

Face à la complexité du monde, adoptons l'intelligence du risque et de la menace



Julien LOPIZZO
*Président Directeur Général
Semkel*

Pandémie mondiale, tensions géopolitiques accrues, crises énergétiques et climatiques à répétition, cyberattaques massives et désinformation généralisée : les entreprises et institutions évoluent aujourd'hui dans un contexte de crises multiples, parfois interdépendantes et d'une intensité rarement observée auparavant.

Dans ce contexte crisogène inédit, aucune organisation ne peut plus se permettre de subir passivement les événements : l'anticipation doit devenir une composante centrale et proactive de toute stratégie durable. Pour ce faire, il ne s'agit plus seulement d'évaluer la probabilité d'un risque, mais de prévenir et d'agir très rapidement dès l'apparition des premières menaces en adoptant ce qu'il est convenu d'appeler une intelligence du risque et de la menace. Car, pour les entreprises, passer de la vigilance à la pro-action, c'est non seulement rendre résiliente leur stratégie, mais aussi renforcer leur agilité, optimiser leurs décisions, protéger leur réputation et saisir plus

rapidement de nouvelles opportunités.

Cette intelligence du risque et de la menace peut notamment se fonder sur trois piliers.

Premier levier : les signaux faibles

Nous savons aujourd'hui que si un homme tousse à l'autre bout du monde, cela peut impacter nos vies et nos entreprises. C'est dire tout l'enjeu qu'il y a à mieux détecter les signaux faibles qui annoncent des évolutions ou des ruptures majeures. Comment ? En cartographiant méthodiquement ses propres dépendances et en installant une veille proactive de son écosystème. Vous êtes tributaire des micropuces de Taïwan ? Mettre une surveillance sur la météo de la zone indopacifique paraît judicieux pour anticiper, comme à l'été 2021, une intense sécheresse qui ralentit la production ; vous pourrez ainsi changer vos propres plans de production ou vos fournisseurs le temps que la crise soit passée.

Détecter les signaux faibles permet ainsi d'être en avance de phase et d'élaborer des réponses adaptées avant même que la menace ne prenne forme.

Deuxième levier : la préparation

Anticiper implique d'être en permanence prêt à parer toute crise. Cela suppose une véritable "culture de crise" intégrée à tous les niveaux de l'organisation. Si, malgré une bonne cybersécurité ou une surveillance de votre écosystème numérique (pour contrer le risque systémique lié à la compromission de votre supply chain), vous étiez touché par une cyberattaque (ransomware, exfiltration de données...) comme c'est arrivé

récemment à Harvest, Mark & Spencer ou Disneyland Paris, alors vous devez vous poser la bonne question : où était la faille ? Plans de continuité d'activité régulièrement actualisés, entraînements périodiques des équipes, dispositifs d'alerte et processus de prise de décision clairement définis, notamment, doivent ainsi être des réflexes. La préparation devient ainsi une capacité stratégique à part entière, permettant aux entreprises de réagir instantanément et efficacement dès les signes avant-coureurs d'une crise.

Troisième levier : la contextualisation

Pour agir efficacement, il ne suffit pas de détecter les signaux faibles, il faut également être en mesure de les replacer dans leur contexte global. Comprendre les dynamiques économiques, sociales, géopolitiques ou technologiques à l'œuvre permet justement d'interpréter correctement la portée réelle d'une menace naissante. Même s'il est parfois difficile de distinguer une simple posture politique d'une menace réelle, le programme du président Trump indiquait dès le départ son intention d'utiliser la hausse des droits de douane comme levier de négociation. Surtout qu'en l'occurrence, le premier mandat du président Trump avait permis de confirmer qu'une telle menace pouvait être mise à exécution... Un tel travail de mise en contexte mobilise une expertise transversale, une connaissance fine de l'environnement dans lequel évolue l'organisation et une capacité à croiser différents domaines de compétence pour obtenir une vision globale des risques émergents.

Ne nous y trompons pas, cette intelligence du risque et de la menace constitue, pour les organisations, un changement radical dans leurs méthodes traditionnelles de gestion des risques et de prise de décision. Elle suppose d'abord d'être équipé pour collecter, trier et analyser en temps réel des flux d'informations complexes et multidimensionnels. Elle requiert aussi la capacité de connecter les

points, c'est-à-dire de comprendre comment des événements apparemment disparates peuvent s'aggraver en crises majeures. Le renseignement économique, la cybersurveillance, l'analyse géopolitique et la veille réputationnelle et informationnelle deviennent, dans ces circonstances, des éléments fondamentaux. Autant de compétences qui ne peuvent plus être pensées isolément : leur efficacité dépend désormais de leur capacité à s'intégrer au sein d'une démarche globale, où ces disciplines dialoguent constamment entre elles, facilitant une compréhension systémique et multidimensionnelle des risques émergents. Ce décloisonnement stratégique s'accompagne d'un changement organisationnel : les entreprises devront soit transformer leur direction du risque actuelle en une véritable direction de l'intelligence du risque et de la menace, soit la créer ex nihilo. Cette nouvelle direction stratégique devra porter, diffuser et ancrer cette doctrine stratégique que ce soit auprès de la direction qu'au sein de chaque branche opérationnelle, facilitant ainsi la prise de conscience collective des enjeux globaux auxquels l'entreprise est confrontée. Une nouvelle organisation qui conciliera vision stratégique, rationalité opérationnelle et mission fondamentale de l'organisation, en intégrant pleinement sa capacité d'anticipation.

Il ne s'agit là rien de moins que d'une véritable révolution culturelle et organisationnelle. Mais elle s'impose aujourd'hui à tous les acteurs, tant une anticipation systémique et décloisonnée est aujourd'hui indispensable pour ne plus subir la complexité et l'incertitude. Loin de constituer une contrainte pour l'organisation, elle en devient, au contraire, un véritable levier stratégique.