



Contrefaçon, kidnapping, cybercriminalité, espionnage industriel : les entreprises qui se développent à l'international peuvent être exposées à de multiples risques criminels. Lors d'une Masterclass animée par Jean-Christophe Gessler, vice-président de La Fabrique de l'Exportation, Philippe Very, professeur de stratégie et chercheur à la chaire Management des risques criminels de l'Edhec, détaille comment s'en protéger.

Philippe Very décrypte les risques criminels à l'international et leur management

JCG : Quels sont les objectifs de la chaire Management des risques criminels de l'Edhec ?

PV : Les activités légales et illégales constituent deux mondes différents mais liés. Il existe aujourd'hui une incursion très forte d'organisations criminelles dans l'économie légale, et l'objectif de la chaire est de comprendre les risques qu'elles posent aux entreprises, puis de trouver des solutions pour les prévenir et les gérer, des solutions qui dépendent bien sûr des types d'acteurs criminels concernés.

La chaire est financée par des entreprises comme Sanofi ou Rio Tinto. Notre recherche se fonde sur des études de cas de terrain, intégrant parfois des rencontres avec les auteurs d'actes illicites, autour de missions variées : problèmes de contrefaçon, ouverture de sites dans des régions où sévissent des guérillas, signature de partenariats dans des pays où les mafias contrôlent une partie de l'économie légale. Nous travaillons aussi avec des associations de directeurs de sécurité d'entreprise, l'Isma et le CDSE, ainsi qu'avec Europol. Ces études de cas nourrissent ensuite nos cours, nos conférences, nos articles académiques et différents médias.

JCG : Comment peut-on classer les différents types d'acteurs et de risques que font courir aux entreprises les organisations criminelles ?

PV : Notre typologie, issue de dix années de recherche, distingue deux grandes familles. La première regroupe des acteurs aux objectifs d'abord idéologiques, organisations terroristes et guérillas, qui attaquent des entreprises perçues comme des symboles de ce contre quoi elles luttent, capitalisme, États-Unis. Ces attaques peuvent prendre la forme d'attentats, de destructions d'installations, de kidnappings ou d'assassinats, destinés à braquer les caméras sur leur cause : c'est le cas des prises d'otages d'AQMI au Sahara ou au Mali, les terroristes se filmant avec leurs otages pour délivrer leur message. Une entreprise peut aussi être victime collatérale d'un attentat, comme Saudia Airlines, dont un équipage a péri lors de l'attaque du Marriott Hotel à Islamabad par l'organisation Fedayeen-e-Islam en 2008. Ces groupes idéologiques ont aussi besoin de se financer, et développent pour cela des actions de prédation, extorsion, kidnapping avec demande de rançon, ou contrefaçon, le Hezbollah ayant par exemple été un spécialiste avéré du CD de contrefaçon, une activité gérée depuis le Paraguay.

JCG : Quel est le deuxième grand type d'acteurs criminels ?

PV : Il regroupe des organisations qui poursuivent un objectif économique plutôt qu'idéologique, le plus souvent des groupes criminels issus de trafics illicites qui s'intègrent de plus en plus dans l'économie légale. On y trouve d'abord des organisations sophistiquées comme les mafias italienne, japonaise, albanaise, turque ou américaine : en Italie, le revenu des mafias est estimé à 7 % du PIB. On y trouve aussi des organisations transnationales issues des trafics illicites, comme les cartels de la drogue mexicains, des gangs internationaux sophistiqués comme les Pink Panthers, issus de l'ex-Yougoslavie et spécialisés dans le vol de bijoux, des guérillas criminalisées passées d'un objectif idéologique à un objectif économique, ou encore des gangs comme les Hells Angels au Canada.

Toutes ces organisations cherchent à s'enrichir en prélevant des ressources aux entreprises : extorsion, comme le pizzo que fait payer la Camorra à Naples ou l'embauche forcée de travailleurs fantômes, vol d'équipements ou de produits, piraterie routière ou maritime, kidnapping d'employés avec demande de rançon, particulièrement difficile à gérer, ou encore fraude et vol de propriété intellectuelle, de données ou de savoir-faire.

JCG : Quelles sont les autres techniques utilisées par ces groupes criminels ?

PV : Au-delà de la prédation, les entreprises peuvent aussi être victimes de parasitisme : plutôt que de développer leur propre logistique, les organisations criminelles s'appuient sur celle de l'entreprise pour organiser leurs trafics, en utilisant par exemple ses camions pour transporter de la drogue, ou les circuits de certains organismes financiers pour blanchir de l'argent sale. Walmart, en 2012, et HSBC, en 2016, ont ainsi été accusés d'avoir blanchi l'argent de cartels mexicains.

Une entreprise qui s'internationalise peut aussi se retrouver face à des sociétés ayant pignon sur rue, mais dont la conception de la compétition sort du cadre légal. Les mafias sont très présentes dans la contrefaçon, un délit bien moins sévèrement puni que le trafic de drogue, et vont parfois jusqu'à contrôler des entreprises entières, notamment les mafias italiennes, voire des marchés entiers, comme ceux de l'agribusiness ou des déchets en Italie, des déchets au Japon avec les Yakuzas, ou du ciment à New York.

Au-delà de ces acteurs criminels organisés, les entreprises exportatrices restent aussi exposées à des risques plus diffus mais tout aussi coûteux : la fraude, qu'il s'agisse de détournements de fonds, de corruption ou de fausses factures ; la cybercriminalité, attaques informatiques, vol de données stratégiques, ransomwares, espionnage numérique, une menace en croissance constante ; et l'espionnage industriel, lorsque certains États ou entreprises concurrentes cherchent à obtenir illégalement des informations sensibles.

Comment s'en protéger : le triptyque détection, prévention, réponse

Les solutions de protection contre les risques criminels s'organisent généralement autour de trois phases : comprendre ce qui pourrait arriver, voir comment s'en prévenir, puis se préparer à répondre aux problèmes qui pourraient se poser, sachant que la réponse implique le plus souvent de revoir les mesures de prévention.

La détection repose avant tout sur l'information, à rechercher auprès des autorités locales et françaises, des chambres de commerce, des ONG, des réseaux de responsables de sécurité d'entreprise, CDSE ou Isma, ou d'entreprises internationales déjà présentes dans le pays visé : il ne faut pas hésiter à ratisser large et à mobiliser ses réseaux. Faire appel à des experts en intelligence économique et en gestion des risques permet aussi d'affiner cette analyse. Des cabinets de conseil spécialisés peuvent mener des investigations sur les risques, les lois et la justice locale, en particulier avant de signer un contrat, et un audit ou une due diligence peut être réalisé avant de choisir un partenaire local pour créer une alliance.

Une partie du risque peut être transférée aux assureurs, dégâts matériels, kidnappings et rançons, décès et blessures, incarcérations illicites, pertes d'exploitation, divulgations d'informations, ou aux autorités locales, comme le parquet anti-mafia en Italie. Mais cela ne suffit pas : il faut aussi développer des solutions internes de formation des employés aux bonnes pratiques de sécurité physique et numérique, d'entraînement à la gestion de crise, et de protection des actifs stratégiques, brevets, R&D, données sensibles, propriété intellectuelle, tout en ajustant son business plan en fonction des moyens, des coûts et des ressources nécessaires selon les acteurs criminels identifiés.

La formation des employés devient essentielle lorsqu'une entreprise se déploie dans une zone à risque : préparer les expatriés, mettre en place des procédures de sécurité, expliquer par exemple qu'ils ne pourront pas se rendre seuls à l'épicerie du coin et devront rester dans le compound, qu'ils doivent utiliser tel véhicule plutôt qu'un autre

lors de leurs déplacements, ou systématiquement demander le numéro de la voiture et le nom du chauffeur. Sur le plan numérique, la mise en place de protocoles de cybersécurité stricts devient tout aussi indispensable face à la montée des attaques informatiques et du vol de données.

L'entraînement à la gestion de crise est tout aussi important : de plus en plus de groupes internationaux réalisent chaque année des exercices de simulation sur différents scénarios, prise de contrôle d'une installation ou du système d'information, kidnapping d'employés, plutôt que d'attendre d'être confrontés à un vrai problème pour s'y préparer.

Le développement de dispositifs de protection peut aussi passer par le choix du mode d'entrée dans le pays : en cas de risques criminels graves, l'entreprise évitera d'envoyer des expatriés, ou en limitera le nombre, et pourra privilégier une forme d'investissement sans partenaire plutôt que de se lier à un allié non fiable. Choisir avec soin ses partenaires et ses fournisseurs, sécuriser ses actifs stratégiques, souscrire des assurances adaptées, risques politiques, enlèvements et rançons, pertes d'exploitation, ainsi que le management des contrats avec les partenaires et les politiques de RSE, d'éthique et de compliance, complètent ce dispositif de protection.

Quand un problème important survient, il s'agit de mettre en place un véritable management de crise, avec un plan prêt à être déployé : identifier en amont les personnes responsables de la gestion de crise, mener les investigations nécessaires, communiquer de manière efficace en interne comme en externe, coopérer avec les autorités locales et internationales, engager le cas échéant des actions en justice, puis réajuster ses stratégies de protection après chaque incident pour éviter toute récurrence. Les solutions dépendent bien sûr largement des acteurs criminels rencontrés et des techniques qu'ils emploient.

Les entreprises qui se développent à l'international ont donc tout intérêt à intégrer la gestion des risques criminels dans leur stratégie globale : une vigilance accrue, une approche préventive et une capacité de réaction rapide sont essentielles pour garantir leur sécurité et leur pérennité.