

2023

Rapport sur la résilience stratégique des entreprises

Positionnez votre entreprise afin qu'elle puisse évaluer
l'évolution des risques, s'y préparer et s'adapter



L'instabilité mondiale, les changements sociétaux et les avancées technologiques ont

ouvert une nouvelle ère de risques que les dirigeants d'entreprise doivent prendre en compte. Les récents progrès réalisés dans le domaine de l'intelligence artificielle (IA) générative témoignent de la vitesse à laquelle les changements peuvent s'opérer, les leaders de gouvernements et les chefs d'entreprise s'empressant de tirer parti de la technologie et de se protéger contre les risques qu'elle représente. Pendant ce temps, les risques géopolitiques, économiques, sociaux, naturels et de cybersécurité continuent d'évoluer.

Alors que les chefs d'entreprise font face à cette situation incertaine d'expositions émergentes et de perturbations imminentes, l'élaboration de stratégies de résilience solides est primordiale. Le Rapport sur la résilience stratégique des entreprises 2023 de CNA Canada donne un aperçu de l'environnement de risque actuel et présente des observations pertinentes pour améliorer la capacité des entreprises à atténuer et à gérer les événements perturbateurs.



Principaux facteurs de renforcement de la résilience :

01 COMPRENDRE
L'ÉVOLUTION
DES RISQUES

02 METTRE EN PLACE
DES COUVERTURES
STRATÉGIQUES

03 RENFORCER ET
AMÉLIORER LA RÉSILIENCE
OPÉRATIONNELLE



01 COMPRENDRE L'ÉVOLUTION DES RISQUES

Les menaces auxquelles sont confrontées les entreprises d'aujourd'hui sont plus complexes et interconnectées que jamais, et chaque entreprise doit faire face à une myriade de défis qui nuisent à sa capacité d'exercer ses activités. Pour gérer avec souplesse les répercussions potentielles, identifier les risques à un stade précoce est essentiel.

Les chefs d'entreprise doivent se poser un certain nombre de questions lorsqu'ils planifient des scénarios perturbateurs, telles que : comment les modifications réglementaires, les avancées technologiques ou les tendances du marché peuvent-elles influencer la trajectoire de l'entreprise ? Ces risques émergeront-ils progressivement, laissant à l'entreprise le temps de se préparer et de s'adapter ? Si ce n'est pas le cas, comment l'entreprise ferait-elle face à une perturbation soudaine qui exigerait une intervention immédiate ? Au cours des dernières années, de très importants changements sont survenus dans le domaine des risques, forçant ainsi les entreprises à se préparer à des répercussions sur tous les aspects de leurs activités.



Intelligence artificielle

Les effets potentiels de l'intelligence artificielle (IA) sont difficiles à surestimer. On estime que celle-ci contribuera à la croissance économique mondiale à hauteur de 15,7 billions de dollars d'ici 2030¹, et de nombreuses entreprises exploitent déjà les capacités de l'IA pour réduire leurs coûts et acquérir un avantage concurrentiel. L'outil ChatGPT d'OpenAI, qu'elles utilisent pour rationaliser les processus et améliorer le soutien à la clientèle, a atteint le chiffre record de 200 millions d'utilisateurs actifs en l'espace de deux mois au début de l'année 2023. Les revenus de l'application devraient dépasser le milliard de dollars en 2024.

Malgré sa promesse de transformation, l'IA, insuffisamment réglementée, présente également des risques importants. L'informaticien Geoffrey Hinton, considéré comme le « parrain de l'intelligence artificielle », affirme que ChatGPT possède des connaissances 100 fois supérieures à celles du cerveau humain, ce qui lui permet de générer des contenus diversifiés (codes d'application, textes, images et vidéos) avec une précision et une efficacité inégalées².

Début 2023, monsieur Hinton a démissionné de son poste pour exprimer librement ses inquiétudes quant aux capacités des machines qu'il avait hautement contribué à développer. Dans une entrevue accordée au *New York Times*, il a mis l'accent sur les risques liés à cette technologie, notamment la prolifération de la désinformation sur Internet, la suppression d'emplois pour des postes liés aux services d'assistance, aux services d'aide personnelle et de traduction,

et l'exploitation potentielle de l'IA par des entités malveillantes à la recherche d'avantages sur les plans criminel, politique ou en lien avec la sécurité nationale³.

La gravité de ces inquiétudes a incité le Future of Life Institute à obtenir le soutien de plus de 1 000 informaticiens en mars 2023, exhortant tous les laboratoires d'IA à prendre une pause immédiate d'au moins six mois. Leur approbation collective souligne l'impact transformateur que l'IA de pointe pourrait avoir sur l'avenir de la vie sur Terre, mais aussi le besoin de mettre en place des contrôles minutieux, des réglementations réfléchies ainsi qu'une surveillance approfondie, avec des ressources adéquates et en temps opportun.

Le Parlement européen travaille à la mise en œuvre des premières lois exhaustives sur l'IA pour la fin de l'année 2023, afin d'établir des contrôles, des

Contribution de l'IA à la croissance économique mondiale

1 milliard de dollars (ChatGPT uniquement)



2024

15,7 billions de dollars



2030

réglementations et des mécanismes de surveillance. Les réglementations visent à garantir que « les systèmes d'IA utilisés dans l'UE sont sûrs, transparents, traçables, non discriminatoires et respectueux de l'environnement. Les systèmes d'IA devraient être supervisés par des personnes, plutôt que par l'automatisation, afin d'éviter des résultats néfastes⁴. »

Compte tenu de la croissance exponentielle de l'IA, de la diversité des cas d'utilisation de la part des chefs d'entreprise et de l'impact potentiel d'une législation imminente, la surveillance des entreprises est primordiale. Les entreprises qui utilisent l'IA considèrent que les risques principaux de cette technologie sont la cybersécurité, la confidentialité des données, la responsabilité, la conformité juridique, la dépendance à l'égard de tiers pour les algorithmes de l'IA, l'absence de réglementation, la réputation, les préjugés et la sécurité physique⁵.

(Remarque : Dans une démonstration concrète de l'utilité de l'IA, ChatGPT a été utilisé pour améliorer la qualité du contenu du présent rapport.)

¹ PWC (n/a) : Artificial Intelligence everywhere. En ligne (septembre 2023) : <https://www.pwc.com/gx/en/issues/data-and-analytics/artificial-intelligence.html>.

² Hamilton, David et The Associated Press (2023) : « The "Godfather of AI" says he's scared tech will get smarter than humans : "How do we survive that?" », Fortune, 4 mai 2023. En ligne : <https://fortune.com/2023/05/04/geoffrey-hinton-godfather-ai-tech-will-get-smarter-than-humans-chatgpt/>

³ METZ, Cade (2023) : « 'The Godfather of A.I.' Leaves Google and Warns of Danger Ahead », The New York Times, 1er mai 2023, en ligne : <https://www.nytimes.com/2023/05/01/technology/ai-google-chatbot-engineer-quits-hinton.html>

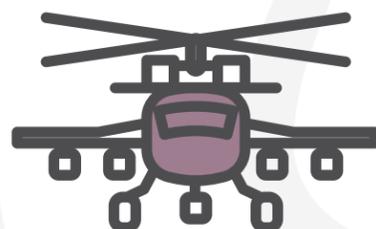
⁴ PARLEMENT EUROPÉEN (2023) : Loi sur l'IA de l'UE : première réglementation de l'intelligence artificielle, 9 juin 2023. En ligne : [Loi sur l'IA de l'UE : première réglementation de l'intelligence artificielle | Actualité | Parlement européen \(europa.eu\)](https://www.europa.eu/press-room/media/infographic/item-10444)

⁵ Corporate Oversight of Artificial Intelligence », Baker McKenzie, 30 mars 2022. En ligne : https://www.bakermckenzie.com/-/media/files/aisurveypptfinalmarch2022.pdf?sc_lang=en&hash=E7BCD28D19AF8D726596FC648F27C9F2.



Conflits et instabilité géopolitique

La méfiance entre les États-Unis et la Chine ainsi que les tensions entre les deux pays sont de plus en plus préoccupantes. Le *New York Times* observe que tous deux « se font concurrence au-delà de leurs propres frontières, rivalisent en matière de technologie et font preuve de manipulation pour obtenir des avantages militaires sur le terrain, dans l'espace extra-atmosphérique et dans le cyberspace⁶ ». En raison d'une dépendance à l'égard du commerce international et des partenariats commerciaux, une nouvelle détérioration pourrait affecter de manière significative le commerce mondial.



Dans les pays clés, les dépenses militaires ont augmenté :

États-Unis	Russie
Chine	Inde
Iran	Arabie saoudite

Ces tensions mènent à une course aux armements moderne. Dans un contexte de renversement de la tendance à la démilitarisation, observée au cours des 15 dernières années avant 2022, les dépenses militaires ont augmenté au sein des puissances mondiales et régionales telles que les États-Unis, l'Iran, la Russie, l'Inde, la Chine et l'Arabie saoudite. En outre, le soutien des 31 pays membres de l'OTAN à l'effort de guerre en Ukraine permettra probablement d'atteindre 7 % du PIB si tous les membres atteignent leurs objectifs de dépenses⁷.

Bien que le rythme de développement des armes d'attaque, leur volume et la tendance se profilant vers des armes plus précises soient difficiles à contrôler sans une collaboration transnationale, les nations tendent à se concentrer sur leurs propres ressources et intérêts en matière de sécurité.

En outre, l'augmentation des investissements militaires locaux, régionaux et mondiaux détourne les ressources nécessaires à l'entretien et à

l'amélioration des infrastructures et du commerce.

L'invasion de l'Ukraine par la Russie a provoqué des difficultés économiques loin des zones de conflit, déclenchant de grandes migrations, ainsi que l'inflation et la fermeture des voies d'approvisionnement. En juillet 2023, la Russie a annoncé ne pas reconduire l'accord sur l'exportation de céréales ukrainiennes (blé, maïs, graines de tournesol et huile végétale) en mer Noire, en raison de la rentabilité croissante de ces exportations⁸. Malheureusement, cette décision signifie que les pays vulnérables du Moyen-Orient et d'Afrique seront davantage exposés à l'insécurité alimentaire à long terme tant que les voies de transport seront bloquées⁹.

Afin de limiter les perturbations potentielles des activités, les chefs d'entreprise doivent suivre de très près les tendances mondiales et se préparer à adapter rapidement leurs activités et leurs chaînes d'approvisionnement.

⁶ U.S.-China Relations: What to Know - The New York Times (nytimes.com) En ligne : <https://www.nytimes.com/2023/07/17/world/europe/ukraine-grain-deal-russia-war.html>

⁷ FORUM ÉCONOMIQUE MONDIAL (2023) : Global risks. En ligne : <https://intelligence.weforum.org/topics/a1Gb0000000pTDXEa2>

⁸ MPOKE BIGG, Matthew, NECHEPURENKO Ivan, ALDERMAN, Liz et al. (2023): « Russia Stops Ukraine Grain Deal, Shaking World Food Markets », New York Times. En ligne : <https://www.nytimes.com/2023/07/17/world/europe/ukraine-grain-deal-russia-war.html>

⁹ Ibid



Changement climatique

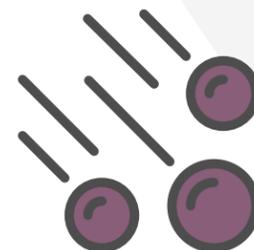
Les effets du changement climatique se font déjà sentir et continueront probablement de s'intensifier en l'absence d'une collaboration mondiale et d'une action collective. Le Groupe d'experts intergouvernemental sur l'évolution du climat (GIEC) des Nations unies affirme que « le réchauffement de la planète continuera de s'aggraver à court terme (2021-2040) [...] dans la quasi-totalité des scénarios envisagés et des trajectoires modélisées. Les risques, les répercussions négatives prévues, les sinistres connexes et les dommages causés par le changement climatique augmentent à chaque étape du réchauffement de la planète (degré de fiabilité très élevé)¹⁰.

La hausse des températures est associée à un changement généralisé des régimes climatiques, notamment à une augmentation des phénomènes météorologiques extrêmes. Au cours du premier semestre 2023, de violents orages convectifs ont entraîné des sinistres assurés estimés à au moins 35 milliards de dollars américains. Parmi ces risques météorologiques, les États-Unis ont enregistré pas moins de 812 tornades, mais la grêle a été la principale cause de dégâts au pays. La National Oceanic and Atmospheric Administration (NOAA) des États-Unis a enregistré au moins 729 cas de grêlons de plus de 5,1 cm de diamètre. Bien que les États-Unis aient représenté 76 % des sinistres assurés mondiaux liés aux catastrophes naturelles, ils sont loin d'être le seul pays à être confronté à des phénomènes météorologiques extrêmes. En Allemagne et en France, par exemple, les orages de juin 2023 ont entraîné des frais d'assurance de plus d'un milliard de dollars américains¹¹.

Au premier semestre 2023, les États-Unis avaient enregistré

76% de tous les sinistres assurés mondiaux liés aux catastrophes naturelles.

La grêle a été la principale cause de dommages.



Les sécheresses provoquées par des températures record ont également frappé l'Amérique du Nord et l'Europe, créant des conditions propices aux feux de forêt dans de nombreux pays. Si le lien entre sécheresse et augmentation du risque de feux de forêt est bien connu, les sécheresses peuvent aussi aggraver la pénurie d'eau existante, obligeant ainsi les autorités locales à prendre des mesures importantes pour restreindre ou interdire l'utilisation de l'eau afin de préserver les ressources pour des fonctions essentielles, telles que les soins de santé, l'accès à l'eau potable et la lutte contre les incendies. Dans de nombreux cas, les autorités locales choisissent de limiter les essais des équipements de protection contre les incendies, tels que les systèmes d'extinction automatique et les pompes de suppression, essentiels au maintien de la fiabilité et à l'identification des problèmes dans ces systèmes de protection contre les incendies et systèmes de sécurité des personnes.

Les phénomènes météorologiques extrêmes, intensifiés par la hausse des températures, continueront de menacer les activités et les chaînes d'approvisionnement des entreprises, et les chefs d'entreprise doivent donc s'organiser en conséquence.

¹⁰ GIEC (2023) : AR6 Synthesis Report: Climate Change 2023. En ligne : <https://www.ipcc.ch/report/sixth-assessment-report-cycle/>

¹¹ GALLAGHER RE (2023) : H1 2023 Natural Catastrophe Report – Preliminary Overview. En ligne : <https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/natural-catastrophe-report-2023-h1.pdf>



Cybersécurité

Chaque jour, les cyberattaques deviennent plus fréquentes, plus complexes et plus coûteuses. Les groupes criminels organisés, les États et les individus mal intentionnés continuent de tirer profit de celles-ci, souvent sans conséquences. Environ le quart des incidents de cybersécurité sont liés à des logiciels de rançon, les trois principaux vecteurs d'action étant les courriels, les logiciels de partage de bureau et les applications Web¹². Les individus mal intentionnés cherchent continuellement de nouvelles façons de mener des cyberattaques et de monétiser des entreprises vulnérables, en trouvant des méthodes complexes et créatives pour obtenir des données d'accès ou en utilisant l'ingénierie sociale telle que le piratage afin d'acheminer des fonds vers un compte criminel.

« Si certains adversaires (pirates informatiques) utilisent des techniques et outils avancés, la plupart d'entre eux profitent de vulnérabilités non corrigées, d'une mauvaise hygiène informatique ou d'une incapacité des entreprises à mettre en œuvre des technologies essentielles telles que l'authentification multifactorielle (AMF). Malheureusement, trop peu d'entreprises comprennent l'importance de l'AMF avant d'être victimes d'une violation ».

Jen Easterly, directrice de la Cybersecurity and Infrastructure Security Agency des États-Unis

1/4 des incidents de cybersécurité sont le fruit de **logiciels de rançon**. Les principaux vecteurs d'action sont les suivants :



Courriel



Logiciel de partage



Application Web

L'objectif des cyberattaquants n'est pas nécessairement de voler des données, mais d'empêcher les entreprises de fonctionner, en prenant leurs données ou leurs ressources en otage jusqu'au paiement d'une rançon. Les cryptomonnaies sont un facteur qui leur permet d'atteindre leur but, car elles sont difficiles à tracer et ne respectent pas les frontières internationales et le droit bancaire. En août 2023, plus de 9 500 cryptomonnaies étaient en circulation, et leur capitalisation boursière totale dépassait 1 000 milliards de dollars américains¹³.

Les mesures réglementaires visant à freiner cette cyberactivité illégale et le paiement de rançons n'ont pas empêché la prolifération de la cybercriminalité. Les législateurs ont fait des progrès en exigeant que

les bourses de cryptomonnaies se conforment aux lois du Bureau du contrôle des avoirs étrangers (OFAC) et de celles contre le blanchiment d'argent dans certains pays. Le Congrès des États-Unis ainsi que quelques États ont proposé d'imposer des restrictions sur les paiements de logiciels de rançon afin d'améliorer les rapports sur la cybercriminalité et d'identifier, de capturer et de fermer les réseaux criminels grâce auxquels ces cyberattaques se poursuivent et dont les dommages punitifs sont limités ou inexistant¹⁴.

À mesure que la cybercriminalité prend de l'ampleur et évolue, toutes les entreprises sont menacées, quels que soient leur taille, leur emplacement ou leur secteur d'activité.

¹² VERIZON (2023) : 2023 Data Breach Investigations Report. En ligne : <https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf>.

¹³ COINMARKETCAP (2023) : Cryptocurrency Prices, Charts and Market Capitalizations. Consulté le 10 août 2023, en ligne : <https://coinmarketcap.com/>.

¹⁴ BRUMFIELD, Cynthia (2021) : « Four states propose laws to ban ransomware payments », CSO, 28 juin 2021. En ligne : <https://www.csoonline.com/article/3622888/four-states-propose-laws-to-ban-ransomware-payments.html>



Attentes en matière de facteurs environnementaux, sociaux et de gouvernance (ESG)

Les intérêts des investisseurs, de la clientèle et de la main-d'œuvre continuent de favoriser les entreprises qui fournissent des informations sur la façon dont elles gèrent les risques et élaborent des stratégies d'affaires pour traiter les questions relatives aux facteurs ESG.

Ces derniers comprennent notamment :



Les sujets environnementaux liés à la manière dont les entreprises gèrent les émissions de carbone, les ressources naturelles, la pollution et la gestion des déchets, et utilisent les technologies et la construction vertes.



Les thèmes sociaux, tels que la manière dont les entreprises gèrent les normes de travail et les celles des fournisseurs, assurent la santé et la sécurité des personnes (employés, consommateurs, communautés), soutiennent les services de santé et de nutrition aux échelles locale et internationale.



Les thèmes de gouvernance, tels que le partage de la façon dont les organisations soutiennent l'éthique, la conformité, la lutte contre la corruption, les dépenses et la reddition de comptes.

Les organismes de l'Union européenne et du Royaume-Uni avancent avec précaution dans l'élaboration de mandats réglementaires visant à normaliser les rapports de divulgation sur les facteurs ESG afin de corroborer

les affirmations à ces derniers, de promouvoir des pratiques commerciales responsables et de permettre aux consommateurs ainsi qu'aux investisseurs de prendre des décisions plus éclairées. La Commission européenne a adopté

la Corporate Sustainability Reporting Directive (la « CSRD »), qui entrera en vigueur à partir du 1^{er} janvier 2024 et exigera des grandes entreprises qu'elles publient un rapport sur les facteurs ESG standard en janvier 2025 sur les données de l'année écoulée¹⁵. Les renseignements sur les facteurs ESG devront être dévoilés dans les rapports annuels, dans un format précis, et en suivant une présentation spécifique des informations, et une assurance sera fournie dans le cadre d'un audit externe¹⁶. Les États-Unis sont pour leur part en retard par rapport à l'Union européenne et le Royaume-Uni dans leurs tentatives de réglementation des facteurs ESG.

Dans son programme de 2023, la U.S. Securities and Exchange Commission (SEC) des États-Unis a fixé des dates pour finaliser 29 règles et proposer 23 autres amendements relatifs à la divulgation d'informations et au rapport sur les facteurs ESG¹⁷. Les législateurs des États ont commencé à élaborer leurs propres réglementations pour ou contre les exigences en matière de rapports sur les facteurs ESG. Les États à majorité républicaine s'efforcent de

minimiser ou d'exclure les considérations liées aux facteurs ESG des décisions de financement, tandis que les États à majorité démocrate élaborent des politiques favorables aux facteurs ESG. Le Forum sur la gouvernance d'entreprise de la Faculté de droit de Harvard s'attend à ce que les gouvernements des États continuent de créer des lois axées sur les facteurs ESG à l'approche de l'élection présidentielle américaine de 2024¹⁸. En mars 2023, au moins sept États ont adopté des lois ou des déclarations de politique générale visant à empêcher ou à décourager les entreprises publiques de prendre en compte les facteurs ESG lorsqu'elles investissent des ressources étatiques¹⁹.

Dans la mesure où les entreprises assujetties aux normes relatives au rapport sur les facteurs ESG peuvent être exposées à des risques d'atteinte à leur réputation si elles ne s'y conforment pas en temps opportun, elles doivent investir dans les ressources nécessaires pour comprendre l'évolution des exigences et fournir des informations exactes.

¹⁵ KPMG (n/a) : « Corporate Sustainability Directive ». En ligne : <https://kpmg.com/nl/en/home/topics/environmental-social-governance/corporate-sustainability-reporting-directive.html>

¹⁶ KPMG (n/a) : « Corporate Sustainability Directive ». En ligne : <https://kpmg.com/nl/en/home/topics/environmental-social-governance/corporate-sustainability-reporting-directive.html>

¹⁷ ACA (2023) : « The SEC Plans to Finalize ESG-Related Rules in 2023 ». En ligne, 17 janvier 2023 : <https://www.acaglobal.com/insights/sec-plans-finalize-esg-related-rules-2023>

¹⁸ MALONE, Leah, HOLLAND, Emily, HOUSTON, Carolyn et al. (2023) : « ESG Battlegrounds: How the States Are Shaping the Regulatory Landscape in the U.S. », Harvard Law School Forum on Corporate Governance. En ligne : [ESG Battlegrounds: How the States Are Shaping the Regulatory Landscape in the U.S. \(harvard.edu\)](https://www.harvardlawjournal.org/article/ESG-Battlegrounds-How-the-States-Are-Shaping-the-Regulatory-Landscape-in-the-U.S.-1)

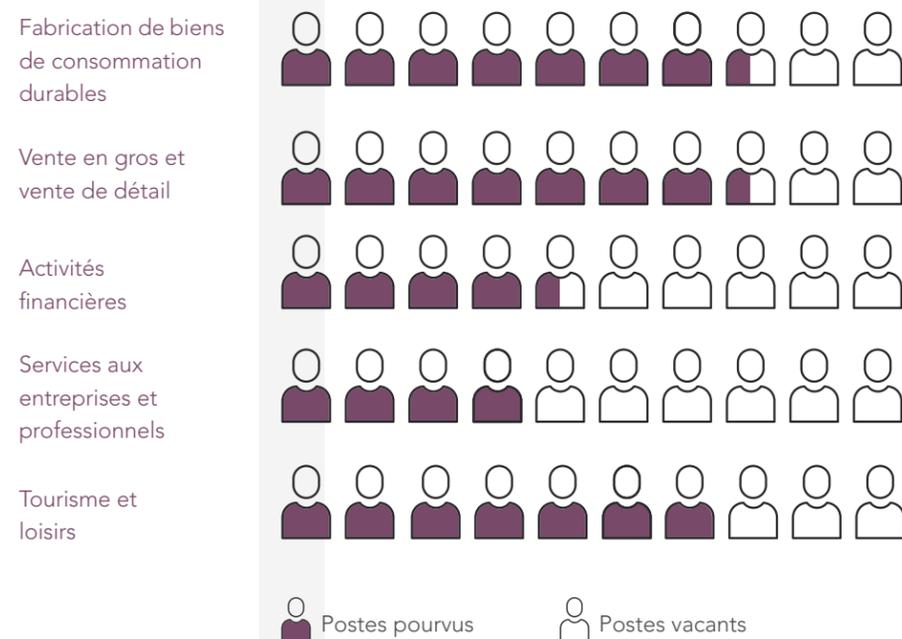
¹⁹ MALONE, Leah, HOLLAND, Emily, HOUSTON, Carolyn et al. (2023) : « ESG Battlegrounds: How the States Are Shaping the Regulatory Landscape in the U.S. », Harvard Law School Forum on Corporate Governance. En ligne : [ESG Battlegrounds: How the States Are Shaping the Regulatory Landscape in the U.S. \(harvard.edu\)](https://www.harvardlawjournal.org/article/ESG-Battlegrounds-How-the-States-Are-Shaping-the-Regulatory-Landscape-in-the-U.S.-1)



Évolution du travail

L'évolution et la fidélisation de la main-d'œuvre sont des éléments essentiels à prendre en compte pour les chefs d'entreprise d'aujourd'hui. La pandémie de la COVID-19 a entraîné une augmentation des retraites anticipées et une réduction de l'immigration, créant ainsi une pénurie de main-d'œuvre aux États-Unis. La Chambre de commerce a estimé à 1,9 million le nombre de citoyens américains en moins au sein de la population active à l'heure actuelle par rapport à février 2020²⁰.

Pénurie de main-d'œuvre par secteur d'activité (juillet 2023)²¹



Certains ménages se sont adaptés à un mode de vie à revenu unique en raison de l'augmentation des coûts des services de garde, de l'alimentation et des services publics²². En juin 2023, 10,1 millions de postes étaient vacants aux États-Unis et un peu plus de 5,7 millions de personnes étaient susceptibles d'avoir besoin d'un emploi²³.

Le monde professionnel d'aujourd'hui, en « télétravail », est très différent de celui d'avant la pandémie. De nombreuses entreprises ayant tenté d'imposer un retour au bureau se sont heurtées à un fort mécontentement de leur personnel²⁴. Les tours de bureaux en centre-ville étaient auparavant le cœur des activités, mais le commerce s'est déplacé dans les quartiers. Bon nombre d'entre elles affichent donc des taux d'inoccupation élevés et leur valeur diminue²⁵.

Selon une récente étude menée par Gallup, les trois quarts des Américains prévoient de chercher un nouvel

emploi en 2023, et les éléments qu'ils prennent en compte peuvent différer de celles des travailleurs du passé. Un sondage de Gallup révèle que les millénariaux et les membres de la génération Z se concentrent davantage sur la qualité de vie et le bien-être, et que plus de la moitié des travailleurs américains ont procédé à des changements ayant entraîné une diminution de leurs revenus ou une stabilisation de ces derniers afin d'améliorer leur mode de vie et leur carrière²⁶.

Dans un contexte de recrutement et de fidélisation du personnel hautement concurrentiel, les entreprises doivent envisager des stratégies novatrices en matière de ressources humaines dans le but de conserver leur personnel actuel et d'attirer des candidats qualifiés. Dans le même temps, l'augmentation du nombre de postes vacants peut favoriser la réduction des frais immobiliers et des frais généraux.

²⁰ U.S. CHAMBER OF COMMERCE (n/a) : America Works Data Center. En ligne : <https://www.uschamber.com/workforce/america-works-data-center>

²¹ U.S. CHAMBER OF COMMERCE (n/a) : America Works Data Center. En ligne : <https://www.uschamber.com/workforce/america-works-data-center>

²² U.S. CHAMBER OF COMMERCE (n/a) : America Works Data Center. En ligne : <https://www.uschamber.com/workforce/america-works-data-center>

²³ GUILFORD, Gwynn (2023) : « Get Ready for the Full-Employment Recession », The Wall Street Journal, 3 juin 2023. En ligne : <https://www.wsj.com/articles/get-ready-for-the-full-employment-recession-bc9937a5>

²⁴ GRANT, Peter (2023) : « A New CEO Says Employees Can't Work Remotely After All, and They Revolt », The Wall Street Journal, 6 juin 2023. En ligne : <https://www.wsj.com/articles/a-new-ceo-says-employees-cant-work-remotely-after-all-and-they-revolt-8113539J>

²⁵ PUTZIER, Konrad (2023) : « Distress in Office Market Spreads to High-End Buildings », The Wall Street Journal, 28 mars 2023. En ligne : https://www.wsj.com/articles/distress-in-office-market-spreads-to-high-end-buildings-cladad48?mod=article_inline

²⁶ FEILER, Bruce (2023) : « The New Rules of Success in a Post-Career World », The Wall Street Journal, 2 juin 2023. En ligne : <https://www.wsj.com/articles/the-new-rules-of-success-in-a-post-career-world-3e54b343.c>

METTRE EN PLACE DES COUVERTURES STRATÉGIQUES

Dans la mesure où elle aide les entreprises à transférer les risques et à assurer leur résilience financière après des incidents perturbateurs, l'assurance est un élément essentiel de tout programme de résilience des entreprises efficace. La forte concurrence pour des ressources limitées, combinée à un contexte difficile en matière de risque opérationnel, oblige les entreprises à examiner attentivement de nombreux facteurs lorsqu'elles choisissent leur couverture.

Une étude récente sur l'évaluation des propriétés a révélé qu'à la suite de l'inflation de l'ère pandémique, qui a atteint son plus haut niveau depuis 40 ans, 68 % des bâtiments évalués entre 2020 et 2021 étaient sous-assurés d'au moins 25 %, et près de 90 % des bâtiments évalués l'étaient en deçà de leur valeur réelle¹. Les entreprises et les courtiers d'assurance travaillent avec des compagnies d'assurance comme CNA pour aider les entreprises à évaluer avec exactitude leurs propriétés, mais aussi à évaluer et à atténuer les risques liés à celles-ci, à la responsabilité civile et à la cybersécurité.

¹ WRIGHT, Alex (2023) : « Underinsured Properties Are Crushing Reinsurers. Why Proper Valuations Will Be a Focus for Years to Come », Risk & Insurance, 8 mars 2023. En ligne : <https://riskandinsurance.com/underinsured-properties-are-crushing-reinsurers-why-proper-valuations-will-be-a-focus-for-years-to-come/>.

Pertes d'exploitation

En fonction de la gravité de l'impact et de la complexité des opérations, des semaines, des mois voire des années peuvent être nécessaires pour redémarrer des activités après un incident perturbateur. L'assurance contre les pertes d'exploitation permet aux entreprises assurées de stabiliser leur situation financière et de couvrir les dépenses courantes pendant la reprise.

La Couverture extension de la période

d'indemnisation apporte un soutien financier au-delà de la période de restauration, en couvrant les pertes de revenus continus tirés d'une entreprise et en aidant au rétablissement de la capacité de vente avant sinistre.



Mesures à envisager :

1. Procédez à une évaluation annuelle pragmatique de l'évolution des dépenses et revenus prévus sur des périodes de 12 et de 24 mois au moment de choisir vos couvertures.
2. Évaluez l'impact sur les revenus de chaque site de votre entreprise à l'aide d'un scénario de sinistre «perte totale» pour comprendre les limites financières potentielles de celle-ci. Cette évaluation permet également d'identifier les activités précises du site pour lesquelles la gestion des risques et la planification de la continuité des activités peuvent être priorisées et ainsi fournir le meilleur retour sur investissement.
3. Examinez votre capacité à payer et à fidéliser votre personnel déplacé pendant la période de redressement économique prolongée, et envisagez fortement d'inclure les salaires ordinaires dans la couverture des dépenses continues afin de conserver votre personnel pendant cette période.

La Couverture revenu d'entreprise

permet de récupérer un revenu net et d'effectuer les dépenses courantes telles que le versement des salaires, le paiement des loyers et des services pendant la reprise.



Mesures à envisager :

1. Estimez les besoins les fonds dont chaque site de votre entreprise aura besoin pour obtenir des ressources de récupération (relocalisation temporaire, entrepôts de récupération, frais d'expédition supplémentaires, par exemple) lorsqu'un incident nuit aux activités.
2. Estimez les besoins en main-d'œuvre contractuelle ou temporaire ainsi que les coûts quotidiens et hebdomadaires qui y sont associés pour soutenir la reprise des activités touchées. Ces coûts incluent le personnel supplémentaire nécessaire pour aider la reprise et le redémarrage des activités perturbées.
3. Tenez compte des points susmentionnés au moment de l'évaluation des couvertures appropriées en matière de perte de temps et de revenus.

La Couverture frais supplémentaires

alloue des fonds pour réduire la durée de redressement économique des entreprises et l'impact des pertes au cours de la phase de reprise, si les circonstances le permettent.



Mesures à envisager :

1. Identifiez les emplacements de votre entreprise où une interruption prolongée des activités pourrait entraîner une perte substantielle de revenus liés aux produits et services de l'entreprise. Ces activités peuvent être, par exemple, un centre de traitement des données faisant partie intégrante des activités de l'entreprise, une unité de production principale ou un entrepôt où sont entreposés des équipements essentiels ou des produits finis.
2. Estimez, pour chacun des sites de votre entreprise, le temps nécessaire pour que le volume des ventes redevienne celui qu'il était avant l'interruption, et ce, une fois que les activités touchées reprennent leur cours normalement comme avant l'incident.
3. Tenez compte des points susmentionnés au moment de l'évaluation des couvertures appropriées en matière de temps et de revenus.

Cybersécurité

Aucune entreprise n'est à l'abri des cybercriminels. Même si des contrôles rigoureux sont mis en place pour limiter les atteintes à la sécurité, les données ou le réseau peuvent être touchés par une attaque. En 2022, les activités des courtiers en matière de cybercriminalité ont augmenté de 112 %, en raison de cybercriminels s'introduisant dans les entreprises afin de vendre ou d'offrir les accès non autorisés à d'autres individus mal intentionnés tels que des opérateurs de logiciels de rançon².



Mesures à envisager :

1. Travaillez avec votre courtier d'assurance pour établir les couvertures appropriées telles que des couvertures en matière de défaillance de réseau, de perte de revenus liés tirés d'une entreprise, de collecte injustifiée, de vol et de piratage psychologique.
2. Mettez en œuvre un cadre de cybersécurité afin d'identifier et de détecter les attaques, de s'en protéger, d'y répondre et de s'en remettre.



Pour en savoir plus sur les tendances en matière de cybersécurité et d'approches de gestion des risques, [écoutez la troisième saison du balado e-Talks de CNA consacré au contrôle des risques.](#)

Responsabilité civile

L'assurance responsabilité civile des entreprises protège ces dernières de la responsabilité financière en cas de dommages corporels ou matériels qui surviennent dans le cadre de leurs activités quotidiennes. Elle paie les frais de défense d'une entreprise et indemnise celle-ci pour les sinistres subis (sous réserve des conditions de la police d'assurance). L'exposition des entreprises aux risques liés à la responsabilité civile ne cesse d'augmenter partout dans le monde, ce qui se traduit par une hausse notable de litiges et de verdicts des tribunaux.



Mesures à envisager :

1. Effectuez une évaluation des risques à l'échelle de l'entreprise afin de comprendre l'exposition de celle-ci aux risques liés à la responsabilité civile et de mettre en place des contrôles (accès sécurisé, déneigement ou déglçage, etc.) pour réduire au minimum les incidents qui pourraient survenir dans vos locaux.
2. Travaillez avec votre courtier d'assurance pour comprendre les tendances en matière de responsabilité civile (intérêts émergents, services liés aux dommages et aux suivis des litiges, par exemple)³.
3. Transférez le risque dans la mesure du possible en imposant des exigences contractuelles en matière d'indemnisation et d'assurance pour toutes les tierces parties impliquées dans vos activités.



² WRIGHT, Alex (2023) : « Underinsured Properties Are Crushing Reinsurers. Why Proper Valuations Will Be a Focus for Years to Come », Risk & Insurance, 8 mars 2023. En ligne : <https://riskandinsurance.com/underinsured-properties-are-crushing-reinsurers-why-proper-valuations-will-be-a-focus-for-years-to-come/>.

³ DENGLER, Meghan (2021) : « Praedicat's Emerging Risk Scenario Platform », Praedicat, 14 avril 2021. En ligne : <https://www.praedicat.com/praedicats-emerging-risk-scenario-platform/>.



Bris d'équipement

L'assurance contre les bris d'équipement (dans le cadre d'une assurance dommages ou à titre de police d'assurance indépendante) couvre la réparation ou le remplacement d'équipement en cas de dommages matériels ainsi que la perte de revenus connexes tirés d'une entreprise et découlant d'un bris mécanique ou d'équipement, selon les conditions de la police d'assurance.



Mesures à envisager :

1. Établissez les exigences de la couverture en identifiant les points de vulnérabilité particuliers ou les équipements de grande valeur, qui, s'ils sont compromis, pourraient entraîner une perte importante de revenus tirés de l'entreprise.
2. Mettez en place une maintenance préventive et prédictive robuste des machines comme première ligne de défense pour permettre la continuité des activités.

Dommmages matériels

Les dommages matériels peuvent perturber considérablement les activités et nuire à la rentabilité, surtout si les biens ne sont pas suffisamment assurés. La persistance de l'inflation, la fluctuation des taux

d'intérêt, les perturbations de la chaîne d'approvisionnement ainsi que les pénuries de main-d'œuvre peuvent avoir une incidence supplémentaire sur les dépenses de reconstruction. En raison du changement climatique, la fréquence croissante des phénomènes météorologiques extrêmes en toutes saisons va également continuer de menacer les biens et les propriétés et les chaînes d'approvisionnement partout dans le monde.



Mesures à envisager :

1. Examinez la valeur de vos biens et les coûts de remplacement réels au moins une fois par année afin de vous aligner sur l'inflation et les conditions de la chaîne d'approvisionnement.
2. Veillez à ce que vos stratégies de résilience et vos couvertures d'assurance reflètent les tendances actuelles en matière de risques naturels et de risques d'origine humaine.
3. Identifiez les délais de réparation et de remplacement des biens spécialisés essentiels à la production de revenus (laboratoires, robotique, installations de manutention, par exemple). Pensez à la couverture des bris d'équipement pour les machines les plus essentielles.
4. Ajustez les couvertures en fonction de l'utilisation actuelle et future des biens. Lorsqu'un bâtiment est inoccupé en raison de facteurs tels que l'organisation du travail à distance, le risque d'incendie et d'infiltration d'eau provenant de sources internes ou externes augmente considérablement.



03 RENFORCER ET AMÉLIORER LA RÉSILIENCE OPÉRATIONNELLE

Une entreprise résiliente fait constamment preuve de prévoyance, d'initiative et de souplesse pour répondre efficacement aux perturbations et aux défis imprévus.

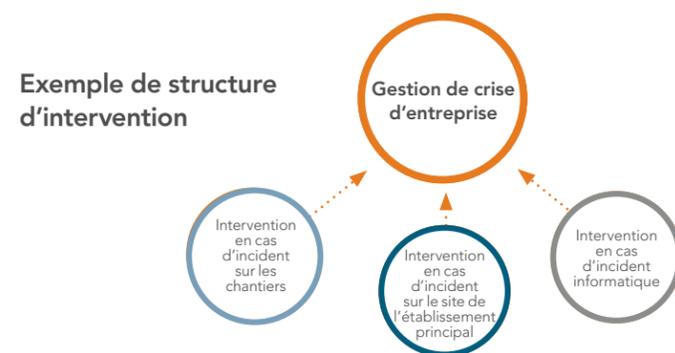
La résilience est soutenue par une gestion globale des risques, associée à des mesures efficaces de redressement et d'adaptation visant à réduire les menaces et à atténuer leur impact sur les activités de l'entreprise.

Gestion du risque d'entreprise

La fonction de gestion du risque est la première ligne de défense pour réduire la probabilité d'incidents perturbateurs et leurs conséquences. Elle prend généralement en compte les risques actuels et émergents, et collabore avec les fonctions opérationnelles appropriées pour mettre en œuvre des plans d'atténuation afin d'éviter ces incidents perturbateurs dans la mesure du possible, ou de réduire le plus possible les conséquences sur l'entreprise. La fonction de gestion du risque surveille également la capacité de l'entreprise à répondre aux incidents, à gérer les crises et à se redresser en cas d'incidents perturbateurs, et supervise souvent les stratégies de transfert du risque (assurance, clauses d'indemnisation des contrats, par exemple) afin de réduire au minimum les conséquences financières.

Capacité d'intervention : un « incident » est un événement susceptible de provoquer une interruption, une perturbation, un sinistre, une situation d'urgence, un désastre ou une catastrophe, et peut se transformer en crise. Chaque seconde compte lorsque votre entreprise est soudainement victime d'une cyberattaque, d'un feu d'installations électriques ou d'une infiltration d'eau dans vos zones de travail critiques. Plus tôt votre entreprise peut intervenir en cas d'incident, traiter les questions de sécurité des personnes et résoudre les problèmes, plus tôt la direction peut maîtriser les conséquences, les messages et les résultats. De nombreux incidents, parmi lesquels les inondations, les feux de forêt et les tornades, touchent habituellement un emplacement précis et ses activités.

Toutefois, certains événements peuvent avoir une portée plus large et exiger la participation de la haute direction pour guider les réponses et superviser les communications. Les plans de réponse aux incidents définissent la structure, l'autorité et les membres de l'équipe requis pour intervenir rapidement en cas d'incident. Plusieurs plans de réponse aux incidents peuvent être nécessaires pour gérer différents sites ou risques. Le plan de gestion des crises de l'entreprise définit les rôles des membres de la haute direction autorisés à diriger les interventions à l'échelle de l'entreprise et à diffuser toutes les communications internes et externes relatives à un incident perturbateur. Certaines polices d'assurance prévoient des garanties pour le recours à des sociétés de relations publiques, qui peuvent être engagées pour soutenir la communication en cas de crise lors d'un incident perturbateur.



Visionnez la vidéo de 3 minutes suivante pour en savoir plus : Améliorer la résilience de votre entreprise



Capacités de reprise : pour mettre en place un cadre de continuité des activités de l'entreprise, qui peut permettre la réparation, le remplacement et le redémarrage de celles touchées, une planification avancée est essentielle. La fonction de gestion de la continuité des activités a pour but d'élaborer des stratégies et des programmes pour s'assurer que les équipes responsables de la reprise des activités disposent des ressources nécessaires pour poursuivre les processus critiques touchés par un incident perturbateur. L'objectif consiste notamment à élaborer des stratégies à la fois pour les éléments de production interne (tels que la main-d'œuvre, l'équipement, les installations, les matériaux et la technologie) et pour ceux de la chaîne d'approvisionnement, notamment les fournisseurs, les distributeurs et la clientèle.



Facteurs clés de succès pour renforcer la résilience

Parrainage de la direction. La haute direction doit comprendre que les structures d'intervention et de reprise, lorsqu'elles sont bien mises en œuvre, peuvent donner un avantage concurrentiel important. Elles exigent des ressources et un soutien à toutes les échelles de l'entreprise pour appuyer les activités de préparation et leur donner la priorité.

Responsabilité. Bien que souvent négligée, la mise en place d'une politique et d'un comité directeur sur la résilience des entreprises est un élément important. Un comité directeur sur la résilience des entreprises se compose d'une équipe interfonctionnelle qui encourage le développement, l'exercice et la capacité de surveillance de la résilience des entreprises. La politique sur la résilience doit quant à elle décrire l'objectif, la portée, les définitions clés ainsi que les rôles responsables de la création et du maintien des équipes et des programmes mis en place pour gérer les efforts d'intervention et de reprise d'une entreprise.

Amélioration continue. La résilience des entreprises est un voyage et non une destination. Passer en revue et répéter les stratégies et les programmes mis en place en utilisant les scénarios envisagés est essentiel au moins une fois par année dans le cadre d'un exercice de table ou sous une autre forme. Ainsi, les responsables et membres désignés sont préparés à mobiliser immédiatement leurs équipes d'intervention et de reprise en cas d'incident perturbateur. L'activation d'un plan de réponse à un incident perturbateur remplace le besoin d'effectuer un exercice. En outre, procéder à un examen après action (AAR) est primordial après chaque activation de plan ou chaque exercice, afin d'affiner le plan d'intervention et d'améliorer les performances des équipes.

Visionnez la vidéo de 3 minutes suivante pour en savoir plus : Valeur de la résilience stratégique des entreprises.



Avantages du renforcement de la résilience pour les entreprises

Éviter l'impact du risque

Réduire les sinistres

Assurer les parties prenantes

Développer le leadership

Accroître la sensibilisation aux risques

Répondre plus efficacement

Se redresser plus rapidement

Maturité du programme de résilience des entreprises

L'amélioration de la résilience des entreprises commence par une évaluation honnête de la position actuelle d'une entreprise et par l'identification de sa place actuelle sur l'échelle de maturité des programmes concernant la mise en place d'une capacité de résilience holistique et coordonnée.

Visionnez la vidéo de 3 minutes suivante pour en savoir plus :
Évaluez votre capacité de résilience.



Quel est le degré de maturité de votre programme de résilience ?

Informel

Structure d'intervention et de reprise créée au moment de l'incident perturbateur.

Défini

Structure d'intervention et de reprise avec mise en place de rôles et de plans d'action

Établi

Plans d'intervention et de reprise et mise en place d'équipes avec formation régulière et exercices.

Géré

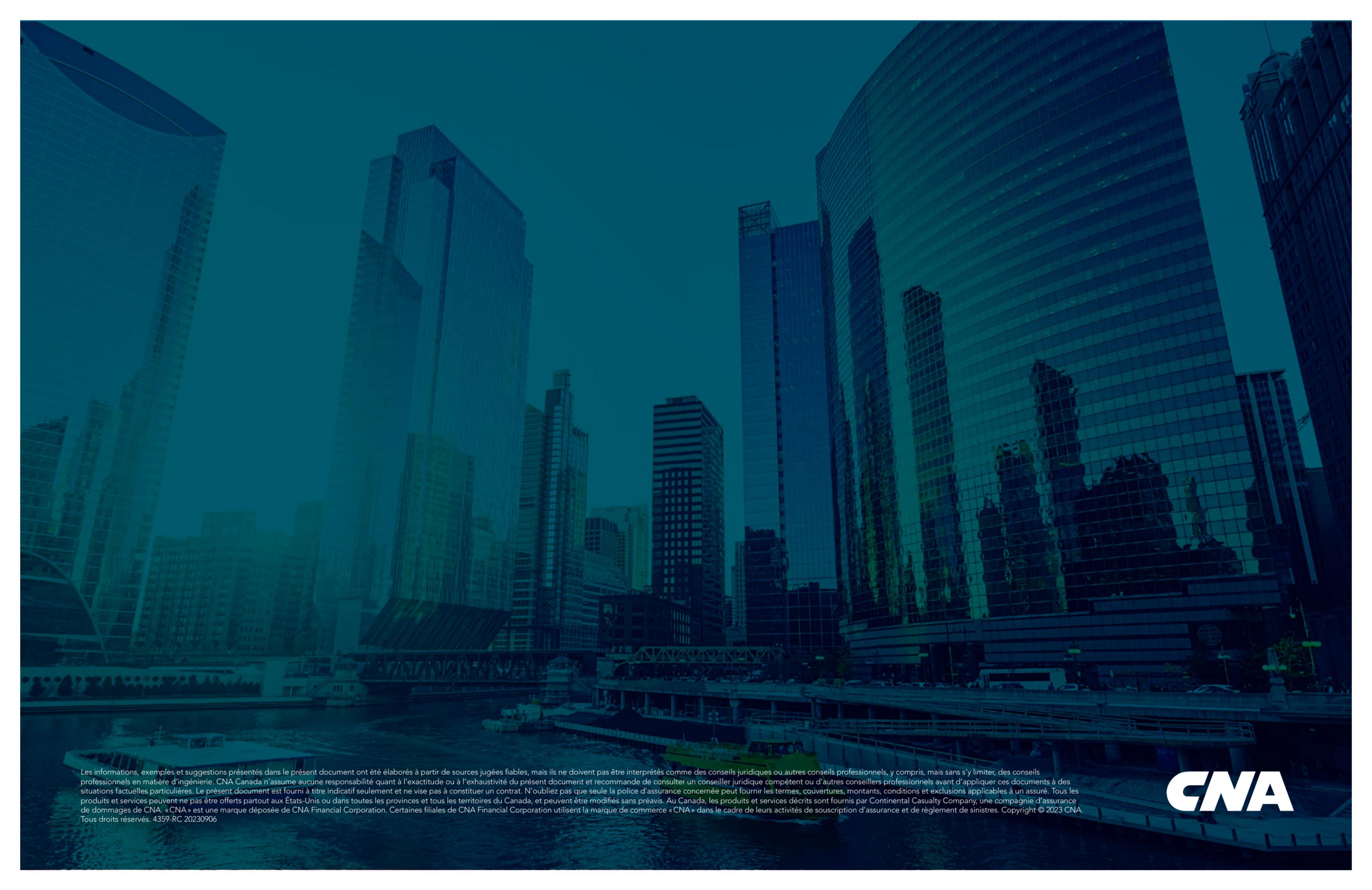
Plans d'intervention et de reprise et activités d'équipe tracées, surveillées et améliorées.

Optimisé

Un état d'esprit résilient stimule la stratégie d'entreprise et des capacités d'intervention continue.

Dans ce contexte de risque complexe, les entreprises doivent continuellement relever des défis nouveaux et en constante évolution, tout en s'efforçant de réussir. Pour les hauts dirigeants, l'intégration de couvertures stratégiques qui améliorent les capacités de réponse et de reprise est un élément essentiel de la gestion des risques d'entreprise. Une meilleure préparation, facilitée par des exercices de formation à l'intention des dirigeants et des membres de leurs équipes et combinée à une surveillance étroite des capacités de résilience, renforce et accroît la résilience des entreprises. Les courtiers et les assureurs peuvent aider à élaborer des stratégies de transfert de risques stratégiques qui permettent aux entreprises de renforcer leur résilience financière et opérationnelle.

Pour en savoir plus sur la gestion des risques et l'amélioration de l'efficacité, visitez le site Internet cna.com/riskcontrol.



Les informations, exemples et suggestions présentés dans le présent document ont été élaborés à partir de sources jugées fiables, mais ils ne doivent pas être interprétés comme des conseils juridiques ou autres conseils professionnels, y compris, mais sans s'y limiter, des conseils professionnels en matière d'ingénierie. CNA Canada n'assume aucune responsabilité quant à l'exactitude ou à l'exhaustivité du présent document et recommande de consulter un conseiller juridique compétent ou d'autres conseillers professionnels avant d'appliquer ces documents à des situations factuelles particulières. Le présent document est fourni à titre indicatif seulement et ne vise pas à constituer un contrat. N'oubliez pas que seule la police d'assurance concernée peut fournir les termes, couvertures, montants, conditions et exclusions applicables à un assuré. Tous les produits et services peuvent ne pas être offerts partout aux États-Unis ou dans toutes les provinces et tous les territoires du Canada, et peuvent être modifiés sans préavis. Au Canada, les produits et services décrits sont fournis par Continental Casualty Company, une compagnie d'assurance de dommages de CNA. «CNA» est une marque déposée de CNA Financial Corporation. Certaines filiales de CNA Financial Corporation utilisent la marque de commerce «CNA» dans le cadre de leurs activités de souscription d'assurance et de règlement de sinistres. Copyright © 2023 CNA. Tous droits réservés. 4359-RC 20230906

CNA