurs, les menaces et les risques, étendre les accords officiels avec les instances fédératrices d'entreprise générales (CDSE, MEDEF, UNIFAB…) ou sectorielles et les différents organisations étatiques (Douanes, DGCRRF, OCLDI, SIRASCO, TRACFIN, ANSM investis d'une mission directe ou indirecte de lutte contre la criminalité sur les produits pour faciliter les échanges, procurer une base légale à coopération, favoriser la détection et les dispositifs de prévention, accroître la souplesse et l'efficacité des opérations, neutraliser les crises potentielles de santé publique et susciter dans la durée une relation de confiance

- Œuvrer fermement à l'adoption par l'Union européenne des mesures de renforcement proposées à l'issue des consultations dans le cadre du Digital Service Act et œuvrer avec le secteur privé pour les faire appliquer rapidement et efficacement

- Mettre en place des dispositifs public-privé permettant de détecter et saisir les produits contrefaits, notamment ceux nuisibles à la santé publique, en transit dans les ports de l'Union européenne

LA PROTECTION DES INFRASTRUCTURES CRITIQUES : UNE COMPOSANTE DE LA REFLEXION STRATÉGIQUE GLOBALE DE L'ENTREPRISE

MICHEL POZZO DI BORGO

Adjoint au directeur de la sécurité de la Banque de France
Président de la commission « OIV & Protection des installations » du CDSE

La caractérisation de la criticité d'une infrastructure est loin d'être chose aisée. Chaque manager peut en effet considérer, en toute bonne foi, que les locaux au sein desquels sont conduites les activités dont il a la responsabilité, ou qui participent à la réalisation de celles-ci, doivent être impérativement préservés en toute circonstance.

Et, de facto, considérer qu'ils sont critiques et doivent faire l'objet de la plus grande protection possible… Maîtriser une telle approche, source d'inflation des demandes et donc des coûts afférents, impose d'analyser la criticité des infrastructures au niveau global de l'entreprise et en prenant en compte les interdépendances avec d'autres opérateurs. Dans cette approche corporate, les infrastructures dont l'atteinte à la pleine opérabilité viendrait compromettre les missions d'importance vitale de l'entreprise ou engendrerait un risque pour la santé voire la vie de la population doivent être considérées comme critiques au sens de la sécurité physique.

Cette définition renvoie inéluctablement à l'analyse stratégique des processus d'activité et des risques associés, qui doit permettre de les hiérarchiser et in fine d'identifier les locaux, zones ou périmètres essentiels sur lesquels il convient de porter les efforts - et les budgets correspondants - de protection.

Un travail collaboratif d'importance est donc à conduire par les directeurs sécurité-sûreté corporate, en lien étroit avec les lignes métiers et sur la base d'une approche faisant jouer les synergies entre les démarches de cartographie des risques, de BIA[1], de carte stratégique ou encore de continuité d'activité…

Au final, ce travail de recensement permet de livrer une cartographie précise des infrastructures sensibles de l'entreprise, qui sont de taille variable (ex. : PC de sécurité, locaux techniques, zones de production de fluides, salle de marchés…) et pouvant être imbriquées les unes dans les autres.

LA DÉMARCHE DE PROTECTION : DE L'ANALYSE GLOBALE DES MENACES À LA MISE EN ŒUVRE DES DISPOSITIFS

L'évaluation du risque est au cœur de chaque décision en matière de sécurité physique. Une approche progressive, par cercles concentriques successifs, est indispensable :

L'analyse globale des menaces a pour objectif d'apprécier l'environnement potentiellement hostile dans lequel évolue l'entreprise. Celles-ci peuvent être classiquement réparties en menaces passives (aléas climatiques, environnementaux, technologiques…) et menaces actives (induites par une personne ou un groupe de personnes), et doivent être évaluées en impact et en probabilité, en tenant compte des caractéristiques de fonctionnement de l'entreprise. À titre d'illustrations, des menaces aussi diverses que celles relevant du terrorisme, de l'activisme social, de la malveillance, mais également de l'exposition à des risques naturels (crue, zones sismiques…) ou industriels (proximité éventuelle d'activités type Seveso ou AZF…) doivent être ainsi analysées. Sur un plan pratique, ce panorama général peut prendre la forme :

- D'analyses transverses, voire de tendance très générale, en utilisant par exemple les méthodes d'analyse stratégique de type PESTEL[2] permettant de caractériser l'environnement de l'entreprise ;
- D'analyses détaillées des différentes thématiques de menaces : chaque étude a pour objectif de clarifier le sujet, de recenser les événements ayant réellement affecté des entreprises dont l'activité est proche ou comparable, d'en évaluer les impacts et la probabilité et de lister les dispositifs de protection ayant fait la preuve de leur efficacité ou, a contrario, de leur inutilité.

Ce travail de surveillance permanente de « ce qui pourrait arriver » (les menaces réalistes ou crédibles), tant en situation d'exploitation normale qu'exceptionnelle[3] doit s'appuyer sur toutes les sources d'informations disponibles (données historiques, benchmarks auprès d'organisations comparables, relations avec les forces de sécurité ou les services ad hoc de l'État…).

- Une fois les menaces crédibles (dont la collection constitue l'environnement de danger de l'entreprise) identifiées, une évaluation de la vulnérabilité doit être réalisée au plus près du terrain, en tenant compte des forces et faiblesses de chaque « zone » de l'entreprise (ex. : zone publique, semi-publique, zones d'accès restreint, zones ultra-confidentielles…). Pour ce faire, l'expérience des hommes de la sécurité de l'entreprise est essentielle car ils doivent être en mesure d'imaginer des scénarii d'événements possibles et d'en caractériser finement le déroulé et les modalités pratiques (ex. : recours à des explosifs, usage de véhicules béliers, attaque via un « comité d'accueil », recours à des drones, utilisation d'agents chimiques ou biologiques…). La conjugaison des menaces et des vulnérabilités permet de caractériser le risque et, de facto, d'engager les actions visant à le prévenir ou en limiter les impacts : ce travail constitue le défi permanent des directeurs sécurité-sûreté corporate et l'unique justification des ressources - significatives - qu'ils sont amenés à mobiliser dans l'organisation.

[1] BIA = Business Impact Analysis ou Analyse des impacts sur l'activité : démarche permettant d'évaluer l'impact de différents événements de nature et d'ampleur variables sur la conduite des activités

[2] Domaines d'analyse de la méthode PESTEL : Politique, Économie, Social, Technologie, Écologie. Il convient en particulier de prêter la plus grande attention aux situations provoquées par la réalisation de travaux (affaissement des défenses périmétriques, recours à de nombreux prestataires, mise en place de procédures dégradées…)

[3] Il convient en particulier de prêter la plus grande attention aux situations provoquées par la réalisation de travaux (affaissement des défenses périmétriques, recours à de nombreux prestataires, mise en place de procédures dégradées…)

> S'agissant des dispositifs de protection à mettre en œuvre, il sera utile de se référer aux concepts et approches usuellement déclinés dans la profession. Sans que la liste présentée ci-après puisse être considérée comme exhaustive, plusieurs notions ressortent en priorité :

- Le concept de « défense en profondeur » permet de concevoir une sécurité graduellement renforcée du périmètre bâtimentaire vers son cœur, en reposant sur une approche zonée ;
- Le concept des 4D – *Deter/Detect/Defence/Delay*[4] fixe les objectifs essentiels de protection ;
- L'approche HOT (Humain/Organisationnel/Technologie) édicte l'absolue nécessité de conjuguer dispositifs techniques, organisationnels, réglementaires… mais également humains pour arriver à une protection efficace et efficiente.

Enfin, la plus grande attention doit être portée au cadre réglementaire régissant le cas échéant l'activité de l'organisation. En étroite articulation avec le service juridique, les directeurs sécurité-sûreté corporate doivent être en situation de se maintenir en conformité avec les multiples – souvent complexes et toujours onéreux – impératifs établis par les autorités étatiques (citons le code de la Défense et l'IGI 6600 de janvier 2014 sur la sécurité des activités d'importance vitale, les directives nationales de sécurité pour chaque secteur d'importance vitale, les exigences de sécurité des systèmes d'information posées par la Loi de Programmation Militaire, le RGPD…). ■

[4] Dissuader / Détecter / Défendre / Retarder

RECOM > MANDATIONS

À l'attention des directeurs de la sécurité

> Considérer la protection des infrastructures critiques comme une résultante de la réflexion stratégique globale de l'entreprise Pour ce faire, faire jouer les synergies entre les différentes approches hiérarchisant la criticité des activités et/ou des risques et coopérer activement avec les lignes métiers utilisatrices de ces infrastructures

> Établir une cartographie détaillée des infrastructures critiques et faire valider celle-ci par les instances dirigeantes de l'entreprise (COMEX ou équivalent)

> Mettre en place un processus de veille permanente sur la nature des menaces et leur évolution, et porter périodiquement ce panorama à la connaissance des autorités dirigeantes

> S'assurer de la complémentarité des dispositifs de protection humains, organisationnels et techniques

À l'attention des autorités

> Associer les directeurs de sécurité-sûreté corporate des grandes entreprises à l'élaboration des textes de référence afin d'en évaluer la pertinence et d'en estimer le coût induit

> Renforcer la convergence et la cohérence des textes, afin que les directeurs sécurité-sûreté corporate puissent bénéficier d'un cadre général de référence plus simple et plus homogène

DÉFINIR UNE POLITIQUE DE SÉCURITÉ GLOBALE AU SEIN DE L'ENTREPRISE

ANTOINE CREUX

Directeur de la sécurité du groupe Société générale
Administrateur et trésorier du CDSE

Force est de constater que les enjeux de sécurité auxquels les entreprises sont confrontées se sont renforcés, depuis quelques années, tout en se diversifiant et en s'entrelaçant.

En France, les entreprises doivent faire face à un risque terroriste qui ne faiblit pas, même s'il a changé de nature, porté essentiellement aujourd'hui par des individus souvent isolés, sous l'influence du groupe État islamique et de sa propagande. La libération de plusieurs dizaines d'islamistes condamnés pour terrorisme comme celle de prisonniers radicalisés au cours des prochaines années, amplifie par ailleurs la menace terroriste. Les actions conduites en marge des mouvements revendicatifs ont atteint un niveau de violence inégalé, comme l'a montré la crise des « Gilets jaunes », et les actions de désobéissance civique se multiplient avec leur impact direct sur l'activité de certaines entreprises.

Les mêmes grandes tendances sont observées à l'étranger. L'impact de la pandémie sur l'environnement géopolitique mondial et l'accentuation des conflits en cours continueront d'alimenter les questions de sécurité régionale. Qu'il s'agisse des troubles sociaux dans les pays en développement, principalement liés au ralentissement de l'activité économique mondiale, des menaces terroristes émergentes notamment dans le nord du Mozambique et dans le Golfe de Guinée qui s'ajoutent à celles en expansion dans la région du Sahel, de la gestion des conflits au Moyen-Orient, de la montée des mouvements de contestation en Europe, des tensions économiques comme vecteurs de conflictualité, les défis de sécurité sont et resteront majeurs pour les opérations et le développement des entreprises françaises à l'international.

Enfin, le contexte actuel est marqué par un niveau de menace cyber extrêmement élevé que confirme le nombre exponentiel d'entreprises ayant fait l'objet d'attaques avec des impacts significatifs en 2021. Les cybercriminels sont souvent à la recherche de gains financiers mais les entreprises peuvent aussi faire l'objet d'attaques, souvent d'origine étatiques, ayant pour but de subtiliser des informations sensibles ou à des fins de déstabilisation.

Ce panorama non exhaustif des menaces conduit à **évaluer à un niveau élevé le risque de sécurité pour les entreprises, quelle que soit leur taille. Les impacts potentiels sont multiples et peuvent être systémiques pour une entreprise :** atteinte à l'intégrité physique des collaborateurs, détérioration ou destruction des infrastructures critiques, vol d'informations sensibles, atteinte à l'image, contraintes sur son développement… Seule une approche globale peut permettre à l'entreprise de réduire ses risques de sécurité qui s'imbriquent et se superposent.

UN ENVIRONNEMENT MIEUX MAÎTRISÉ POUR DÉVELOPPER L'ACTIVITÉ

Il s'agit donc pour la direction de la sécurité de définir une **politique de sécurité globale** qui décline cette approche globale des risques afin d'anticiper, de protéger, d'être en mesure de réagir et d'améliorer en permanence les réponses aux risques de sécurité, afin de **permettre à l'entreprise de développer son activité dans un environnement mieux maîtrisé.**

Cette politique de sécurité globale intègre l'ensemble des domaines de sécurité : sécurité des personnes et des biens, matériels et immatériels, intelligence stratégique et sécurité économique, gestion de crises et résilience opérationnelle. Elle doit être construite en partenariat étroit entre toutes les équipes qui contribuent à la sécurité au sein de l'entreprise et en dialogue permanent avec les métiers.

Elle s'appuie sur les fondamentaux d'une démarche de sécurité :

> Évaluer le **niveau de menace** et identifier les risques induits ;

> Définir les **politiques de sécurité des différents domaines** et les bonnes pratiques ;

> Concevoir et mettre en œuvre les **dispositifs de sécurité,** adaptés au niveau de menace ;

> Appuyer le **développement du business** ;

> Répondre aux **obligations légales et réglementaires** ;

> Définir et tester les **plans de contingence** ;

> Apporter l'expertise de **gestion des crises** ;

> Évaluer et tirer les **enseignements** ;

> **Sensibiliser, former, entraîner…**

En fonction du domaine d'activité de l'entreprise, de ses implantations et d'autres critères éventuels, la direction de la sécurité pourra porter effort dans tel ou tel domaine, mais elle devra toujours veiller à consacrer suffisamment de ressources à l'anticipation. Il est recommandé de formaliser la politique de sécurité et de la faire valider au plus haut niveau de l'entreprise. Enfin, la mise en place d'indicateurs de type KRI (Key Risk Indicator) permet de mesurer l'efficacité des choix effectués.

LES CONDITIONS DE LA RÉUSSITE D'UNE POLITIQUE DE SÉCURITÉ GLOBALE

L'efficacité d'une politique de sécurité résulte bien sûr de la qualité de sa mise en œuvre et des moyens qui lui sont consacrés. Ainsi, c'est tout un dispositif qui doit être mobilisé afin de réduire l'exposition aux risques de sécurité de l'entreprise.

L'efficacité de **LA GOUVERNANCE** repose sur l'implication de la direction générale et des différents responsables d'entités (business units, usines, filiales…) et sur un alignement des équipes contribuant à la sécurité dans les différents domaines et au sein de l'ensemble des établissements ou géographies de l'entreprise. La direction de la sécurité a dans ce cadre le rôle important d'animation de la communauté de sécurité dans un cadre hiérarchique ou fonctionnel selon les organisations.

De plus, **LES RELATIONS EXTÉRIEURES** à l'entreprise développées avec les services de l'État contribuant à la sécurité sont de nature à éclairer l'appréciation de situation comme le partage d'expérience avec nos pairs, en France et à l'étranger. Le CDSE apporte pour cela un appui précieux aux directeurs de sécurité.

Enfin, **LA RESPONSABILISATION** de l'ensemble des collaborateurs de l'entreprise sur les enjeux de sécurité reste indispensable tant le facteur humain peut être source de vulnérabilité. De nombreuses actions doivent être engagées pour cette mobilisation : formation, messages réguliers, événements particuliers… ■

RECOM > MANDATIONS

> **Une analyse des risques centrée sur l'activité de l'entreprise et son environnement est un prérequis à la mise en place d'une politique globale de sécurité et l'anticipation est clef**

> **Une politique globale de sécurité doit adresser l'ensemble des domaines : sécurité des personnes et des biens, matériels et immatériels, intelligence stratégique et sécurité économique, gestion de crises et résilience opérationnelle**

> **La mise en place d'une gouvernance de la sécurité incluant la direction de l'entreprise, fédérant l'ensemble des équipes et mobilisant les collaborateurs sur les enjeux de sécurité conditionne la réussite de toute politique de sécurité globale**

III. NOUVEAUX ENJEUX & PERSPECTIVES DE LA SÉCURITÉ

LE PHÉNOMÈNE DE RADICALISATION : UN RISQUE POUR L'ENTREPRISE

PIERRE TRAMIER

Directeur sécurité Europe du groupe Danone
Président de la commission « Radicalisations » du CDSE

L'entreprise est un miroir de la société. Que ce soit par conviction idéologique, religieuse, politique, ethnique, ou par sensibilité accrue face aux grands défis de notre temps, un nombre croissant de personnes adoptent des comportements déviants pour faire valoir leurs idées ou croyances.

La cristallisation et l'hypersensibilisation de la société, largement relayée et alimentée par les réseaux sociaux favorisent l'émergence de ce type d'attitude. Auparavant isolé, l'individu trouve un relai à ses craintes ou ses certitudes dans l'espace internet et devient rapidement un acteur, conscient ou inconscient, agissant au nom de la défense ou de la promotion d'une cause qu'il a fait sienne.

L'entreprise fait face aujourd'hui à ces nouveaux acteurs internes et externes qui challengent les organisations et de plus en plus fréquemment, ont recours à l'action violente ou spectaculaire pour donner un écho à leurs convictions et attirer l'attention du plus grand nombre sur leurs initiatives. La visibilité offerte par internet et les réseaux sociaux sur le plan international favorise une appropriation des causes par tout un chacun et une accélération du processus de radicalisation.

Par ailleurs, si jadis une candidature pour un emploi était souvent motivée, entre autres, par la perspective d'évolution de carrière, le salaire, la sécurité que pouvait offrir l'organisation, de nos jours, c'est le choix sociétal, l'investissement dans des causes perçues comme « justes », dans lequel la personne se retrouve, qui arrive en tête des critères de choix des plus jeunes.

LE COMPORTEMENT DÉVIANT : UNE MENACE DIFFUSE

Face à cette nouvelle donne, l'entreprise, en quête de légitimité et soucieuse d'attirer les talents et de capter les savoirs faire, risque ainsi de perdre sa neutralité et d'être à son tour engagée dans un processus militant. Le risque que représente l'activisme ou les différentes formes de radicalités est bien présent et menace essentiellement l'image et la réputation. En effet, la notion de marque est largement malmenée et très souvent remise en question ou challengée par telle ou telle mouvance radicale.

Dans l'agro-alimentaire par exemple, l'insertion du doute dans l'esprit du consommateur sur la légitimité de l'entreprise ou sur sa capacité à garantir la sécurité des aliments suffit à fragiliser durablement le capital confiance de tout un chacun et conduit parfois à la disparition pure et simple de l'organisation. Dans l'industrie, une remise en question de l'éthique instrumentalisée par des groupes radicaux peut sinon être fatale mais au moins contraindre l'industriel à de profondes réorganisations couteuses et incertaines.

LE DIRECTEUR SÛRETÉ : UN ACTEUR MAJEUR

Si l'action sur ce phénomène de société se situe hors du périmètre de contrôle de l'entreprise, il revient toutefois à la direction sûreté de participer à l'action de sensibilisation, sous le leadership de Ressources Humaines, afin de mettre en œuvre, par anticipation, un cadre favorable pour protéger l'entreprise.

À ces fins, quatre étapes apparaissent nécessaires :

LA SENSIBILISATION des Comités exécutifs et la prise en compte du risque de radicalité dans le champ des possibles est une première étape indispensable. Pour nombre d'entre nous, le phénomène de radicalisation est encore trop souvent et systématiquement associé aux convictions religieuses et au passage à l'acte violent, au terrorisme. Dès lors que leurs activités n'ont jamais été impactées, nombre d'organisations ne se sentent pas concernées.

Avec l'appui d'un sponsor au sein du Comité exécutif, la direction des ressources humaines pourra initier une démarche transversale en installant autour d'une table les directions des finances et juridiques, ainsi que toutes les entités de l'entreprise ayant une légitimité pour traiter ce sujet. La direction sûreté apportera son analyse et son expertise.

Cette deuxième phase, dédiée à **L'ANALYSE** consistera à :

- Identifier, nommer et définir avec précision, au sein de l'entreprise, les comportements que celle-ci considère comme conformes à ses valeurs et à son fonctionnement ;
- Favoriser et installer une démarche pragmatique et dénuée de toute notion émotionnelle dans le traitement des sujets de radicalité. Il ne s'agit pas de juger de la valeur, de l'intérêt ou du bien fondé de telle ou telle croyance ou conviction. Il s'agira de définir si l'expression de celles-ci sont compatibles ou non avec le fonctionnement de l'entreprise.

La troisième étape sera celle de **LA FORMALISATION** par l'entreprise ou l'organisation, dans tous ses documents statutaires et règlementaires des comportements conformes aux attentes de l'organisation. Plus cette formalisation sera précise, plus il sera aisé d'identifier un comportement déviant et de le traiter.

Enfin, la dernière étape sera consacrée à **LA FORMATION** de l'ensemble de la structure managériale en veillant à équiper les managers de l'ensemble des outils nécessaires et des procédures de gestion d'escalade à suivre pour traiter les cas de comportements déviants auxquels ils pourraient être confrontés.

C'est en installant un véritable dialogue, transparent, objectif, sincère, et dénué de tout aspect émotionnel que l'organisation sera en mesure de définir avec précision son identité et de créer les conditions indispensables à sa protection. En agissant ainsi, la direction sûreté protège d'une part la sérénité et la capacité de l'entreprise à prendre des risques pour se développer et, d'autre part, participe activement au rôle d'éducation et de formation qui incombe de plus en plus aux organisations. ■

RECOM > MANDATIONS

> La direction sûreté doit participer à l'action de sensibilisation au phénomène de radicalisation afin de mettre en œuvre un cadre favorable pour protéger l'entreprise

> La sensibilisation des comités exécutifs et la prise en compte du risque de radicalité dans le champ des possibles est fondamental

> Favoriser et installer une démarche pragmatique et dénuée de toute notion émotionnelle dans le traitement des sujets de radicalité

> Identifier, nommer et définir avec précision, au sein de l'entreprise, les comportements que celle-ci considère comme conformes à ses valeurs et à son fonctionnement et les formaliser dans tous ses documents statutaires et règlementaires

> Former l'ensemble de la structure managériale en veillant à équiper les managers de l'ensemble des outils nécessaires et des procédures de gestion d'escalade à suivre pour traiter les cas de comportements déviants

DIGITALISATION DE LA FONCTION SÉCURITÉ-SÛRETÉ : DES OPPORTUNITÉS & DES RISQUES

CDSE LAB

*Cet article a été rédigé au titre du CDSE Lab par **Clémentine de LAMBILLY** (Orange) et **Pierre-Arthur MAZEAU** (Thales) sous la direction de **Jean GARCIN** (Manpower), co-président du CDSE Lab*

L'invention du PC au milieu des années 70 marque le basculement de notre société vers « l'ère numérique ». Cette ère se caractérise par une croissance exponentielle du nombre d'appareils numériques en circulation et de leurs applications.
Dans les entreprises, ces outils faciles d'utilisation ont permis de fluidifier et d'accélérer la circulation ainsi que la diffusion d'informations en masse, notamment grâce à Internet.

Par ailleurs, les nouvelles technologies transforment les usages tout en apportant de nouvelles solutions. L'utilisation des technologies de sûreté par la fonction sécurité-sûreté dans les entreprises en est une parfaite illustration. Cette mutation numérique constante s'accompagne de l'apparition de nouveaux risques et de l'augmentation de la surface d'attaque des entreprises et organisations. Ainsi, la numérisation des activités nécessite inexorablement la mise en place de mesures défensives face à l'évolution de la menace.

VERS UNE FONCTION SÉCURITÉ-SÛRETÉ « AUGMENTÉE »

Pour les directions sécurité-sûreté corporate, l'utilisation de l'IA (intelligence artificielle), du big data, l'exploitation des données libres d'accès, ou le recours à des dispositifs tels que les drones constituent une révolution de nature à permettre une dissuasion, une réaction et une anticipation toujours plus importantes. Cette révolution est à mettre en perspective avec l'évolution technique des moyens de protection plus traditionnels (clôtures, portes, blindages, etc...) qui, grâce à la technologie, deviennent plus fiables, plus sûres et plus faciles d'utilisation car interfaçables avec les évolutions numériques.

Cette digitalisation accrue implique de repenser le fonctionnement de la fonction sécurité-sûreté en entreprise, sans jamais négliger l'importance de l'humain. En effet, si l'on ne peut décemment faire reposer entièrement une chaîne de sûreté sur des systèmes technologiques, ceux-ci doivent venir appuyer l'action humaine en apportant une aide à la décision et en permettant l'automatisation de certaines tâches. Une utilisation proportionnée et assimilée de la technologie permet ainsi une montée en compétence de la filière, intégrant de nouveaux métiers avec de nouveaux profils plus techniques, au service d'une sécurité globale plus efficiente.

La digitalisation des outils de veille, d'analyse et de gestion de crise est à ce titre une opportunité. Elle permet une réduction du temps de traitement de l'information (montante et descendante), une automatisation de tâches (veille, intégration avec des outils internes-externes), une facilité de préparation et d'accès à l'information (format des procédures de sécurité, accès en multi-plateforme, instantanéité des notifications). Une bonne intégration et utilisation de solutions digitales adaptées permet ainsi d'accroître la productivité et d'augmenter la rapidité d'exécution d'une tâche. Par ailleurs, chaque entreprise possède un nombre exponentiel de données propres à son environnement et à ses activités. Pour les directions sécurité-sûreté corporate, le traitement et l'analyse de ces données par le biais d'applications métiers peut permettre d'affiner la perception des zones de vulnérabilités, de construire des stratégies de protection dédiées, et de mieux anticiper. À ces fins, les directions sécurité-sûreté corporate comptent de plus en plus de data scientist dans leurs rangs.

Les directions sécurité-sûreté peuvent développer leurs propres outils ou acheter des solutions pour traiter rapidement et intelligemment cette masse d'information au quotidien. Cependant, la multiplication des outils, des besoins et des coûts peut rendre complexe le choix entre différentes solutions. Si les directions sécurité-sûreté veulent disposer de solutions performantes, il est souvent nécessaire de recourir à des solutions étrangères, ce qui implique des questions en termes de compliance et de souveraineté des données. Alors que la souveraineté numérique doit devenir un critère de choix, une veille au niveau européen permettant de qualifier des outils adaptés pourrait être un compromis entre besoin et contraintes légales.

La digitalisation de la fonction sûreté, et de façon plus large la numérisation de la société, emportent des enjeux cruciaux quant à l'acceptation par le plus grand nombre quant à l'utilisation de ces nouvelles technologies. Des garde-fous sont ainsi indispensables en matière de respect des libertés individuelles. Ainsi, la définition du cadre juridique propre à chaque outil, l'implémentation de garanties relatives à la protection des données personnelles (contrôle de la CNIL) et du patrimoine informationnel de l'entreprise constituent des préalables indispensables à cette acceptation. À ce titre, les Jeux Olympiques de 2024 représentent une opportunité exceptionnelle pour accélérer la transition vers une utilisation mature, encadrée et acceptée des nouvelles technologies de sécurité-sûreté.

DES ENJEUX DE CYBERSÉCURITÉ MULTIPLES

Cette digitalisation de la fonction sécurité-sûreté n'est pas sans risque. L'ensemble des systèmes de sûreté sont informatisés sur des réseaux locaux ou d'entreprise rendant les organisations plus exposées et plus vulnérables aux risques cyber. La sûreté doit ainsi être au cœur des problématiques de sécurité informatique et la direction sécurité-sûreté corporate doit collaborer efficacement avec les métiers IT, et notamment les experts SSI (sécurité des systèmes d'information) de l'entreprise. La mise en œuvre d'un ensemble de techniques et de solutions de sécurité pour protéger la confidentialité, l'intégrité et la disponibilité des données est indispensable pour garantir des systèmes fiables. Des méthodes comme la *security by design* permettent, dès la conception d'une solution, d'intégrer la sécurité dans le code source. C'est pourquoi l'aide des experts SSI est essentielle afin de garantir une architecture réseau sûre dès l'installation de nouveaux outils de sûreté.

D'autre part, l'utilisation quotidienne d'outils digitaux par le plus grand nombre dans la sphère privée a poussé les outils grand public au cœur du monde professionnel. Cet usage comporte une réelle problématique pour la sécurité informatique des organisations et notamment pour ce qui concerne l'apparition du shadow IT : l'utilisation de technologies matérielles et logicielles par les employés de l'entreprise sans l'accord de leur DSI (direction des systèmes d'information). Le manque d'accompagnement, de garantie de disponibilité de service, de souveraineté des données et de niveau de sécurité informatique des solutions grand public entraînent des failles internes au sein des organisations. Ainsi, le grand cabinet de conseil américain Gartner prévoyait en 2016 qu' *« un tiers des cyberattaques menées avec succès contre les entreprises [en 2020] prendraient pour cible leurs ressources Shadow IT ».* Les grandes attaques cyber, telles que NotPetya en 2017, les lois pour la protection des données personnelles ou la loi de programmation militaire et ses contraintes de sécurité pour les OIV (opérateurs d'importance vitale) ont permis une certaine prise de conscience quant à l'importance des enjeux de cybersécurité.

NOUVELLES TECHNOLOGIES & ACCEPTABILITÉ JURIDIQUE

Nos organisations font face à une digitalisation et une dépendance accrue aux outils numériques. Cette mutation introduit de nouvelles normes alors que nous ne sommes qu'au début du phénomène de numérisation comme le démontrent les projets de « ville intelligente » ou l'avènement de l'Internet des objets. À l'aune des JOP de Paris 2024, l'État doit fixer un cadre juridique précis pour l'usage des nouvelles technologies de sécurité comme la biométrie ou la reconnaissance faciale, tant dans le domaine public que privé, et notamment dans les entreprises.

En effet, le manque de clarté peut nuire aux efforts de digitalisation, puisque les entreprises ne possèdent pas toujours les moyens légaux pour déployer de nouveaux outils. Malgré l'entrée en vigueur du RGPD et le contrôle grandissant de la CNIL, l'utilisation des nouvelles technologies de sécurité est encore perçue comme étant particulièrement intrusive. En adaptant l'environnement juridique et donc l'encadrement de l'utilisation de ces nouvelles techniques, l'État optimiserait non seulement l'efficacité de la sécurité publique, il appuierait la mission des directeurs sécurité-sûreté corporate dans leur mission de protection de leurs intérêts, de leurs salariés et de leurs clients pour une sécurité plus globale de l'ensemble des citoyens tout en garantissant la protection de leurs données personnelles. ■

RECOM > MANDATIONS

> Doter les technologies de sécurité d'un cadre juridique, sous le contrôle strict de la CNIL afin de garantir la protection des libertés publiques et individuelles

> Mettre en place des politiques hybrides dans les directions sécurité-sûreté alliant un apport plus important des technologies de sûreté permettant à l'humain de gagner en réactivité, anticipation et compétence

> Intégrer les compétences d'analyse et de traitement des données (big data) au sein de la fonction sécurité-sûreté

> Intégrer la SSI dès la conception ou la mise en place de nouvelles technologies de sûreté

> Prévoir des solutions alternatives non numériques aux technologies de sécurité-sûreté afin de se prémunir en cas de cyberattaque et tester la mise en place de ces solutions lors d'exercices planifiés

> Intégrer et promouvoir les critères de souveraineté dans le choix des solutions numériques

PENSER & IMAGINER L'IMPENSABLE, MANAGER L'INCERTITUDE

COMMISSION « GESTION DE CRISE & CONTINUITÉ D'ACTIVITÉ » DU CDSE

*Cet article a été rédigé au titre de la commission « Gestion de crise et Continuité d'activité » du CDSE par **Gabrielle BERTHELOT**, head of crisis management au sein de la direction sûreté du groupe Kering et **Anne PICOT-PERIAC**, directrice sûreté du groupe Atos.*

Penser l'impensable, manager l'incertitude… ces ambitions pourraient faire sourire, et pourtant il est nécessaire de s'y attarder afin d'augmenter ses chances de survie dans un monde en constante évolution, dans lequel les bouleversements s'accélèrent à une vitesse vertigineuse depuis le début du 20e siècle, le rendant ainsi de plus en plus complexe.

Cependant, notre cerveau humain n'apprécie pas l'incertitude et se refuse souvent à imaginer l'impensable. Peu importe la nature du cataclysme ou de l'attaque, les seules considérations à prendre en compte sont les effets et impacts sur l'organisation et comment les limiter et les surmonter. Le scénario n'est finalement qu'une aide à l'imaginaire et l'analyse des impacts permet d'élaborer une réponse pragmatique afin de se préparer.

Cet exercice de réflexion permet de réduire l'effet de surprise lorsqu'un événement perturbateur et imprévu survient.

Parmi les nombreux modèles existant pour accompagner la conduite du changement, celui du Dr Kübler-Kloss peut être utilisé pour comprendre les étapes par lesquelles peuvent passer les individus confrontés à un changement brusque (choc, déni, colère, peur, tristesse, dépression, acceptation, pardon, quête de sens, sérénité, croissance). Tout l'enjeu est de limiter le temps passé dans les premières étapes, qui sont très énergivores pour le cerveau humain, afin d'atteindre rapidement la phase dite de l' « acceptation », qui permet de passer à l'action avec un état d'esprit plus positif et éclairé.

Percevoir en amont qu'un fait va se produire, est la meilleure manière d'anticiper un événement perturbateur, un incident ou une crise. A minima au niveau corporate, il faut mettre en place des alertes sur :

> La situation géopolitique, sanitaire, climatique là où l'organisation a des intérêts ;

> Les mots clés dans les médias sociaux ;

> Les nouveaux textes de lois, la jurisprudence et les évolutions de règlementation ;

> Les nouveaux virus informatiques, les nouvelles failles et les mises à jour.

Il ne faut pas négliger la veille interne à l'organisation (exemples : la surveillance des réseaux informatiques, « l'écoute » du climat social…). Les échanges que chaque département peut avoir à l'extérieur avec des partenaires, des clients ou des concurrents dans son propre secteur d'activités ou dans d'autres, doivent également figurer dans le dispositif de veille. Cette pratique permet de capter les tendances et évaluer les aspects qualitatifs.

COMMENT IDENTIFIER LES RISQUES DE L'ORGANISATION ?

Plusieurs normes ISO et référentiels portent une approche de la sécurité par les risques : regarder les processus de l'entreprise, **identifier les actifs/ressources utiles** pour mener ce processus à bien (exemples : sites, personnes, chaine d'approvisionnement, systèmes d'information…), les menaces et les vulnérabilités qui pèsent sur ces actifs, et enfin évaluer la probabilité et l'impact en cas de matérialisation d'un de ces risques. La phase suivante consiste à définir les plans d'actions pour limiter les impacts.

Un entretien avec les membres du comité de direction permet une approche complémentaire : elle offre l'opportunité de demander à chacun d'entre eux quel serait ***« leur pire cauchemar pour l'entreprise »*** dans leur domaine de compétence. Ce point de vue constitue une bonne base de travail pour imaginer des scénarios de crise.

COMMENT APPRENDRE À DÉCIDER DANS L'INCERTITUDE ?

S'il est indispensable de s'exercer par des simulations de crise basées sur des scénarios réalistes et adaptés à l'activité de l'organisation pour tester les plans et procédures, il est également nécessaire de former les équipes qui seront amenées à affronter un événement d'ampleur, à appréhender l'effet de surprise, gérer l'incertitude et ainsi développer leurs facultés d'adaptation.

La mise en marche rapide et efficace de l'organisation de crise dépend donc des équipes, de leur capacité à comprendre rapidement la situation, se poser les bonnes questions et trouver les ressources pour y répondre.

Avant chaque prise de fonction, et quel que soit son domaine d'activité, un manager devrait être sensibilisé aux problématiques de « remontée » d'événement perturbateur, de gestion de crise et de continuité d'activités. La probabilité est grande qu'il/elle y soit confronté directement ou indirectement au cours de sa carrière.

Mais si l'expérience est un facteur de succès, elle peut aussi induire des biais, et cela requiert beaucoup d'efforts et d'humilité pour appréhender chaque situation avec un regard neuf, afin de poser le problème, comprendre les impacts, délimiter ce qui entre dans le périmètre de responsabilité de l'organisation et intégrer les contraintes qui ne peuvent être contrôlées.

Pour développer, entraîner et renforcer les capacités cognitives des équipes de crise, il serait intéressant de les exercer à penser, réagir et décider tout en étant déstabilisées et sorties de leur zone de confort. Intervertir les rôles de chacun dans la cellule de crise à chaque session de formation, ou les rôles des cellules de crise entre elles, travailler sur des scénarios inconnus, voire complètement loufoques, ou supprimer les moyens et outils habituels peuvent être des façons de développer la cohésion et l'empathie, mieux comprendre les enjeux et les contraintes de chacun tout en envisageant l'impensable avec humilité.

L'utilisation de la technologie dans nos modes de travail donne une fausse sensation d'assistance, de sécurité et de contrôle. Cependant, face à des situations extrêmes qui dépasseraient toutes les prévisions et/ou priveraient l'organisation de ses moyens, il pourrait être utile de pouvoir compter sur des équipes qui savent prendre des décisions avec bon sens et en faisant confiance à leur intuition malgré l'incertitude.

Au début de la crise, il est bien sûr recommandé de rechercher des crises similaires pour s'inspirer des bonnes pratiques et utiliser les éléments comme base de travail. Cela a deux vertus : faire gagner du temps sur la compréhension des enjeux, des pièges et l'identification des acteurs de la crise et éviter de partir d'une feuille blanche. Le corollaire inévitable est que, dans l'esprit des membres de la cellule de crise, un parallèle peut s'établir entre les deux crises.

Il faut rester prudent. L'attribution des tâches (collecte d'informations, analyse, projection de l'impact pour l'organisation) à des équipes distinctes doit y contribuer.

Une vérité à un instant T peut s'avérer fausse quelques heures après. Là encore, des modèles comme la roue de Deming ou la boucle OODA prennent leur sens. **Observer, s'Orienter, Décider, Acter** et reprendre l'observation et l'analyse des changements à la fin de cette première boucle pour lancer la deuxième. **Accepter de se tromper.**

Les membres des équipes de crise doivent être rassurés, leur responsabilité clairement explicitée et leur périmètre de décision et d'action défini avec des limites liées à l'organisation et des compétences précises. Au préalable, les objectifs de chaque cellule de crise doivent être énoncés. La cellule de crise doit se recentrer à intervalle régulier sur ceux-ci. Une entreprise privée ne va pas se substituer aux services d'urgence. En revanche, il relève de sa responsabilité de bien s'interfacer avec eux dans l'intérêt de ses collaborateurs et de sa continuité d'activités.

En conclusion, s'il est impossible de penser l'impensable, il est possible de réfléchir sur les conséquences de l'impensable pour l'organisation et ainsi, manager l'incertitude. ■

RECOM > MANDATIONS

L'objectif est de voir comment l'organisation peut mettre en place des contre-mesures, pour pallier ces indisponibilités. Ensuite, en prenant des scénarios catastrophes, il est possible de projeter ces indisponibilités dans le contexte proposé et d'ajuster les plans proposés.

Avec cette approche rationnelle, il sera plus facile de convaincre un comité de direction d'investir dans une contre-mesure même si le scénario proposé à une probabilité faible voir nulle.

> Réfléchir à l'indisponibilité des ressources :

- Personnes

  Comment ferions-nous si les collaborateurs pour X raison(s) ne pouvaient pas venir travailler ? Comment ferions-nous s'ils n'étaient pas en état de travailler même depuis leur domicile ?

- Sites

  Comment ferions-nous si les sites étaient inaccessibles, partiellement ou totalement détruits ?

- Système d'information

  Comment ferions-nous sans réseau informatique ? Sans système d'information ? Sans système de communication ?

- Chaîne d'approvisionnement

  Comment ferions-nous si nos fournisseurs ne pouvaient plus nous livrer ?

> Analyser l'impact de scénarios apocalyptiques sur l'organisation

> Équiper les équipes de crises pour faire face à des situations extrêmes en développant leurs capacités cognitives sous stress

> OSER !

LES DIRECTEURS SÉCURITÉ-SÛRETÉ CORPORATE DANS LE CONTINUUM DE SÉCURITÉ : UNE VOLONTÉ À CONCRÉTISER

ANNICK RIMLINGER

Directrice Sûreté-Sécurité, Cyber & Data protection du groupe Aema

Les attentats de 2015 ont mis en exergue, dans un pays traumatisé par ces événements, que la sécurité de la Nation est aussi, reprenant une assertion popularisée par beaucoup d'experts et d'hommes politiques, « l'affaire de tous ».

Ce nouveau paradigme qui consacre un rôle à chacun de ces acteurs se manifeste également par l'apparition d'une sémantique nouvelle autour de la notion de *continuum* de sécurité qui n'avait jusqu'alors jamais été utilisée en tant que tel pour décrire un transfert de certaines missions et le rôle de nouveau acteurs. Le *continuum* de sécurité a ainsi comme ambition de faire prospérer une chaîne d'intelligence collective dans la sécurité, qui peut contribuer à l'objectif vital de diffuser une culture de vigilance formant le meilleur rempart pour défendre la République et ses idéaux.

Dans la continuité du lancement en 2017 de la réforme de la Police de Sécurité du Quotidien (PSQ) dans les premiers mois du quinquennat d'Emmanuel Macron, l'exécutif a souhaité conceptualiser cette chaîne reliant tous les acteurs de la sécurité nationale, base d'une sécurité globale construite sur une collaboration pleine et entière entre les forces de sécurité publique et les acteurs privés.

Les travaux des députés de la majorité LREM Alice Thourot et Jean-Michel Fauvergue ont de ce point de vue constitué une première étape. Dans leur rapport intitulé *« D'un continuum de sécurité vers une sécurité globale »*, commandé par le ministre de l'Intérieur Gérard Collomb et remis au Premier ministre Edouard Philippe en septembre 2018, les deux parlementaires formulaient 78 propositions, dont un certain nombre étaient relatives à la place des entreprises et des directeurs sécurité-sûreté dans le *continuum* de sécurité, telles que :

> Revaloriser le rôle et le positionnement des directeurs de la sécurité dans les entreprises ;

> Créer un statut de correspondant sécurité (CS) au sein des entreprises ;

> Ouvrir la possibilité d'habiliter les titulaires de ces fonctions au confidentiel-défense.

En succédant à Gérard Collomb, place Beauvau, en octobre 2018, Christophe Castaner, s'approprie ces préconisations et indique, lors son discours en ouverture de l'édition 2019 du colloque du CDSE, que le directeur sécurité *« doit être un acteur central pour la notoriété d'une société, pour ses collaborateurs en France comme à l'étranger, pour ses clients et ses fournisseurs, pour ses processus de fabrication ou ses systèmes d'information »*. Le ministre de l'Intérieur poursuivait en assurant que *« l'État est disposé à aider le directeur sécurité pour mener à bien sa mission, y compris en créant un réseau de confiance afin d'échanger au plus haut niveau des informations sensibles ». « Il est essentiel que ce cercle de confiance se construise entre nous »*, appuyait-il.

Néanmoins, force est de constater qu'aucun directeur sûreté ne ressemble à un autre, et qu'il y a autant de périmètres de responsabilités que d'organisations de la fonction sécurité-sûreté au sein des entreprises. Malgré ce paysage tout en contraste, leur positionnement s'ancre bien dans le cadre du *continuum* mais il n'est à ce stade pas encore assez affirmé pour peser dans le débat public.

DES DIRECTIONS SÛRETÉ HÉTÉROGÈNES MAIS DOTÉES D'UNE NOUVELLE VISIBILITÉ

Depuis les années 2000, la grande majorité des entreprises a pris conscience de l'importance de mettre en place une démarche de sûreté au sein de leur structure. Pour certains groupes, il s'agit d'une véritable stratégie qui, au même titre que d'autres, favorise son développement. Les dirigeants ont en effet bien mesuré qu'il leur appartient d'organiser la sécurité et la sûreté de leur organisation. Mais la plupart du temps, il reste encore à mettre en œuvre une organisation en adéquation avec les objectifs assignés au directeur sécurité-sûreté.

La mission des directeurs sécurité-sûreté en entreprise (DSE) est complexe et étendue. Ils doivent tout à la fois identifier les nouveaux risques portant sur les assets les plus sensibles ou précieux de leurs entreprises, mais aussi assurer la protection de leurs collaborateurs, de leurs clients, lutter contre les atteintes à l'image ou à la réputation et enfin prévenir toutes les formes de malveillances perpétrées dans le monde physique ou dans le cyberespace. Le périmètre des missions d'un DSE est large et l'approche de sécurité globale, que tous appellent de leurs vœux, n'est pas le quotidien d'un certain nombre d'entre eux, confrontés à un éclatement des responsabilités avec des expertises qui peuvent être exercées dans d'autres directions.

Néanmoins, l'étude sur les métiers de la filière sécurité-sûreté corporate du CDSE[1] montre que 75 % des DSE sont rattachés à la direction générale, au secrétariat général ou au comité exécutif. Ce qui permet à un nombre non négligeable de directeurs sûreté de peser sur les décisions stratégiques des entreprises et d'en être de véritables « business partner ». Ce nouveau positionnement interne acquis notamment à la faveur du rôle déterminant joué lors de crises (attentats, covid, incidents internes, prévention des risques…) conforte le rôle décisionnel de ces derniers. Cette légitimité interne conquise auprès des Directions Générales et des métiers se traduit également par une nouvelle visibilité externe favorisée par le lobbying du CDSE auprès des politiques et des services de l'État.

Le DSE est donc à la fois le représentant et l'interlocuteur de son entreprise auprès des institutions au premier rang desquelles, le ministère de l'Intérieur, et devient de facto partenaire du *continuum* de sécurité. C'est ce rôle que reconnaissait le ministre Christophe Castaner dans son intervention mentionnée plus haut.

LE RÔLE DES DIRECTEURS SÛRETÉ DANS LE CONTINUUM

Le rôle des directeurs sûreté dans le *continuum* de sécurité a donc trouvé toute sa reconnaissance dans les travaux de conceptualisation menés par l'État depuis 2018. Néanmoins, la présence d'un DSE dépend aujourd'hui de la seule volonté de l'entreprise qui décide d'investir dans la prise en compte du risque sûreté. Les fonctions du DSE font de lui l'interlocuteur légitime des services de sécurité de l'État. Cette reconnaissance constitue un premier maillon de la chaîne du *continuum*. Pour certaines entreprises particulièrement exposées, l'idée que ce professionnel soit habilité « confidentiel défense » a prospéré. C'est également le cas pour ce qui concerne l'État, et notamment le SGDSN[2]. Néanmoins, si l'idée de créer un tel « cercle de confiance » a été reprise et présentée dans différentes instances, elle n'a cependant pas trouvé de concrétisation à ce jour.

Le directeur sécurité-sûreté est donc appelé à devenir le point focal de la collaboration voulue entre les forces de sécurité publique et le secteur privé. Il est attendu de sa part de faire remonter aux différents services de l'État les informations dont il dispose et les éventuelles problématiques qu'il rencontre (signaux faibles, suspicions de radicalisation…). Ces échanges existent dans les faits depuis l'arrivée des premiers directeurs sûreté dans les entreprises et bénéficient d'un encadrement juridique pour les DSE exerçants dans des OIV[3], du fait de leur statut d'officier de sécurité. Pour les autres, cet échange d'informations reste souvent structuré autour de réseaux personnels relatifs au passé régalien du directeur ou à des ponts bâtis de façon empirique au cœur d'une crise. Cependant, si les échanges existent, ils restent souvent unilatéraux, les DSE ne bénéficiant que rarement de retours sur les situations signalées. À cet égard, le lobbying du CDSE permet toutefois de faire se rencontrer les directions et services de l'État (SGDSN, ANSSI, Police, Gendarmerie, services de renseignement…) et les DSE à l'occasion de commissions sectorielles et conférences.

Toutefois, le *continuum* peut aussi se matérialiser par des initiatives locales et pragmatiques : depuis décembre 2018 et le début du mouvement dit des « Gilets jaunes », le CDSE assiste chaque semaine à une réunion animée par le préfet de police de Paris en amont des manifestations. Les informations partagées permettent aux entreprises d'anticiper et de mieux se prémunir contre les actes de malveillance qui peuvent accompagner ces mouvements.

[1] Cf. « *Le directeur Sûreté : une fonction stratégique au cœur d'un large écosystème d'acteurs et de compétences* », P. 18

[2] SGDSN : Secrétariat général de la défense et de la sécurité nationale

[3] OIV : Opérateur d'importance vitale

Les entreprises peuvent en outre faire remonter leurs points d'attention avec les services de la Préfecture de Police dans un échange « gagnant-gagnant ».

Un deuxième maillon du *continuum* s'incarne dans les nouvelles formations sur la sécurité-sûreté corporate qui se sont développées et qui réunissent un public mixte composé d'agents publics et de collaborateurs du privé. Ces enseignements de haut niveau proposés à l'IHEMI, à l'IHEDN ou encore à l'ENSP et à l'EOGN permettent de parfaire une forme de connaissance réciproque et de mettre en exergue les apports du privé et du public en matière de sûreté. Ces formations illustrent la porosité désormais assumée entre sécurité publique et privée, ainsi que les besoins mutuels. Mais dans un contexte de menaces permanentes, terroristes ou économiques, les entreprises bénéficient également d'actions de sensibilisation de la part des services de l'État, tels que la DGSI (Direction Générale de la Sécurité Intérieure) ou le Renseignement Territorial, qui permettent de diffuser une culture commune sur des problématiques telles que l'ingérence économique, les radicalisations, la cybersécurité, et ainsi d'associer et de responsabiliser au plus haut niveau de l'entreprise. Les DSE sont souvent à l'initiative de ces interventions et deviennent ainsi de facto les interlocuteurs naturels des services sollicités.

Enfin le *continuum* de sécurité s'illustre par la capacité offerte aux directeurs sûreté de solliciter, partout sur le territoire, des référents sûreté, policiers et gendarmes spécialisés, afin d'être accompagnés sur les problématiques spécifiques de leurs assets, en termes de niveau de sécurité optimal à mettre en œuvre pour certains sites sensibles ou encore d'installation des systèmes de vidéoprotection.

Les unités d'intervention de la police et de la gendarmerie nationales, le RAID et le GIGN, proposent également aux DSE exerçant dans des groupes plus particulièrement exposés au risque terroriste, de partager une cartographie des actifs de leur entreprise. Le but est de pouvoir intervenir en cas de crise en connaissant la géographie des bâtiments, tout en bénéficiant d'un interlocuteur privilégié et mobilisable, le directeur sécurité-sûreté corporate.

À l'étranger, les DSE des grandes entreprises françaises peuvent compter sur le réseau des attachés de sécurité intérieure, présents dans chaque ambassade et pilotés par la Direction de la coopération internationale de sécurité (DCIS). Ces derniers leur permettent de disposer d'informations sur l'état des menaces mais peuvent aussi leur prêter concours et assistance dans certaines situations qui exposent leurs collaborateurs.

LA PLACE DU DSE DANS LE CONTINUUM RESTE À CONSOLIDER

Le *continuum* et la nouvelle association public-privé qu'il promeut ne posent aujourd'hui plus réellement question et semblent s'être inscrits dans le sens de l'Histoire. Mais les modalités de sa mise en œuvre restent à préciser… Et surtout pour les directeurs sécurité-sûreté corporate.
La formalisation du *continuum* reste ainsi souvent à la main des entreprises qui doivent être proactives pour se faire connaître des services de l'État (indépendamment des OIV et des plus grandes d'entre elles qui bénéficient de leur notoriété). Les DSE exerçant ainsi dans ces entreprises « moins visibles » doivent avoir une démarche volontariste et aller à la rencontre des différents interlocuteurs régaliens, tant les services de sécurité ignorent souvent que de tels professionnels existent.

Le niveau de relation reste également conditionné aux obligations réglementaires. Le « cercle de confiance », dont ne bénéficient aujourd'hui que certains de ces professionnels exerçants dans des OIV et OSE[4] , doit sans plus tarder s'étendre à tous les directeurs sécurité-sûreté corporate. Ainsi, pour les directeurs qui en feraient la demande, la mise en œuvre de l'habilitation « confidentiel défense », demandée depuis 2011 et le premier « Livre blanc du CDSE », constituerait un signal fort et alimenterait la dynamique engagée. La relation de confiance ne se décrète pas, elle se construit dans le temps. De fait, le *continuum* ne saurait reposer exclusivement sur l'existence de relations interpersonnelles qui permettent d'obtenir de l'information. Les directeurs sûreté, par les fonctions qui leurs sont confiées, sont des partenaires de confiance et doivent « pouvoir avoir à en connaître » mais aussi « pouvoir avoir à en partager ».

La question du recensement simple et de l'identification de l'ensemble de ces professionnels, dans chaque entreprise, reste un écueil pour lequel aucune solution ne s'est imposée à ce jour. La délivrance d'une carte professionnelle par le CNAPS[5], évoquée par certains observateurs, ne saurait être satisfaisante dans la mesure où elle consisterait à confier au même établissement public de régulation la carrière du donneur d'ordre et de son prestataire. Si le donneur d'ordre doit agir en toute responsabilité, la fonction de directeur sécurité-sûreté en entreprise n'est ni régulée, ni régulable : elle ne peut entrer dans le périmètre de contrôle du CNAPS. Toutefois, un enregistrement volontaire des directeurs sécurité-sûre-

[4] OSE : Opérateurs de services essentiels

[5] CNAPS : Conseil national des activités privées de sécurité

té auprès du ministère de l'Intérieur aurait l'avantage de les rendre visibles et accessibles auprès des services. Et ainsi pouvoir, à tous moments et pour tous les sites, disposer d'un interlocuteur de haut niveau capable de leur faire ouvrir chaque porte de l'entreprise en cas de besoin.

Le *continuum* doit aussi s'incarner et être animé pour s'ancrer dans le paysage de la sécurité en France. Le délégué ministériel aux partenariats, aux stratégies et aux innovations de sécurité (DPSIS) du ministère de l'Intérieur joue ce rôle d'interface et d'animateur. Mais son rôle pourrait être renforcé en devenant le réel point d'entrée de l'ensemble des revendications sectorielles des DSE.

Pour faire connaître les missions des DSE, les formations des cadres de la police et de la gendarmerie devraient intégrer un module sur la sûreté en entreprise. Les directeurs pourraient y intervenir pour former les officiers sur les spécificités et contraintes de leur métier et, ce faisant, favoriser les futurs échanges.

S'INSPIRER DE LA RSE POUR FAVORISER LE POSITIONNEMENT DE LA FONCTION SÛRETÉ : INTÉGRER LA SÛRETÉ AUX CRITÈRES DE COTATION DE L'ENTREPRISE

En reprenant le modèle de la RSE (Responsabilité sociétale des entreprises), considérée depuis plusieurs années par la Banque de France comme un **« levier de transformation des pratiques et de la gouvernance, vecteur d'innovation et génératrice d'efficience sur le long terme »,** la sûreté pourrait être intégrée, ainsi que cela avait été proposé lors du **colloque 2019 du CDSE**, dans la cotation de l'entreprise pour avoir une vision plus globale de celle-ci, mieux la comprendre et ainsi affiner l'analyse de sa résilience.

La sûreté pourrait, chaque fois que les informations recueillies le permettent, être prise en considération pour apprécier le profil global qui permet d'affiner un critère extra-financier. Le fait de donner ce nouveau rôle à la sûreté favoriserait le positionnement des directeurs sécurité-sûreté et inciterait les CEO à les inviter à siéger au comité de direction ou au comité exécutif.

Si le *continuum* est devenu un peu plus efficient, notamment avec l'action du ministère de l'Intérieur et des ministères qui traitent historiquement des sujets de sécurité des entreprises (Premier ministre, Armées, Europe et Affaires étrangères, Économie et Finances…), il n'a que peu de matérialité avec d'autres (Santé, Travail, Culture…), sauf à travers l'action des Hauts fonctionnaires de Défense, pourtant en première ligne dans la gestion de la crise sanitaire ou de la menace terroriste. Par ailleurs, dans la sûreté du quotidien, il n'existe pas ou très peu de lien entre les entreprises et les représentations de ces ministères dans les territoires.

En 2020, les propositions du rapport Fauvergue-Thourot ont su trouver un nouvel écho dans le Livre blanc de la sécurité intérieure. Ce document, issu d'une large concertation menée par le ministère de l'Intérieur, proposait des évolutions pour une prise en compte de l'ensemble des acteurs et une approche globale des enjeux de la sécurité intérieure. Il positionnait ainsi *« les directeurs de sécurité des entreprises comme des parties prenantes au continuum de sécurité »* et proposait de *« renforcer leur reconnaissance en tant que tels »* par la mise en place *« d'une relation de confiance mutuelle partageant le secret professionnel »*. Néanmoins, ces recommandations n'ont pas trouvé de concrétisation dans la loi du 25 mai 2021 pour une *« sécurité globale préservant les libertés »*. Ce texte, bien que déposé par les députés Thourot et Fauvergue, traite de l'ensemble des contributeurs au *continuum* (polices municipales, sécurité privée, forces de sécurité de l'État…) en omettant cependant les entreprises.

Pourtant, les entreprises privées sont les premiers acteurs de leur propre sécurité et sûreté, ainsi que de celle de leurs parties prenantes (salariés, clients, prestataires…) et, de ce fait, elles sont les premiers donneurs d'ordre de la sécurité privée. Les directeurs sécurité-sûreté corporate concourent ainsi tous les jours dans les faits au *continuum* de sécurité à travers les actions, missions et dispositifs qu'ils mettent en œuvre.

L'État et les entreprises doivent désormais opérer leur rapprochement de manière concrète, afin de mieux se connaitre, développer des relations régulières et instaurer une confiance mutuelle. *« Nous sommes de plus en plus consultés et très souvent plus écoutés qu'entendus. Toutefois, nul doute qu'il est possible de faire mieux encore »*, indiquait Stéphane Volant, président du CDSE, dans une interview publiée en octobre 2021[6]. Ce « mieux » doit enfin se concrétiser par la loi, dans un texte qui consacre la fonction de directeur sécurité-sûreté corporate et le rôle que ces professionnels jouent au quotidien dans les entreprises.

Car les entreprises ne sont jamais qu'une extension du territoire de la République.

Et les directeurs de sécurité-sûreté sont des maillons forts de la chaîne de sécurité globale, du *continuum* de sécurité. ■

[6] Interview de Stéphane Volant, président du CDSE, *Le Monde de la sécurité*, 14 octobre 2021

RECOM > MANDATIONS

- **Intégrer des modules dédiés à la sécurité-sûreté en entreprise dans les formations des cadres de la police et de la gendarmerie**
- **Renforcer le rôle du DPSIS du ministère de l'Intérieur comme animateur du continuum pour les directeurs de sécurité-sûreté**
- **Permettre un enregistrement volontaire des directeurs sécurité-sûreté auprès du ministère de l'Intérieur dans une logique de recensement et d'identification**
- **Consacrer les directeurs de sécurité des entreprises comme des parties prenantes au continuum de sécurité et renforcer leur reconnaissance en tant que tels par la loi**
- **Faciliter les échanges d'informations public/privé dans un «cercle de confiance» bâti sur le secret professionnel ou un processus d'habilitationessus d'habilitation**

QUELLES COMPÉTENCES POUR LE DIRECTEUR SÉCURITÉ DE DEMAIN ?

AURÉLIEN LAMBERT

Directeur sécurité-sûreté du groupe Egis

La pression augmente continuellement sur les sujets de sécurité dans les organisations. Du fait de la complexification des risques et du besoin de confiance que ce phénomène a entraîné pour les parties prenantes, l'enjeu est reconnu comme stratégique. Ainsi, davantage d'entreprises, de toutes tailles et dans tous les secteurs d'activité, se décident à identifier un directeur de la sécurité, à renforcer ses capacités ou son positionnement.

La fonction de directeur sécurité[1] se professionnalise et se normalise donc progressivement pour répondre à ces besoins. Son positionnement évolue progressivement d'un rôle de technicien, lié à l'application de contraintes règlementaires, à celui de chef d'orchestre, en soutien direct des activités.

Dans cette évolution, le directeur sécurité reste encore très seul en France pour se former, structurer sa fonction ou définir des standards pour son organisation. Alors que la pression s'accentue, un enjeu clé des prochaines années pour poursuivre cette montée en compétence sera un travail collectif à mener par les professionnels eux-mêmes.

UNE FONCTION QUI SE DÉVELOPPE LENTEMENT ET DE MANIÈRE HÉTÉROGÈNE EN FRANCE

Lorsque que l'on analyse ces dix dernières années, on note une certaine contradiction. D'un côté les ruptures ont été nombreuses dans l'environnement du secteur privé : terrorisme sur le territoire national et à l'étranger, Covid-19, Ebola, catastrophes naturelles en série, accélération de la menace par le vecteur cyber, guerre commerciale entre les USA et la Chine, Brexit, accord puis rupture avec l'Iran, conflits armés au Levant, au Mali, en Libye, en Ukraine, etc.

Malgré ces événements, nous avons observé une progression relativement lente du rôle du directeur sécurité en France. La fonction reste principalement fondée sur les mêmes jurisprudences depuis dix ans, et donc souvent associée à un rationnel de contrainte règlementaire, plutôt que sur un rationnel d'investissement au profit des organisations et leurs activités. Les raisons sont multiples, probablement relatives à un manque d'alignement des professionnels du secteur, à une insouciance de beaucoup d'organisations, à l'absence de vision de l'État sur l'opportunité du *continuum* de sécurité pour protéger son tissu économique. Pourtant les organisations sont souvent en première ligne face à des risques qui se multiplient. L'accélération des menaces par le vecteur cyber a notamment entrainé une prise de conscience chez beaucoup de dirigeants et au sein de l'État. Cela amène chaque organisation à s'organiser et investir de manière très hétérogène. Ainsi on constate que les lignes de rattachement, périmètres, degrés d'autorité, tailles des équipes, budgets, etc. des directeurs sécurité sont extrêmement variables selon les organisations.

[1] *« Sécurité »* est entendu dans cet article comme couvrant un ou plusieurs sujets qui peuvent se rassembler sous ce terme. Selon les organisations ce périmètre peut varier et intégrer : sûreté, santé, sécurité, sécurité de l'information, gestion de crise, continuité d'activité, etc. Afin de simplifier la lecture du texte, il est noté directeur, sans rajout de la mention H/F.

LA COMPLEXIFICATION DES RISQUES ENTRAÎNE UN BESOIN DE CONFIANCE

Loin de simplement s'additionner, les risques se multiplient par leurs imbrications. Les effets de la Covid-19 l'illustrent parfaitement, et toutes les organisations ont été concernées. Un risque sanitaire pour les collaborateurs pousse à changer les modes de travail, faisant bondir la menace en termes de cybersécurité, de fraudes, des risques psychosociaux, etc. Mais la pandémie accentue aussi les risques sur les chaînes d'approvisionnement, la réputation, la conformité, l'environnement politique et géopolitique. Des problématiques, et donc des expertises, qui étaient souvent considérées séparément se croisent, sont interdépendantes, à l'image d'un monde globalisé, réticulaire.

L'incertitude qu'apporte la complexification des risques entraîne un besoin de confiance de la part des parties-prenantes internes et externes à l'organisation. Les clients, assureurs, régulateurs mais aussi les collaborateurs, les fonctions des risques et de l'audit, demandent des garanties de sécurité et de résilience. Le blanc-seing et la discrétion qui ont parfois entouré la fonction sécurité en France se transforment en exigence de résultat et de transparence. Le directeur sécurité prend ainsi progressivement la dimension stratégique qui lui revient dans un nombre croissant d'organisations.

LE DIRECTEUR SÉCURITÉ, UNE FONCTION EN TRANSITION ENTRE LA POSITION DE « TECHNICIEN » ET CELLE DE « CHEF D'ORCHESTRE »

Les tendances de multiplication des risques et de besoin de confiance amènent le directeur sécurité à sortir progressivement des questions techniques. Car il ne peut pas avoir toutes les clés des questions de cybersécurité, de mesures sanitaires, de protection physique des infrastructures, de continuité d'activité, etc. Il doit suffisamment les comprendre pour les combiner de manière cohérente, donner à chacun une direction, un rythme. Il orchestre une dynamique entre différentes fonctions, sur de multiples sujets, à plusieurs niveaux de son organisation et sur un périmètre géographique souvent international. Ce nouveau positionnement n'est cependant pas une nouveauté, il s'observe à l'international depuis plusieurs années déjà, en particulier chez les anglo-saxons avec la création du rôle de « Chief Security Officer ».

On peut ainsi décliner des compétences qui deviennent nécessaires au directeur sécurité dans cette évolution. Cette liste ne prétend pas être exhaustive mais plutôt souligner celles qui deviennent incontournables. Ces compétences complètent les invariables, tels que la maîtrise du processus de gestion des risques sécurité, la compréhension des aspects juridiques de la fonction, etc.

> **CONSTRUIRE UNE VISION STRATÉGIQUE SPÉCIFIQUE À SON ENTREPRISE :** face à la complexité, le premier défi est de méthodiquement prioriser son action. Cela ne peut se faire qu'avec une connaissance profonde de l'organisation, de son secteur, de ses risques, des centres de décisions formels et informels, de la stratégie de l'entreprise. Le directeur sécurité doit ainsi saisir toutes les complexités de son organisation pour proposer une stratégie de sécurité réaliste, alignée sur les priorités de l'entreprise.

> **MESURER LES AMBITIONS ET RÉSULTATS :** comme toute fonction, les investissements nécessitent d'identifier une cible à atteindre et de mesurer régulièrement les progrès à travers les indicateurs clairs de performance, de risques, de contrôle (les « KPI, KRI, KCI »). Cela amène le directeur sécurité à davantage quantifier et rendre intelligible son action dans l'entreprise.

> **RASSURER, CRÉER UN AVANTAGE COMPÉTITIF :** l'approche méthodique, une connaissance profonde de la conformité, parfois renforcée par des certifications (ISO 31030, 27001, etc.) doit permettre de répondre au besoin de confiance des parties prenantes. Le directeur sécurité a ici l'opportunité de positionner son sujet comme un avantage concurrentiel, qui renforcera la posture business de la fonction.

> **RASSEMBLER ET MOTIVER UNE COMMUNAUTÉ :** face à des risques plus complexes, le périmètre et les interdépendances augmentent. L'équipe au sens large (directe, indirecte, interne, externe) s'élargit et s'enrichit d'experts de multiples disciplines et horizons. Le directeur sécurité identifie, rassemble, coordonne et motive ces ressources afin que leurs actions se complètent pour couvrir les risques de l'organisation. Il s'adapte pour cela à des interlocuteurs qui ont des visions, des langages, des cultures très différents, depuis l'analyste géopolitique, au spécialiste du SOC (« Security Operation Center »), à l'expert en analyse de données, au chef de projet, au responsable de contrôle interne, au directeur des risques, au directeur juridique, etc.

- **INCARNER ET INFLUENCER :** les organisations étant souvent matricielles, la direction de la Sécurité a rarement une autorité verticale très forte. En opposition à cette contrainte organisationnelle, les risques (cyber, sanitaires ou terroristes) nécessitent pourtant la vigilance permanente de chacun des collaborateurs. C'est donc par influence que la direction sécurité doit faire évoluer les comportements individuels à tous les niveaux de l'organisation, depuis les membres d'un comité exécutif, aux managers, aux collaborateurs et jusqu'aux sous-traitants. C'est également par son influence et sa capacité à incarner qu'il pourra défendre ses enjeux vis-à-vis des comités exécutifs, directeurs généraux, directeurs financiers, et donc disposer des ressources dont il a besoin.
- **DISPOSER D'UN SOLIDE « BUSINESS ACUMEN » :** comme toute fonction dans une organisation, le directeur sécurité doit s'adapter à ses objectifs, sa hiérarchie, sa culture, ses processus. Il se doit de parfaitement comprendre les activités, les priorités, les contraintes, les règles formelles et informelles. Il maîtrise les processus transverses de gestion de budget, des ressources humaines, la gestion de projets, la conformité, la performance, etc. Enfin, il maîtrise l'anglais et les outils de bureautique à des niveaux avancés. Sur tous ces aspects, le directeur sécurité ne peut être moins performant que ses pairs dans l'organisation : c'est une condition de sa crédibilité vis-à-vis de ses parties prenantes.
- **RESTER PROCHE DES RÉALITÉS DU TERRAIN :** la complexification tend parfois à développer une approche administrative de la sécurité, à travers des tableaux de bord et des rapports. Bien qu'il s'agisse d'outils indispensables, s'il ne se fie qu'à ceux-là, le directeur sécurité court le risque de se détacher de la réalité. Il est crucial de maintenir un lien régulier, personnel, avec les opérations. Accepter de tester régulièrement et réalistement son organisation permet de mesurer les progrès et déceler les failles potentielles afin d'ajuster son action. Connaître la réalité du terrain permet aussi d'ajuster les mesures à mettre en place, pour répondre aux besoins des opérations.

LA MONTÉE EN COMPÉTENCES PASSE PAR DAVANTAGE DE COLLECTIF

En France, la fonction de directeur sécurité a évolué lentement au cours de dernières années et manque encore de structure. Aujourd'hui, sous l'effet de la complexification des risques et du besoin de transparence qui en résulte pour les organisations, la pression s'accentue et se répercute désormais sur l'ensemble du tissu économique français, notamment sous l'effet de la menace de cybersécurité, de la Covid-19, du conflit Ukrainien. Cela permet à la fonction de directeur sécurité de poursuivre sa reconnaissance dans les organisations et donc sa normalisation et sa professionnalisation.

Pour continuer - voire accélérer - le développement de la fonction et la montée en compétences qui l'accompagne, le directeur sécurité doit pouvoir disposer de filières de formations, de référentiels organisationnels ou techniques, de bonnes pratiques, de partages d'expériences, de filières de recrutement, etc.

À titre de comparaison, on a pu observer plusieurs modèles qui ont permis cette évolution à l'international. On peut citer aux États-Unis la centralité de l'ASIS (American Society for Industrial Security) qui a permis de structurer ce secteur et qui est même devenue une référence internationale. Un autre exemple a été la règlementation de la fonction de directeur de sécurité en Espagne, à travers la loi de sécurité privée de 2014, qui donne un cadre à ses missions, formations et compétences.

S'inspirant de ces exemples, la première étape indispensable est donc de renforcer les associations professionnelles et leur alignement (CDSE, ASIS France, CESIN, Clusif, etc.). Cela permettra d'avoir les débats nécessaires entre professionnels de la sécurité, soit pour proactivement définir un cadre commun, soit pour étroitement collaborer avec l'État afin de règlementer la fonction.

Le temps presse, car les récents événements en Ukraine montrent que les changements s'accélèrent. Il appartient alors aux professionnels d'être au rendez-vous avec ces évolutions et de proposer des solutions qui permettent de protéger au mieux nos organisations. À défaut, le risque est de se voir appliquer par l'État un cadre qui ne corresponde pas au besoin. ■

RECOM > MANDATIONS

> DÉPASSER LE POSITIONNEMENT DE PUR TECHNICIEN

Pour répondre au besoin de son organisation, le directeur sécurité doit appréhender le contexte général de celle-ci et participer à la réalisation de la stratégie de son entreprise. Les aspects techniques ne disparaissent pas, mais sont subordonnés aux objectifs « business » à atteindre.

Cela peut signifier, par exemple : encourager le partage de connaissances à tous les niveaux de l'organisation entre la fonction sécurité et les fonctions stratégie, finance, juridique, etc. afin de développer des liens plus étroits entre les parties prenantes.

> EMBRASSER LA COMPLEXITÉ ET APPORTER DE LA CLARTÉ

Les organisations, la société, les risques sont mouvants. Dans cette complexité, une plus-value du directeur sécurité est justement de pouvoir identifier des priorités et donner de la transparence aux décideurs et parties prenantes sur le niveau réel des risques et les actions à prendre.

Cela peut signifier, par exemple : partager régulièrement son tableau de bord à destination des membres d'un comité de direction en y intégrant des scenarios concrets illustrés par des exemples d'actualité.

> DÉVELOPPER LA CENTRALITÉ DES ASSOCIATIONS DE PROFESSIONNELS

Le directeur sécurité en France renforcera sa propre légitimité et son approche si celles-ci sont adossées à des associations professionnelles solides et crédibles.

Cela peut signifier, par exemple : adhérer et participer activement à plusieurs associations professionnelles afin de créer du lien entre leurs différentes initiatives pour assurer une action collective cohérente.

18

RECOM > MANDATIONS STRUCTURANTES

18 RECOMMANDATIONS STRUCTURANTES

POUR UNE FONCTION SÉCURITÉ-SÛRETÉ STRATÉGIQUE
DANS L'ENTREPRISE & PLEINEMENT INTÉGRÉE
AU CONTINUUM DE SECURITÉ

POUR UNE FONCTION SÉCURITÉ-SÛRETÉ STRATÉGIQUE & TRANSVERSALE AU SERVICE DU BUSINESS

1. INTÉGRER LA DIRECTION SÉCURITÉ-SÛRETÉ CORPORATE À LA GOUVERNANCE DE L'ENTREPRISE

Par un rattachement à la direction générale et/ou à un membre du comité exécutif.

Pour > Les dirigeants d'entreprise

2. DÉVELOPPER UNE POLITIQUE DE SÉCURITÉ GLOBALE & ÉTHIQUE

En adressant l'ensemble des domaines de la sécurité-sûreté : sécurité des personnes et des biens matériels et immatériels, cyber, intelligence stratégique et sécurité économique, supply chain, fraude et compliance, international, gestion de criseset résilience opérationnelle, radicalités.

Pour > Les directeurs sécurité-sûreté

3. SE FAIRE CONNAÎTRE & RECONNAÎTRE AU SEIN DE L'ENTREPRISE

Le directeur sécurité-sûreté doit se mettre au service de tous les départements de l'entreprise et apporter une plus-value concrète.

Pour > Les directeurs sécurité-sûreté

4. S'EMPARER DU SUJET INTERNATIONAL POUR L'INTÉGRER AUX BESOINS & À LA STRATÉGIE DE L'ENTREPRISE

Acteur transversal, le directeur sécurité-sûreté bénéficie d'une vision à 360 degrés pour mieux dérisquer à l'international sur le long terme.

Pour > Les directeurs sécurité-sûreté > Les dirigeants d'entreprise

5. CONFIER À LA DIRECTION SÉCURITÉ-SÛRETÉ UN RÔLE MAJEUR DANS L'ANIMATION DES DISPOSITIFS DE CRISE & DE CONTINUITÉ D'ACTIVITÉ

La fonction sécurité-sûreté dispose dans son ADN de capacités d'anticipation, de réactivité, de transversalité et d'organisation indispensables à la gestion de crise et à la continuité d'activité.

Pour > Les dirigeants d'entreprise

6. SENSIBILISER LES FUTURS DIRIGEANTS D'ENTREPRISE AUX RÔLES & FONCTIONS DE LA SÉCURITÉ-SÛRETÉ

En développant une stratégie éducative à destination des grandes écoles (ENA, Sciences PO, grandes écoles de management et de commerce…)

Pour > Les directeurs sécurité-sûreté > Les dirigeants d'entreprise > Le CDSE et les acteurs de la profession

7. RENFORCER LA PROFESSIONNALISATION DE LA FILIÈRE MÉTIERS SÉCURITÉ-SÛRETÉ CORPORATE

Par des cursus de formation dédiés et des parcours de carrière intégrant des mobilités externes à la filière dans l'entreprise et avec les institutions.

Pour > Les directeurs sécurité-sûreté > Le CDSE et les acteurs de la profession

POUR UN DIRECTEUR SÉCURITÉ-SÛRETÉ INTÉGRÉ DANS UN CONTINUUM DE SÉCURITÉ EFFECTIF & PRAGMATIQUE

8. CRÉER UN « CERCLE DE CONFIANCE » PUBLIC-PRIVÉ BÂTI SUR LE SECRET PROFESSIONNEL OU UN PROCESSUS D'HABILITATION FAVORISANT LE PARTAGE D'INFORMATIONS

En instituant les directeurs sécurité-sûreté comme acteurs incontournables du *continuum* de sécurité et interlocuteurs privilégiés des forces régaliennes et de l'État dans l'Entreprise.

Pour > Les pouvoirs publics

9. INTÉGRER DES MODULES DÉDIÉS À LA SÉCURITÉ-SÛRETÉ EN ENTREPRISE DANS LES FORMATIONS DES CADRES DE LA POLICE & DE LA GENDARMERIE NATIONALES

Pour > Les pouvoirs publics > Le CDSE et les acteurs de la profession

10. DÉVELOPPER LES ÉCHANGES ENTRE LES DIRECTEURS SÉCURITÉ-SÛRETÉ, LE CNAPS[1] & LA DPSIS[2]

Notamment dans le cadre de la mission de conseil de l'établissement public de régulation des activités privées de sécurité, ainsi que pour une relation plus directe entre les directeurs sécurité/donneurs d'ordre et le ministère de l'Intérieur.

Pour > Les pouvoirs publics

11. SUIVRE LES RECOMMANDATIONS DU CAHIER TECHNIQUE DU CDSE « LA PRESTATION DE GARDIENNAGE : LE GUIDE DU DONNEUR D'ORDRE » DANS L'ACHAT DE PRESTATION DE SÉCURITÉ PRIVÉE

Définir le positionnement de la surveillance humaine dans la stratégie de sécurité globale de l'entreprise, confier le pilotage du processus d'appel d'offres au binôme des fonctions « Achats » et « Sécurité-Sûreté », privilégier le « mieux-disant » plutôt que le « moins-disant ».

Pour > Les directeurs sécurité-sûreté > Les dirigeants d'entreprise

18 RECOM > MANDATIONS STRUCTURANTES

12. RÉFORMER LA FORMATION PROFESSIONNELLE EN SÉCURITÉ PRIVÉE

Pour revaloriser les compétences des agents, faire émerger un véritable métier d'encadrant en sécurité privée, améliorer la qualité de l'offre et des prestations.

Pour > Les pouvoirs publics

13. INSTAURER UN MÉCANISME DE TYPE GARANTIE FINANCIÈRE POUR LES ENTREPRISES DE SÉCURITÉ PRIVÉE

Pour s'assurer des capacités financières des entreprises de sécurité privée et de la volonté de leurs dirigeants de s'inscrire durablement et de manière responsable dans ce marché.

Pour > Les pouvoirs publics

14. RENFORCER L'ACTION DE L'ÉTAT DANS LA LUTTE ANTI-CONTREFAÇON

En mettant en œuvre les recommandations du rapport Blanchet-Bournazel sur l'évaluation de la lutte contre la contrefaçon[3].

Pour > Les pouvoirs publics

[1] CNAPS : Conseil national des activités privées de sécurité

[2] DPSIS : Délégation ministérielle aux partenariats, aux stratégies et aux innovations de sécurité

[3] Rapport d'information du Comité d'évaluation et des contrôles des politiques publiques de l'Assemblée nationale présenté par les députés Christophe Blanchet et Pierre-Yves Bournazel en octobre 2020

POUR UNE CYBERSÉCURITÉ & DES TECHNOLOGIES DE SÉCURITÉ MAÎTRISÉES

15. ADOPTER UNE DÉMARCHE SYSTÉMIQUE QUANT AU POSITIONNEMENT STRATÉGIQUE DE LA SSI DANS L'ENTREPRISE

Prétendre définir une organisation type, où la sécurité des systèmes d'information (SSI) de l'entreprise doit être sous la responsabilité du directeur sécurité-sûreté ou pas, est illusoire. À chaque entreprise son organisation selon son secteur d'activité, son histoire et sa culture.

Pour > Les directeurs sécurité-sûreté > Les dirigeants d'entreprise

16. INTÉGRER & PROMOUVOIR LES CRITÈRES DE SOUVERAINETÉ DANS LE CHOIX DES SOLUTIONS NUMÉRIQUES

Choisir de se tourner vers des solutions numériques souveraines revient à limiter le risque d'ingérence numérique malveillante et à mieux protéger ses données.

Pour > Les directeurs sécurité-sûreté

17. INTÉGRER LA SSI DÈS LA CONCEPTION OU LA MISE EN PLACE DE NOUVELLES TECHNOLOGIES DE SÛRETÉ

L'aide des experts SSI est essentielle afin de garantir dès l'installation de nouveaux outils de sûreté une architecture réseau sûre.

Pour > Les directeurs sécurité-sûreté

18. DOTER LES TECHNOLOGIES DE SÉCURITÉ D'UN CADRE JURIDIQUE

Sous le contrôle strict de la CNIL afin de garantir la protection des libertés publiques et individuelles.

Pour > Les pouvoirs publics

CDSE
CLUB DES **DIRECTEURS**
DE **SÉCURITÉ**
DES ENTREPRISES

6 place d'Estienne d'Orves
75009 Paris
01 72 31 73 18
contact@cdse.fr

cdse.fr