ECONOMIST IMPACT

Réinitialisation des risques : passer de la réaction à l'anticipation

Sponsorisé par

IRON MOUNTAIN®

Table des matières

À propos de la recherche et remerciements

Réinitialisation des risques : le passage de la réaction à l'anticipation est un programme de recherche mené par l'Economist Impact et sponsorisé par Iron Mountain. Il examine les principaux facteurs internes et externes qui déterminent l'approche d'une entreprise en matière de risques et le rôle que les dirigeants, les technologies et l'organisation institutionnelle jouent dans leur gestion. L'Economist Impact s'est basé sur des données issues d'entretiens avec des experts et sur une enquête personnalisée menée auprès de 656 dirigeants exerçant dans des secteurs d'activité clés en Australie, au Brésil, au Canada, en France, en Allemagne, à Hong Kong, en Inde, au Mexique, en Nouvelle-Zélande, à Singapour, au Royaume-Uni et aux États-Unis.

Nous tenons à remercier les experts suivants pour le temps qu'ils nous ont consacré et les informations qu'ils nous ont fournies :

- Simeon Fishman, vice-président exécutif et directeur des risques chez The Clearing House
- Sophie Heading, responsable des risques mondiaux au Forum économique mondial
- Le Dr Witold J. Henisz, vice-doyen et directeur de faculté de l'initiative Environnement, Social et Gouvernance de la Wharton School

Ce document d'information a été produit par une équipe de chercheurs, de rédacteurs et de concepteurs de l'Economist Impact, notamment :

- Monica Ballesteros - directrice de projet
- Durukhshan Esmati - chef de projet
- Kathleen Harrington - analyste
- Alasdair Ross - rédacteur
- Amanda Simms - rédactrice en chef
- Designer - EMC Design Ltd

L'Economist Impact est le seul responsable du contenu de ce rapport.
Les conclusions et les points de vue exprimés dans ce rapport ne reflètent pas nécessairement ceux de notre sponsor, de nos partenaires ou des experts ayant participé aux entretiens.

Avant-propos d'Iron Mountain

Au cours des trois dernières années, de nombreuses entreprises ont subi d'importantes transformations en réponse aux menaces émergentes et aux perturbateurs mondiaux. Cette évolution nous a tous obligés à devenir plus résilients, en abandonnant les mesures réactives au profit d'une anticipation proactive. En renforçant leur résilience face aux menaces potentielles futures au lieu de se contenter de répondre aux menaces habituelles, les entreprises sont en mesure de s'adapter aux risques imprévus et de saisir les opportunités émergentes.

Depuis plus de 70 ans, Iron Mountain permet à ses clients du monde entier d'atténuer les risques qui pèsent sur leur marque, leur réputation et leur situation financière tout en leur donnant les moyens de servir efficacement leurs clients, leurs patients ou leurs concitoyens. C'est pourquoi nous avons le plaisir de parrainer la dernière étude d'Economist Impact, qui se penche sur l'évolution des perceptions de la gestion des risques organisationnels.

Comme vous le découvrirez dans ce rapport, plus de 90 % des entreprises mettent davantage l'accent sur la gestion des risques en raison des récentes perturbations mondiales et économiques. En ce qui concerne les risques émergents, le rapport souligne les inquiétudes persistantes en matière de cybersécurité. La prolifération des technologies émergentes, avec l'intelligence artificielle générative, par exemple, qui crée de nouveaux risques et accroît la capacité des gestionnaires de risques à détecter ces menaces en même temps, constitue une autre inquiétude. Si la protection des actifs physiques reste cruciale pour notre entreprise, nous reconnaissons que tout le monde est désormais plus vulnérable aux cybermenaces, et nous avons évolué avec le marché pour protéger les données des clients dans un espace numérique.

Les conclusions du rapport montrent également que les dirigeants accordent plus d'attention aux risques environnementaux qu'ils ne l'ont fait par le passé. En ce qui concerne le développement durable, notre objectif d'atteindre la carboneutralité se concentre sur la réduction de la consommation d'énergie, l'électrification de nos systèmes et de nos véhicules, l'installation de systèmes d'énergie renouvelable et l'approvisionnement en énergie verte afin de réduire l'exposition à l'augmentation des prix des combustibles fossiles et aux réglementations locales en matière d'émissions. En poursuivant nos propres objectifs environnementaux, sociaux et de gouvernance et en aidant nos clients à atteindre les leurs, nous ne nous contentons pas d'atténuer les risques liés à l'évolution des réglementations, au changement climatique et aux inégalités sociales, mais nous ouvrons également la porte à de nouvelles perspectives.

Nous sommes encouragés par les résultats de l'enquête qui montrent que les cadres gèrent les risques et renforcent la résilience de manière plus proactive. Cela est au cœur de notre mission. Les données présentées dans ce rapport nous permettent d'examiner de plus près la manière dont nous pouvons mieux nous préparer, et mieux préparer nos clients, à l'avenir.

Larry Jarvis
Vice-président senior, Directeur de la sécurité des informations
Iron Mountain

Résumé

La gestion des risques est de plus en plus intégrée dans la structure organisationnelle de l'entreprise et est représentée à des niveaux plus élevés. Les responsables risques rassemblent des données sur les menaces potentielles et coordonnent la réponse de l'entreprise. Mais comme ces menaces évoluent à un rythme effréné, il est essentiel que la discipline s'oriente vers l'anticipation des risques qui ne sont pas encore détectés par l'entreprise plutôt que de se contenter de répondre aux incidents au fur et à mesure qu'ils surviennent.

Economist Impact, sponsorisé par Iron Mountain, a mené une étude primaire pour comprendre comment les dirigeants perçoivent les principaux facteurs internes et externes qui déterminent l'approche d'une entreprise en matière de risques et le rôle que les dirigeants, les technologies et l'organisation institutionnelle jouent dans la gestion des risques. Economist Impact s'est appuyé sur les données issues d'entretiens avec des experts et sur une enquête personnalisée menée auprès de 656 dirigeants exerçant dans des secteurs d'activité clés (services financiers, santé et sciences de la vie, énergie et secteur public) en Australie, au Brésil, au Canada, en France, en Allemagne, à Hong Kong, en Inde, au Mexique, en Nouvelle-Zélande, à Singapour, au Royaume-Uni et aux États-Unis.

Les responsables des risques s'efforcent de mieux comprendre la façon dont les risques se répercutent sur l'entreprise, par exemple, comment un arrêt de production ou une faille de sécurité chez un fournisseur clé pourrait affecter ses opérations, son chiffre d'affaires et sa réputation. La prise de conscience des risques contingents est en hausse, mais des progrès restent à faire.

La gestion globale et préventive des risques, qui répond aux menaces émergentes, doit être menée par direction de l'entreprise, avec une réponse aux risques systématiquement coordonnée, adoptée et "maîtrisée « par tous les membres du personnel. Au-delà de l'entreprise, la sensibilisation aux risques doit être intégrée dans la culture, des partenaires, fournisseurs et des distributeurs.

Les technologies numériques émergentes telles que l'apprentissage automatique et l'intelligence artificielle (IA) promettent d'élargir la boîte à outils du responsable des risques, en identifiant des schémas dans les données que les analystes en chair et en os pourraient manquer. Cependant, les pirates ont également accès à ces technologies et pourraient les utiliser pour trouver des failles ou lancer des attaques de type hameçonnage plus efficaces. Ces technologies naissantes doivent faire l'objet d'un suivi attentif à mesure que leurs véritables implications deviennent plus claires.

Nous examinons quatre domaines dans lesquels l'évolution des pratiques transforme le paysage de la gestion des risques :

L'évolution du lieu de travail : le personnel d'une entreprise est à la fois son plus grand atout et sa plus grande faiblesse, ce qui se reflète dans les efforts et les ressources que les entreprises consacrent au recrutement, à la rétention et à la formation des travailleurs. La numérisation a rapproché le personnel des processus critiques, augmentant les risques et accélérant le rythme auquel ils se manifestent. Parallèlement, le passage au télétravail a rendu les frontières numériques de l'entreprise plus poreuses. Attirer et conserver le personnel devient également plus difficile, car une génération adopte une approche du travail plus axée sur les valeurs. Notre enquête suggère que les responsables des risques se tiennent au courant de ces nouvelles tendances : 96 % des personnes interrogées indiquent que leur entreprise a développé de nouvelles politiques et procédures de gestion de la main-d'œuvre, y compris le travail hybride, par exemple.

La cybersécurité et la gouvernance des données : l'informatique numérique n'a pas seulement été à l'origine d'une nouvelle vague de gains de productivité, mais a également créé de nouvelles sources de risque. L'information circule plus rapidement et plus largement que jamais et, surtout, plus rapidement que la faculté de réaction de l'homme. Les LLes risques éventuels augmentant également du fait de l'émergence d"entreprise géantes, décentralisées et multinationales, la protection de la présence numérique d'une entité contre les dommages accidentels ou malveillants est devenue une question de survie. Le lancement de modèles d'IA générative ouverts a fait apparaître soudainement un risque longtemps attendu dans la salle de réunion, mais les impacts de cette technologie naissante restent difficiles à prévoir. Les responsables peuvent répondre au mieux à cet environnement changeant en se concentrant sans relâche sur trois domaines majeurs de risques liés aux données : la gouvernance, la sécurité et la confidentialité.

La durabilité environnementale : le changement climatique menace notre avenir, et ses effets se font déjà ressentir. Les phénomènes météorologiques extrêmes sont de plus en plus intenses et fréquents, tandis que la biodiversité est de plus en plus menacée. Le commerce et les infrastructures subissent également des conséquences catastrophiques et, à ce titre, les entreprises s'efforcent de maintenir des chaînes d'approvisionnement diversifiées et flexibles. Tandis qu'elles se concentrent sur la résilience, les

parties prenantes font également pression sur elles pour qu'elles contribuent à résoudre les problèmes sous-jacents : l'épuisement des ressources, la dégradation de l'environnement et les émissions dangereuses. L'absence d'action sur ces questions pourrait avoir de graves répercussions. La grande majorité des personnes interrogées dans le cadre de notre enquête le reconnaissent, 80 % d'entre elles soulignant l'importance des indicateurs de risque de réputation.

L'efficacité opérationnelle : alors que les entreprises font face à une vague croissante de risques émergeant hors de leurs enceintes, les responsables des risques doivent continuer à se concentrer sur les menaces internes, que leur source en soit les personnes, les processus ou les exigences réglementaires. Les entreprises sont tombées dans le piège de percevoir la fonction de gestion des risques comme un centre de coûts qui fait obstacle à la réalisation de bénéfices. Les gestionnaires de risques sont devenus plus aptes à fournir à la direction des indicateurs qui permettent d'équilibrer les coûts du maintien de pratiques saines en matière de risques et les pertes potentielles résultant d'une négligence. La façon dont le risque opérationnel se manifeste varie considérablement en fonction des entreprises et des secteurs, mais notre enquête suggère que les responsables des risques reconnaissent systématiquement l'importance de l'investissement dans ce domaine.

Si la gestion des risques évolue en fonction du paysage changeant des menaces, elle reste confrontée à des défis considérables. Parmi ces derniers, on peut citer :

L'évaluation : si les coûts du déploiement d'un système de gestion des risques sont clairs, il n'en va pas de même pour la mesure de ses avantages. Une partie du rôle de la fonction consiste à veiller à ce que les menaces potentielles ne se concrétisent pas, mais l'évaluation du coût de quelque chose qui ne s'est pas encore produit est problématique. Et si l'investissement est immédiat, les bénéfices peuvent s'accumuler au fil des ans, ce qui ajoute au défi de la mesure. L'essentiel est de mettre en place des mesures qui relient les risques à des objectifs organisationnels mesurables.

L'affectation des ressources : les entreprises ont tendance à financer la gestion des risques de manière à refléter le paysage du passé au lieu d'investir pour préparer l'avenir. À une époque où de nouveaux risques apparaissent et où les anciens évoluent, cette situation tend à laisser l'effort de gestion des risques sous-financé, sous-doté en personnel et, potentiellement, sous-qualifié.

La coordination : une fonction de gestion des risques tournée vers l'avenir, efficace et résistante nécessite une prise de conscience et une coordination uniques dans l'ensemble de la structure de l'entreprise plutôt que dans les fonctions traditionnelles cloisonnées. Elle nécessite à la fois un leadership descendant et une collaboration et une exécution ascendantes, et devrait s'étendre au-delà de l'entreprise pour inclure ses partenaires, ses fournisseurs et d'autres parties prenantes.

Introduction

Il n'y a pas de certitudes dans le fonctionnement des entreprises. La possibilité que quelque chose se passe mal au sein de chaque entreprise et à chaque point de sa chaîne de valeur est omniprésente. Qu'il s'agisse d'un ralentissement des marchés clés, d'une perturbation des approvisionnements essentiels ou des actions malveillantes d'un employé mécontent, les risques difficiles à anticiper ou à éviter pèsent sur les résultats et les objectifs des entreprises. Les dommages peuvent aller d'une irritation mineure à la faillite et à l'emprisonnement dans les cas extrêmes.

La lutte contre ces menaces est une discipline complexe qui évolue rapidement. Elle est compliquée par le fait que l'intensité, la nature et l'étendue des risques changent au fil du temps. Pendant et immédiatement après la crise financière de 2008-2009, le risque de ne plus recevoir de crédit était une préoccupation majeure. Pendant la pandémie de COVID-19, l'accent a été mis sur la continuité des activités, les entreprises ayant été contraintes de fermer leurs portes en raison des confinements. Lorsque les chars russes ont pénétré en Ukraine en 2022, les restrictions en matière d'approvisionnement mondial en denrées alimentaires et en carburant ont fait grimper les prix en flèche et ont perturbé les chaînes d'approvisionnement.

L'essor de formes de technologie de plus en plus avancées et facilement accessibles, associé à la généralisation et au renforcement du télétravail, a introduit un nouveau niveau de risque. Les frontières géographiques des entreprises se sont étendues, passant de bureaux spécialement construits et centralisés à des greniers, des bureaux et des vérandas de résidences privées, souvent situés à de nombreux kilomètres du siège social et fréquemment dans un autre pays. La sécurisation des processus et des données propriétaires dans un environnement aussi dispersé est doublement complexe, car chaque employé devient un point de fuite ou de sabotage potentiel.

Economist Impact, sponsorisé par Iron Mountain, a mené une étude primaire pour comprendre comment les dirigeants perçoivent les principaux facteurs internes et externes qui déterminent l'approche d'une entreprise en matière de risques et le rôle que les dirigeants, les technologies et l'organisation institutionnelle jouent dans la gestion des risques. Economist Impact s'est appuyé sur les données issues d'entretiens avec des experts et sur une enquête personnalisée menée auprès de 656 dirigeants exerçant dans des secteurs d'activité clés en Australie, au Brésil, au Canada, en France, en Allemagne, à Hong Kong, en Inde, au Mexique, en Nouvelle-Zélande, à Singapour, au Royaume-Uni et aux États-Unis.

La gestion des risques : tendances et perceptions

La gestion des risques a évolué en discipline visant à faire face aux menaces grandissantes. Elle a progressivement gagné en profondeur et en importance dans la structure d'une entreprise, impliquant davantage de personnes et de ressources (mais jamais assez, semble-t-il) à un niveau plus élevé. La responsabilité des risques est souvent assumée par le conseil d'administration, les responsables des risques rendant compte directement au directeur financier ou au président-directeur général. Parallèlement, les responsables des risques sont moins considérés comme les chefs d'une division distincte que comme des coordinateurs d'activités répartis dans l'ensemble de l'entreprise. La propriété des risques et la responsabilité de leur signalement dans la chaîne incombent souvent aux chefs de division, la fonction de gestion des risques fournissant des conseils, rassemblant des données et recommandant des mesures correctives à la haute direction.

Le chemin a été long depuis le risque à peine reconnu jusqu'à l'architecture du risque à l'échelle de l'entreprise d'aujourd'hui. La prise de conscience du risque en tant que préoccupation organisationnelle existentielle est apparue dans la seconde moitié du siècle dernier, mais les premiers gestionnaires des risques n'ont été nommés que dans les années 1980, et ce n'est qu'au début de ce siècle que cette fonction a été considérée comme une réponse générale au risque. Aujourd'hui, la gestion des risques est reconnue comme une compétence clé des cadres supérieurs. Plus de quatre entreprises sur cinq représentées dans notre enquête déclarent avoir investi dans des équipes de gestion des risques à l'échelle de l'entreprise dans le cadre de leur approche tactique de la discipline.

Notre étude suggère que le parcours reste incomplet, bien que les responsables des risques seniors aient une compréhension de plus en plus sophistiquée de la discipline. Par exemple, l'attention passe de la réaction aux risques lorsqu'ils apparaissent à l'anticipation et au renforcement de la résilience de l'entreprise avant que les dommages ne se produisent. L'identification des risques a gagné en importance depuis 2020 pour plus de 90 % des personnes que nous avons interrogées, tout comme la modélisation prédictive des risques pour presque autant d'entre elles. L'accent mis sur l'anticipation s'étend au remodelage de l'entreprise à cette fin, et 28 % déclarent chercher à améliorer leur capacité à identifier et à anticiper les menaces, tandis que 41 % disent anticiper les risques en surveillant les menaces émergentes et en identifiant les anomalies dans les processus. Ce changement d'orientation n'est guère surprenant compte tenu de la succession de crises qui ont pris de court les dirigeants d'entreprises au cours des dernières décennies.

Les entreprises sont également confrontées à l'interconnexion des risques. Une évolution

défavorable dans une partie de l'entreprise, ou du monde, peut se répercuter sur les opérations de multiples façons. La fermeture d'un fournisseur clé à la suite d'une catastrophe naturelle peut entraîner des retards de production, une augmentation des coûts due à la recherche d'autres sources d'approvisionnement, une perte de revenus en raison du retard ou de l'absence d'exécution des commandes, ainsi qu'une atteinte à la marque et à la réputation de l'entreprise au fur et à mesure que la nouvelle de la perturbation circule. À partir d'un simple risque lié à un tiers, toute l'entreprise est entraînée dans la gestion de la crise. L'anticipation de ces menaces éventuelles est un élément clé de la gestion des risques moderne.

Là encore, les entreprises font des progrès, mais des améliorations sont possibles. Sophie Heading, responsable des risques mondiaux au Forum économique mondial, explique que « la connectivité entre les risques est mieux perçue, mais qu'elle évolue encore. Avec un peu d'imagination, l'implication d'événements survenus dans une partie du monde peut être utilisée pour prévoir un risque potentiel dans une autre. L'absence d'une telle vision peut rendre l'entreprise vulnérable aux risques qui découlent de ces événements. »

Simeon Fishman, vice-président exécutif et directeur des risques chez The Clearing House, estime que l'on s'intéresse de plus en plus aux risques émergents, c'est-à-dire les risques qui sont moins définis et moins apparents. Il explique que « maintenant, il est davantage important pour les entreprises d'avoir une plus grande visibilité sur l'horizon et d'essayer de mieux comprendre ces risques. Le risque technologique, qui est en constante évolution, constitue un domaine crucial des risques émergents. Par exemple, seuls quelques fournisseurs proposent des services d'informatique dématérialisée, ce qui a le potentiel d'entraîner une concentration du cloud. Une entreprise axée sur la technologie, au travers du logiciel qu'elle utilise ou développe, peut ainsi sans le vouloir mettre tous ses œufs dans un seul ou quelques paniers. »

Les responsables sont aidés dans ce passage d'une gestion réactive à une gestion proactive des risques par un ensemble émergent d'outils numériques, comme le montrent les réponses à notre enquête, où 43 % des dirigeants ont déclaré utiliser les technologies cognitives et l'IA pour gérer les risques. Toutefois, si le changement est la marque de fabrique des responsables des risques, le rythme du changement que nous observons dans le domaine de l'IA comporte ses propres défis. Il est clair que l'apprentissage automatique offre une nouvelle façon d'interroger les données qui entrent et sortent d'une grande entreprise, en aidant les analystes en chair et en os à repérer des schémas qu'ils n'auraient peut-être pas identifiés d'eux-mêmes. Mais il pourrait aussi devenir un vecteur de cyberattaques, les pirates et les escrocs utilisant la technologie pour renforcer leur programmation. Il est encore trop tôt pour dire comment cette technologie se développera et quel sera son impact net sur la gestion des risques.

Les technologies ne peuvent pas vous mener loin si vous n'avez pas la bonne conception, la bonne architecture de risque ou les bonnes données dans vos systèmes. Il est également essentiel de comprendre comment les processus commerciaux et les données sont liés. Une fois la conception et les données en place, les outils d'analyse et de consultation des données peuvent être exploités pour parvenir à une compréhension plus complète des risques présents dans une entreprise.

Simeon Fishman, vice-président exécutif et directeur des risques chez The Clearing House

La nécessité d'anticiper les risques et leurs impacts dans l'ensemble de l'entreprise, à une époque où les changements technologiques sont rapides, souligne l'importance d'adopter une approche holistique de la gestion des risques. En se contentant de réagir aux menaces une fois qu'elles apparaissent, les entreprises sont prises au dépourvu et peinent à rattraper leur retard. De plus, le fait de se concentrer séparément sur chaque domaine d'activité expose l'entreprise à des risques éventuels. La réponse ne consiste pas simplement à s'appuyer sur des technologies innovantes. En adoptant aveuglément l'innovation, les entreprises s'exposent à de nouvelles menaces imprévues. Mme Heading met en garde contre le fait que « la technologie permet de gérer les risques. Mais elle doit être associée à l'élément humain. »

L'approche holistique de la gestion des risques nécessite un leadership au sommet et une coordination vers le bas et à travers la structure organisationnelle afin de porter toutes les informations disponibles à l'attention des personnes les mieux placées pour les interpréter et agir. Le Dr Witold J. Henisz, vice-doyen et directeur de faculté de l'initiative Environnement, Social et Gouvernance de la Wharton School, est du même avis, ajoutant que « rendre les données compréhensibles, transparentes et faciles à comprendre est extrêmement important lorsque l'on réunit des personnes ayant des compétences différentes en matière de données et des antécédents fonctionnels divers. »

Comme le suggère l'appellation « holistique », la gestion des risques devient la responsabilité de l'ensemble de l'entreprise (et de ses fournisseurs, partenaires et distributeurs). Les responsables des risques mettent en œuvre et coordonnent le système, mais contrairement au directeur du marketing ou au directeur des opérations, il ne s'agit pas d'une compétence qui leur est réservée. La gestion des risques est passée d'un bureau intégré quelque part dans l'organigramme à un élément intégral de la culture organisationnelle, au même titre que la marque, la déclaration de mission ou l'approche du développement et la rétention du capital humain. Elle comprend des engagements à l'échelle de l'entreprise, tels qu'une déclaration relative à la propension au risque, une caractéristique de plus en plus

courante des entreprises modernes, qui définit le niveau de risque acceptable et l'attitude générale de l'entreprise en matière de prise de risques.

La coordination entre les différentes unités de l'entreprise, sa chaîne d'approvisionnement élargie et ses principales parties prenantes est au cœur de cette approche. Comme le montre notre enquête, de nombreux gestionnaires de risques seniors prônent cette approche au sein de leur entreprise. Parmi les personnes interrogées, 77 % reconnaissent que la gestion des risques doit prendre en compte toutes les parties de l'entreprise, tandis que 46 % déclarent avoir investi dans des équipes de gestion des risques à l'échelle de l'entreprise. Par ailleurs, 36 % des personnes interrogées déclarent que l'intégration de la gestion des risques dans la stratégie globale de l'entreprise et dans le processus décisionnel est une priorité.

Cela nécessite « des changements structurels qui varient en fonction du type et de la taille de l'entreprise », selon M. Fishman. « La communication entre la haute direction et le P.-D.G., d'une part, et l'ensemble des employés, d'autre part, devient de plus en plus essentielle pour garantir que la gestion des risques fait partie de l'ADN de toute l'entreprise et qu'elle ne constitue pas seulement une fonction établie qui s'engage particulièrement dans la promotion de la gestion des risques. »

Mais les dirigeants ne parviennent toujours pas à atteindre la situation idéale. 57 % ont déclaré que leur entreprise devait améliorer la collaboration interfonctionnelle. Seuls 4 % des dirigeants interrogés ont déclaré disposer d'un comité de gestion des risques directement responsable de la gestion des risques, tandis que 27 % ont indiqué que leur P.-D.G./président/associé en était directement responsable. Plus de 60 % des personnes interrogées pensent que leur entreprise doit améliorer l'engagement des employés et le partage d'informations entre les fonctions, les équipes et les partenaires externes.

La gestion des risques au niveau des quatre piliers

Par nature, le risque est diffus. Même lorsque les sources sont claires (ce qui est rare), il est difficile de prévoir le chemin que prend le risque : où il entre dans l'entreprise et comment il s'y déplace. Dans cette section, nous examinerons quatre manifestations distinctes du risque organisationnel, nous suivrons leurs effets et nous étudierons la manière dont les dirigeants y font face. Les quatre piliers sont les suivants :

- L'évolution du lieu de travail
- La cybersécurité et la gouvernance des données
- La durabilité environnementale
- L'efficacité des opérations

L'évolution du lieu de travail

Une entreprise n'est guère plus que le groupe de personnes qu'elle réunit pour poursuivre sa mission. Leurs différents talents se combinent pour transformer les intrants en extrants de plus grande valeur. À juste titre, de nombreuses entreprises accordent une très grande importance à leurs ressources humaines et investissent de l'argent et des efforts pour les recruter, les former et les conserver. Cependant, parallèlement à leurs compétences et à leur énergie, les humains sont imprévisibles et ont tendance à commettre des erreurs. Les risques liés aux personnes sont parmi les plus difficiles à gérer, et ce, pour trois raisons. Tout d'abord, les personnes servent de médiateur à tous les processus qu'une entreprise exécute, avec ou sans technologie, de sorte que les risques qu'elles posent se manifestent partout. Deuxièmement, elles sont soumises à l'action de l'homme, ce qui rend leurs performances imprévisibles par rapport à celles d'une machine. Troisièmement, la relation entre les entreprises et leur personnel évolue, le télétravail devenant de plus en plus courant, de sorte que ce qui prévaut aujourd'hui peut s'avérer différent de ce qui prévaudra demain.

Les personnes ont toujours été la plus grande force et la plus grande faiblesse des entreprises, mais des développements récents ont accru les risques. La transformation numérique de ces dernières décennies a stimulé la productivité en général, mais elle a également rapproché les employés des processus critiques et des données précieuses. En raison de cette proximité, le personnel négligent ou mal intentionné peut causer plus de dégâts qu'auparavant. Plus récemment, la pandémie de COVID-19 a provoqué une transformation profonde et soudaine de nombreux environnements de travail : les entreprises ont fait face à une pénurie de personnel à un moment critique et se sont précipitées pour mettre en place des systèmes de travail à domicile. Comme l'explique M. Fishman, elles ont également été confrontées à un nouveau défi managérial. « Il se peut que nous n'ayons pas la même compréhension des rôles et des responsabilités de chacun. La visibilité des comportements de chacun et de certaines vulnérabilités aux risques devient plus difficile avec le télétravail », explique-t-il.

À mesure que la pandémie se résorbe, les entreprises constatent que l'attitude de leurs employés à l'égard du travail a changé, peut-être de façon permanente. Le personnel en place est souvent peu enthousiaste à l'idée de retourner au bureau, tandis que les nouvelles recrues potentielles s'attendent à ce que le télétravail devienne la norme. Les entreprises ont également connu une pénurie de main-d'œuvre, en partie à cause des effets à long terme de la pandémie sur la santé, mais également en raison d'une tendance surnommée « la grande démission », qui a été provoquée par une confluence de facteurs, tels que la protestation contre les lieux de travail toxiques.

À l'avenir, les changements générationnels dans les attitudes et les attentes des employés, y compris la priorité croissante accordée à des valeurs telles que la diversité, la durabilité environnementale et la justice sociale, rendront plus difficiles l'attraction et la rétention du personnel. Le salaire seul ne suffira pas. Cela risque de créer une inadéquation entre les compétences requises dans un environnement

technologique en évolution rapide et la disponibilité et la volonté des recrues sur le marché. Les entreprises peuvent se trouver confrontées à un manque de compétences, ce qui nuit à la productivité et augmente le risque d'erreurs et d'actes malveillants.

Comme dans d'autres domaines de risque, les entreprises ne suivent pas toutes l'évolution de la situation, même si beaucoup le font. Les plus innovantes délocalisent leurs bureaux pour s'adapter à la nouvelle réalité, plus décentralisée. Les résultats de notre enquête montrent que 94 % des entreprises ont diversifié leur approche du bureau physique et du lieu de travail, la pandémie ayant incité 45 % d'entre elles à le faire au cours des trois dernières années. À ce titre, 96 % des personnes interrogées ont indiqué que leur entreprise a développé de nouvelles politiques et procédures de gestion de la main-d'œuvre, y compris le travail hybride. Les entreprises évaluent également les besoins en matière de talents pour un monde du travail en mutation, ce qui inclut la fonction de gestion des risques. Les grandes entreprises « examinent leur modèle de recrutement du personnel afin de s'assurer qu'elles disposent de gestionnaires risques compétents sur le plan technologique », déclare M. Fishman. « Le rôle des experts en technologie en matière de risque et de reprise après sinistre est essentiel, comme celui des experts du cloud et de l'IA. »

Les entreprises recueillent également davantage de données sur les questions liées à la main-d'œuvre et développent des processus plus méthodiques pour gérer le recrutement et la conservation du personnel. Notre enquête le confirme : la moitié des personnes interrogées déclarent exploiter davantage de données à cette fin, et un peu plus indiquent avoir développé un vivier de talents.

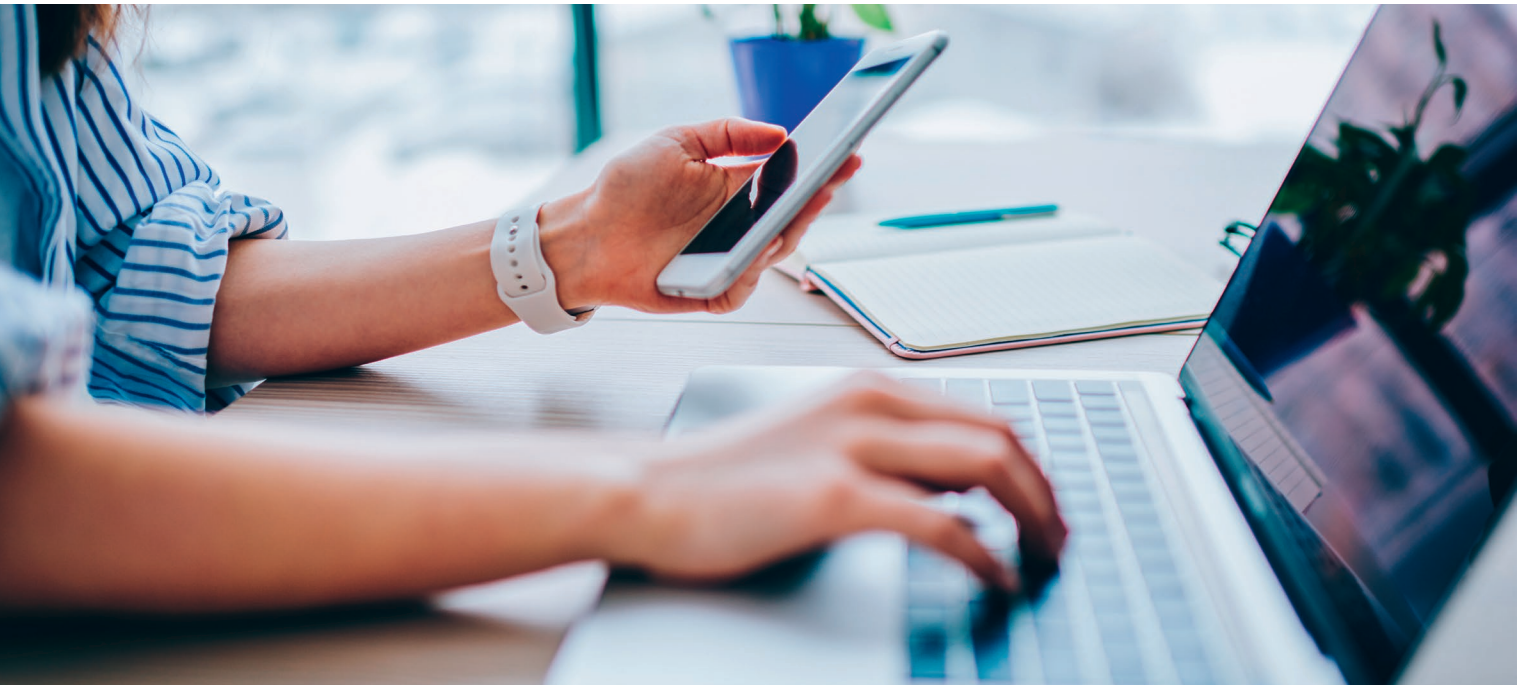
La cybersécurité et la gouvernance des données

L'adoption enthousiaste des technologies de l'information par les entreprises a transformé leurs opérations. Depuis l'époque des installations centralisées avec des armées de travailleurs supervisées par des responsables austères dans des hiérarchies strictes, les entreprises sont devenues plus souples, plus agiles et beaucoup plus productives, en grande partie grâce à la numérisation. Les ordinateurs, l'automatisation et Internet ont profondément bouleversé les modèles de travail, et les développements futurs tels que l'informatique quantique, l'Internet des Objets omniprésent et le métavers promettent des changements tout aussi fondamentaux.

De manière générale, l'impact de la révolution numérique sur la gestion des risques organisationnels est triple : les risques apparaissent plus soudainement et se propagent beaucoup plus rapidement ; les données, leur stockage, leur transmission et leur interprétation sont devenus un ingrédient essentiel des opérations ; et, si la numérisation a créé de nouveaux domaines de risque, elle a également donné naissance à de nouveaux outils pour y faire face.

Lorsque les informations circulent à la vitesse de la lumière sur un réseau numérique mondial, les choses évoluent trop vite pour que l'être humain puisse réagir. Les ordinateurs prenant de plus en plus de décisions à la place des humains, les processus peuvent passer par de nombreuses itérations avant qu'une erreur ou un résultat inattendu ne soit détecté. Les clients et les partenaires étant tous branchés sur les médias de communication mondiaux, la réputation d'une marque peut se retrouver dans le tribunal de l'opinion publique avant que les dirigeants de l'entreprise n'aient pleinement réalisé ce qui se passe.

Avec l'IA générative, nous assistons à l'émergence d'un nouveau risque informatique potentiel. Le rythme de son adoption a laissé la société dans son sillage, les décideurs et les régulateurs, ainsi que les créateurs pionniers de la technologie, s'efforçant de suivre le mouvement. Les responsables des risques ne savent pas vers qui se tourner pour obtenir les meilleurs conseils à ce stade précoce de ce qui pourrait s'avérer aussi perturbateur pour les modèles d'entreprise que l'Internet lui-même. « Qui dispose d'une expertise en matière de risque sur l'évolution de l'IA générative ? », demande M. Fishman. « Quels moyens sophistiqués pouvons-nous adopter pour mieux surveiller la concentration du cloud ? Compte tenu de l'évolution du paysage informatique, comment pouvons-nous continuer à intégrer la résilience dans nos infrastructures et nos processus ? »



Ce domaine pose des questions pressantes et des défis complexes aux responsables des risques et aux entreprises. Dans ces cas-là, il est bon de commencer par les principes de base. Il est primordial que les entreprises se concentrent sur trois grands domaines de risque lorsqu'il s'agit de gérer leurs actifs numériques :

- La gouvernance des données : garantir l'exactitude, la cohérence et l'accessibilité des données.
- La sécurité des données : protéger les données contre l'accès, l'utilisation, la divulgation, la perturbation, la modification ou la destruction non autorisés.
- La protection des données : protéger la vie privée des individus en contrôlant la manière dont leurs données à caractère personnel sont recueillies, utilisées et partagées.

Les mêmes principes de proactivité et d'analyse de l'horizon restent valables, mais avec plus d'urgence qu'auparavant. De même, assurer la conformité est un plus grand défi dans un paysage réglementaire aussi incertain et en évolution rapide, mais n'en est pas moins vital.

Les résultats de notre enquête indiquent que les entreprises ont fait preuve de dévouement et de cohérence dans leurs efforts visant à atténuer les risques liés aux données et à la cybersécurité par le biais de différentes mesures. Au cours des trois dernières années, 49 % des entreprises ont investi dans des plans de reprise après sinistre/de continuité des activités pour les systèmes numériques, et 48 % dans des services de cloud/stockage sur le cloud et dans la surveillance et la prévention permanentes des risques et des menaces informatiques. Au cours de la même période, 46 % des dirigeants interrogés ont également fait état d'investissements dans les talents en matière d'informatique et de cybersécurité, ainsi que dans la formation à la maîtrise des données et des techniques.

En parallèle, les responsables des risques devraient s'intéresser de près à l'évolution de l'IA, non seulement en tant que source de risques, mais aussi en tant que moyen de les atténuer. Parmi les personnes interrogées 43 % déclarent utiliser les technologies cognitives et l'IA dans les processus de gestion des risques. Correctement formée et dirigée, l'IA peut détecter des modèles

étranges, identifier des tendances, élaborer des scénarios et repérer des zones de risque que les analystes en chair et en os pourraient ne pas voir.

Peu d'entreprises sont à l'abri des cyberrisques, mais certains secteurs y sont plus exposés que d'autres. Par exemple, les secteurs de la santé et de la finance gèrent tous deux d'énormes quantités de données sensibles sur les clients Tirer le meilleur parti de cette mine de données, notamment pour calculer les risques encourus par le client ou l'entreprise, tout en veillant à leur sécurité, est une tâche colossale. Le coût d'un échec peut être dévastateur. Sans surprise, parmi tous les secteurs, c'est dans celui de la santé que le pourcentage de personnes ayant répondu à l'enquête est le plus élevé (83 %), ce qui témoigne de l'importance croissante des indicateurs technologiques au cours des trois dernières années. Il s'agit notamment du temps de fonctionnement du réseau, des incidents de cybersécurité et des erreurs logicielles.

Le secteur de l'énergie s'appuie également sur les données pour rationaliser ses opérations, tandis que l'État moderne s'appuie fortement sur les données des citoyens pour fournir des services publics avec une efficacité maximale. Dans le cas des gouvernements, le coût de l'échec en matière de réputation peut être particulièrement préjudiciable, mettant les hommes politiques et leurs partis en conflit direct avec leur électorat.

Le développement durable

L'industrialisation a apporté à l'humanité des bienfaits inimaginables pour nos ancêtres de l'ère préindustrielle. Mais en brûlant des combustibles fossiles pour l'alimenter, nous avons mis en péril la durabilité de notre mode de vie - et nos vies. Les gaz à effet de serre (GES) libérés dans l'atmosphère, en grande partie à cause de notre activité économique, augmentent les températures moyennes de la planète. Les effets seront potentiellement catastrophiques au cours des prochaines décennies, mais nous ne sommes pas obligés d'attendre aussi longtemps. Les phénomènes météorologiques extrêmes se multiplient, le niveau des mers monte et la biodiversité est menacée.

L'impact sur les entreprises est double. Premièrement, les opérations et les chaînes d'approvisionnement sont susceptibles d'être perturbées par des phénomènes météorologiques extrêmes et d'autres effets environnementaux difficiles à anticiper. Les événements des trois dernières années ont incité 47 % des entreprises interrogées à se concentrer sur le maintien de réseaux de chaînes d'approvisionnement diversifiés et flexibles. Deuxièmement, les parties prenantes des entreprises, qu'il s'agisse des clients, des investisseurs ou des employés, attendent à juste titre des entités qu'elles pèsent de tout leur poids dans la lutte contre l'épuisement des ressources, la dégradation de l'environnement et les émissions de gaz à effet de serre.

Pour l'instant, la seconde est plus urgente pour les responsables des risques (bien que la première soit une menace croissante). Les groupes d'activistes désignent rapidement ce qu'ils considèrent comme des contrevenants flagrants aux pratiques durables et disposent d'un arsenal croissant de moyens créatifs pour attirer l'attention du public. Les compagnies pétrolières et énergétiques, ainsi que les investisseurs et les banques qui les financent, font l'objet d'attaques constantes. Ces campagnes peuvent perturber directement les activités commerciales, mais elles peuvent avoir un impact plus néfaste en compromettant la réputation et le « permis d'exploitation social d'une entreprise.

L'importance des indicateurs de risque de réputation pour les dirigeants s'est accrue ces dernières années en raison de la complexité croissante des environnements opérationnels et de la nécessité pour les entreprises d'être plus transparentes, plus responsables et plus citoyennes. Un pourcentage non négligeable (80 %) des personnes interrogées dans le cadre de notre enquête ont identifié les indicateurs de risque de réputation comme étant les plus cruciaux en matière d'importance croissante pour leur surveillance des risques.

Comme pour la cybersécurité, la durabilité environnementale et les domaines connexes de la politique sociale et de la gouvernance (ESG) constituent un paysage de risques en évolution rapide. Les préoccupations environnementales ont pris de l'importance dans l'agenda public, et les entreprises ont réagi en publiant des déclarations faisant état de leurs compétences « vertes ». Toutefois, ces déclarations sont souvent qualifiées « d'éco-blanchiment » et ne suffisent pas à protéger les entreprises de la colère de

l'opinion publique. Les déclarations relatives à la mission écologique sont de plus en plus souvent remplacées par des promesses d'atteindre zéro émission nette de GES, accompagnées de feuilles de route indiquant la stratégie pour y parvenir.

Pour les grandes entreprises, cela ne suffit plus. Les citoyens font pression pour que les entreprises et le secteur public adoptent une attitude « positive à l'égard de la nature », les entreprises étant invitées à présenter des plans visant à faire revenir l'environnement à son état préindustriel ou, au moins, à ramener les indicateurs climatiques dans des limites compatibles avec une économie durable. Mme Heading souligne « une évolution de la gestion des risques, qui passe du simple examen de la réglementation/conformité, un exercice de type « cocher la case », à une fonction beaucoup plus stratégique, qui incorpore des valeurs sociétales telles que les critères ESG. »

Notre enquête reflète le fait que les critères ESG figurent désormais dans les registres des risques des entreprises. Près de la moitié des entreprises interrogées ont consacré davantage de ressources aux initiatives ESG, tandis qu'un nombre similaire se concentre sur les rapports de performance ESG, qui sont exigés par les organismes de réglementation dans certaines juridictions.

L'efficacité opérationnelle

Pour les entreprises et leurs responsables des risques, ce sont les opérations internes qui les touchent de plus près. La plupart d'entre eux ne peuvent guère influencer les circonstances au-delà de leurs murs, physiques ou virtuels, mais ce qui se passe à l'intérieur de l'entreprise est pour l'essentiel sous leur contrôle direct. Qu'il s'agisse des personnes, des processus ou des exigences réglementaires, l'efficacité des rouages internes d'une entreprise fait la différence entre la réussite et l'échec. Et elle comporte des risques : le personnel peut ne pas fournir les performances attendues, être déçu par l'équipement sur lequel il s'appuie ou être victime de vulnérabilités dans les processus conçus pour le rendre collectivement productif.

La protection contre ces risques est un élément central de la gestion des risques depuis les débuts de cette discipline. En tant que tels, les responsables des risques peuvent facilement tomber dans le piège des vieilles perceptions selon lesquelles ils ne sont guère plus qu'un policier interne qui met des bâtons dans les roues des autres services. La fonction de gestion des risques est donc considérée comme un centre de coûts et un fardeau pour l'esprit d'entreprise des secteurs verticaux « lucratifs ». Cette perception était (et est parfois encore) un poids pour les gestionnaires de risques, mais les choses changent. Ces derniers ont appris à mieux mesurer les coûts des défaillances opérationnelles et à les comparer au coût du maintien d'une fonction de gestion des risques adaptée. Le coût d'une fonction de gestion des risques agile est moins élevé que celui d'une suspension des opérations pour rétablir un processus défaillant, d'une lourde sanction réglementaire pour mauvaise manipulation des données des clients ou d'une perte de clients due à une défaillance éthique très médiatisée.

Il n'y a pas deux entreprises identiques et il n'existe donc pas de modèle unique pour atteindre l'efficacité opérationnelle. En effet, ce que l'on entend par « opérations » peut varier considérablement au sein d'une même entreprise et d'une entreprise à l'autre. Le secteur de l'énergie se concentre sur les équipements et les processus, car le forage pétrolier ou l'extraction de minerais sont des activités à forte intensité de capital, dont la défaillance peut entraîner des catastrophes humaines et environnementales. Le secteur financier est à la fois riche en données et vulnérable aux défaillances de son personnel en raison de violations illégales des politiques et des rôles, d'une mauvaise exécution, d'un manque de formation et d'un comportement contraire à l'éthique. Ceux-ci peuvent entraîner des pertes directes ainsi que des coûts réglementaires, juridiques et de restructuration. La conformité juridique et réglementaire est particulièrement importante, d'autant plus que de nombreuses banques et institutions financières opèrent dans diverses juridictions. D'autres secteurs se concentrent plus ou moins sur la gestion du risque opérationnel, ce qui est l'un des nombreux facteurs qui compliquent la tâche des responsables des risques.

Notre enquête reflète l'importance du risque opérationnel pour les entreprises, et il apparaît clairement que les investissements dans ce domaine améliorent les performances et les résultats financiers. Plus particulièrement, 42 % des personnes interrogées font état d'une amélioration des performances résultant de

l'application de bonnes pratiques de gestion dans l'aménagement des installations et de l'espace de travail physique. Un pourcentage similaire indique une amélioration significative de l'efficacité opérationnelle de leur entreprise. Toutefois, deux tiers des personnes interrogées reconnaissent qu'il s'agit d'un enjeu à long terme et que l'investissement dans la gestion des risques perturbe les opérations à court terme.

Selon le Dr Henisz, il est essentiel de reconnaître le lien entre l'investissement et le rendement. « Nous pouvons monétiser l'impact des risques en calculant les jours d'arrêt et la perte de production », explique-t-il. « Il est essentiel de traduire les données dans le langage de la finance ou des opérations. Sinon, la fonction de gestion des risques ne sera considérée que comme un coût, alors que toutes les autres engendrent des recettes. »

Les défis rencontrés par la gestion des risques

La profession de responsable des risques est devenue plus influente et plus sophistiquée au fil du temps et elle est ancrée dans la culture et la structure de la plupart des grandes entreprises. Mais son rôle et ses méthodologies sont soumis à une pression constante pour s'adapter à un environnement de risque en constante évolution. On a eu tendance à considérer comme suffisante une stratégie de gestion des risques capable de faire face à toutes les menaces passées, alors que le passé est souvent un mauvais indicateur de la manière dont les risques se manifesteront à l'avenir. En conséquence, la gestion des risques doit évoluer en permanence à mesure que de nouvelles menaces et de nouveaux perturbateurs apparaissent. La profession doit continuer tout particulièrement à passer de la réaction à l'anticipation, en renforçant sa capacité de résistance aux menaces à venir, au lieu de se contenter de répondre à celles qu'elle connaît déjà.

À cet égard, notre enquête révèle certains progrès, mais suggère qu'il reste encore beaucoup à faire. Une écrasante majorité des dirigeants interrogés sont convaincus que les initiatives de gestion des risques mises en œuvre par leur entreprise sont suffisantes pour atténuer ou prévenir les dommages causés par les risques. Cela laisse entrevoir un certain degré d'excès de confiance de la part des entreprises, qui pourrait les laisser plus exposées qu'elles ne le pensent. Pour combler cette faille potentielle, il faut se concentrer sur trois domaines principaux : l'évaluation, l'affectation des ressources et la coordination.

L'évaluation

Le suivi des performances en matière de gestion des risques est intrinsèquement délicat. En cas d'échec de la gestion des risques, les coûts encourus peuvent être imputés au programme de gestion des risques. Cela semble clair, mais la détermination du pourcentage des coûts à attribuer à la fonction est loin d'être évidente. Il est encore plus difficile de reconnaître la contribution de la gestion des risques lorsque tout va bien. On a tendance à considérer que ce n'est rien d'autre que le « cours normal des activités » et à nier complètement la contribution des responsables des risques. Même lorsque l'on s'efforce de reconnaître la contribution de la fonction, il est difficile de quantifier ce qui doit être inscrit dans la colonne « positif ».

La fonction de gestion des risques devrait-elle rendre compte des investissements réalisés en prévision de risques qui ne se sont jamais matérialisés ? Devrait-elle être responsable des événements de type « cygne noir » (difficiles à prévoir mais qui, rétrospectivement, semblaient inévitables) qui n'ont pas attiré son attention ? Au lendemain de la crise financière mondiale de 2008-2009, largement considérée comme un événement de type cygne noir, la discipline du risque - y compris les agences de notation - a été ébranlée dans ses fondements. Il ne fait aucun doute que le resserrement du crédit était une indication de l'échec à comprendre et à gérer les risques, mais les erreurs politiques et l'insouciance du public étaient également en cause. Dans de telles circonstances, il est difficile de procéder à une évaluation détaillée des performances de la gestion des risques, ne serait-ce qu'avec un semblant de précision.

La gestion des risques partage également la difficulté, rencontrée dans de nombreux domaines opérationnels, de justifier des investissements à court terme pour en tirer des bénéfices à long terme. « Vous investissez dans quelque chose aujourd'hui et vous n'en verrez peut-être pas les bénéfices avant cinq ou dix ans, ou, à l'inverse, vous pourriez les observer dans trois mois », explique Mme Heading. « En fonction de ce que vous essayez de contrôler, il peut être très difficile de formuler ce type de coût-bénéfice de manière à ce qu'il soit facilement compris par les dirigeants. »

Les dirigeants reconnaissent les défis posés par la mesure des performances de la gestion des risques. Environ trois quarts des personnes ayant répondu à l'enquête reconnaissent que l'absence de paramètres d'évaluation standardisés pour mesurer les risques rend difficile la mise en évidence des progrès réalisés.

« Il est essentiel d'élaborer des paramètres d'évaluation qui relient les risques aux objectifs de l'entreprise et de veiller à ce qu'ils soient clairs, pour les travailleurs sur le terrain comme pour le conseil d'administration et la direction générale », déclare M. Fishman. « Les outils peuvent aider, mais la structure visant à mesurer les risques directement liés aux activités et à leur impact est fondamentale. Vous avez non seulement besoin d'examiner l'impact, mais devez également comprendre les facteurs de causalité. Par exemple, bien que l'évaluation des événements informatiques soit importante, l'efficacité avec laquelle les processus et les systèmes pallient aux vulnérabilités et garantissent la continuité des activités l'est tout autant. »

L'affectation des ressources

Peu de services s'estiment suffisamment financés, mais le cas des responsables des risques est particulièrement flagrant. Cela s'explique en partie par le fait que les entreprises ont tendance à financer cette fonction de manière à refléter le paysage des risques du passé au lieu de l'équiper pour préparer l'avenir. L'ampleur et la complexité des risques auxquels les entreprises sont confrontées ne cessent de croître à mesure que les chaînes d'approvisionnement s'allongent et s'allègent et que la technologie accélère le rythme du changement. De même, les entreprises peuvent se prévaloir d'un ensemble croissant d'outils de surveillance des risques et de renforcement de la résilience, mais ces outils nécessitent des dépenses initiales importantes et, comme nous l'avons vu, le calendrier et l'ampleur du retour sur investissement sont difficiles à quantifier.

Les personnes interrogées dans le cadre de l'enquête ont le sentiment que les services en charge de la gestion des risques manquent de ressources. Les dirigeants estiment que les ressources financières, technologiques et humaines consacrées par leur entreprise à la gestion des risques sont insuffisantes, près des deux tiers d'entre eux déclarant que leur entreprise doit s'améliorer sur ce plan.

Le défi réside en partie dans le fait que les responsables des risques doivent disposer d'un champ d'expertise plus large, alors que les entreprises deviennent de plus en plus numériques. Cela signifie que même pour maintenir un niveau de protection cohérent, les entreprises doivent dépenser davantage pour attirer les compétences requises vers la fonction de gestion des risques. « Les responsables des risques sont une denrée très recherchée », déclare M. Fishman. « Même avec les licenciements massifs dans les secteurs de la finance et de la technologie, il est difficile de trouver de bons responsables des risques. »

Avec des avancées telles que l'IA, l'automatisation et la robotique demandant toutes de l'attention, ce goulot d'étranglement est susceptible de s'aggraver. Si l'on ajoute à cela l'approche de technologies à grande échelle, telles que l'informatique quantique et les grands livres distribués, il n'y aura pas de place pour la complaisance dans le secteur de la gestion des risques dans un avenir proche.

La coordination

Comme nous l'avons vu, l'une des principales exigences en matière de gestion des risques dans les années à venir sera la capacité d'introduire l'idée de risque dans tous les secteurs de l'entreprise. Les flux d'informations ascendants doivent être coordonnés dans l'ensemble de l'entreprise, les responsables des risques établissant les règles et les outils que chaque service et employé doit utiliser. Les dirigeants doivent donner le ton pour que le rôle central du renforcement de la résilience face aux menaces connues et inconnues imprègne la culture de l'entreprise. Les partenaires, les fournisseurs et les clients doivent être inclus dans le réseau, ce qui permettra d'étendre le radar de risque de l'entreprise bien au-delà de ses murs. L'ensemble du dispositif de gestion des risques doit être axé sur ce qui se passe au quotidien dans l'entreprise, mais aussi, et c'est essentiel, sur ce qui pourrait se produire à l'avenir compte tenu des tendances émergentes. Les entreprises les plus performantes seront celles dans lesquelles cet effort sera conçu et coordonné par des responsables des risques de haut niveau, dotés des compétences et des ressources requises par un environnement en évolution rapide et bénéficiant du soutien des plus hauts dirigeants.

Le parcours de la gestion des risques n'est pas encore achevé, mais la direction prise est prometteuse.

Conclusion

La gestion des risques a parcouru un long chemin depuis sa première apparition en tant que fonction organisationnelle distincte. D'une discipline limitée principalement au secteur bancaire, où la solution consistait à constituer des coussins financiers plus généreux pour garantir la liquidité en cas d'évolution défavorable du marché, elle est devenue une pièce maîtresse de la gestion moderne. Les responsables des risques occupent une place prépondérante dans les entreprises de toutes les industries, tant dans le secteur privé que dans le secteur public. Ils saisissent et quantifient les menaces à travers un large éventail de facteurs, survenant à la fois au sein de l'entreprise et hors de ses murs, où la visibilité et le contrôle sont moindres. La gestion des risques a été adoptée à des niveaux de plus en plus élevés de l'entreprise, de nombreux responsables des risques opérant aujourd'hui au même niveau que les cadres de direction et ayant accès au P.-D.G. ou au conseil d'administration. C'est la direction prise depuis quelques décennies, et la fonction continue de s'ancrer plus profondément.

Mais de nouveaux défis apparaissent, et les anciens se transforment à mesure que les technologies, la géopolitique et les changements sociaux affectent l'environnement opérationnel. La gestion des risques a toujours été une discipline dynamique, mais le besoin de changement se fait de plus en plus pressant. Ce début de siècle a été le théâtre d'une succession de bouleversements à l'échelle mondiale . Qu'il s'agisse de la crise financière mondiale de 2008-2009 et de la crise de confiance dans la démocratie libérale qui s'en est suivie, de la pandémie de COVID-19 ou de l'invasion de l'Ukraine par la Russie, les mouvements tectoniques dans les affaires mondiales ont multiplié les incertitudes. Cela s'est produit dans le contexte d'une transition déjà ancienne, mais qui s'accélère, vers un paysage numérique, ainsi que de préoccupations environnementales qui ont des répercussions sur les entreprises, la société, la politique et l'économie mondiale.

L'accélération de l'adoption numérique, illustrée par l'émergence de modèles linguistiques génératifs pré-entraînés, est à la fois prometteuse et menaçante. Si elle promet d'engendrer une nouvelle génération d'outils pour aider les entreprises à surveiller les risques et à y répondre, elle risque aussi de doter les agents malveillants d'armes tout aussi innovantes pour voler ou corrompre des données précieuses. Les nouveaux modèles de travail, en particulier le développement du télétravail, élargissent et font disparaître la ligne de front numérique de l'entreprise, ouvrant de nouvelles voies aux cybermenaces.

Les responsables des risques poursuivent le voyage entamé il y a plusieurs décennies, en intégrant une approche des opérations axée sur le risque dans l'ensemble de l'entreprise. Ils sont confrontés à la nature de plus en plus contingente du risque, où un événement dans un coin éloigné de la chaîne d'approvisionnement peut engendrer des ramifications imprévues ailleurs.

Il est essentiel qu'ils passent d'une position réactive à une position proactive. La première approche se concentre sur le renforcement de la résilience face aux menaces attendues et sur la réponse à y apporter lorsqu'elles se matérialisent.

Dans le cadre de la deuxième approche, les responsables des risques consacrent des ressources et des efforts à scruter l'horizon à la recherche de menaces qui ne figurent pas dans le registre des risques, en se préparant à des scénarios qui peuvent sembler improbables mais qui comportent un fort potentiel de dommages.

Dans le contexte actuel des risques, caractérisé par des changements plus vastes, plus rapides et plus complexes que jamais, l'adoption d'une approche proactive pourrait être un des moyens les plus efficaces que la discipline de la gestion des risques puisse mettre en œuvre pour se préparer à l'avenir.

ECONOMIST IMPACT

LONDON

The Adelphi
1-11 John Adam Street
London WC2N 6HT
United Kingdom
Tel: (44) 20 7830 7000
Email: london@economist.com

GENEVA

Rue de l'Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
Email: geneva@economist.com

SÃO PAULO

Rua Joaquim Floriano,
1052, Conjunto 81
Itaim Bibi, São Paulo,
SP, 04534-004
Brasil
Tel: +5511 3073-1186
Email: americas@economist.com

NEW YORK

900 Third Avenue
New York, NY 10022
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
Email: americas@economist.com

DUBAI

Office 1301a
Aurora Tower
Dubai Media City
Dubai
Tel: (971) 4 433 4202
Fax: (971) 4 438 0224
Email: dubai@economist.com

HONG KONG

1301
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
Email: asia@economist.com

SINGAPORE

8 Cross Street
#23-01 Manulife Tower
Singapore
048424
Tel: (65) 6534 5177
Fax: (65) 6534 5077
Email: asia@economist.com