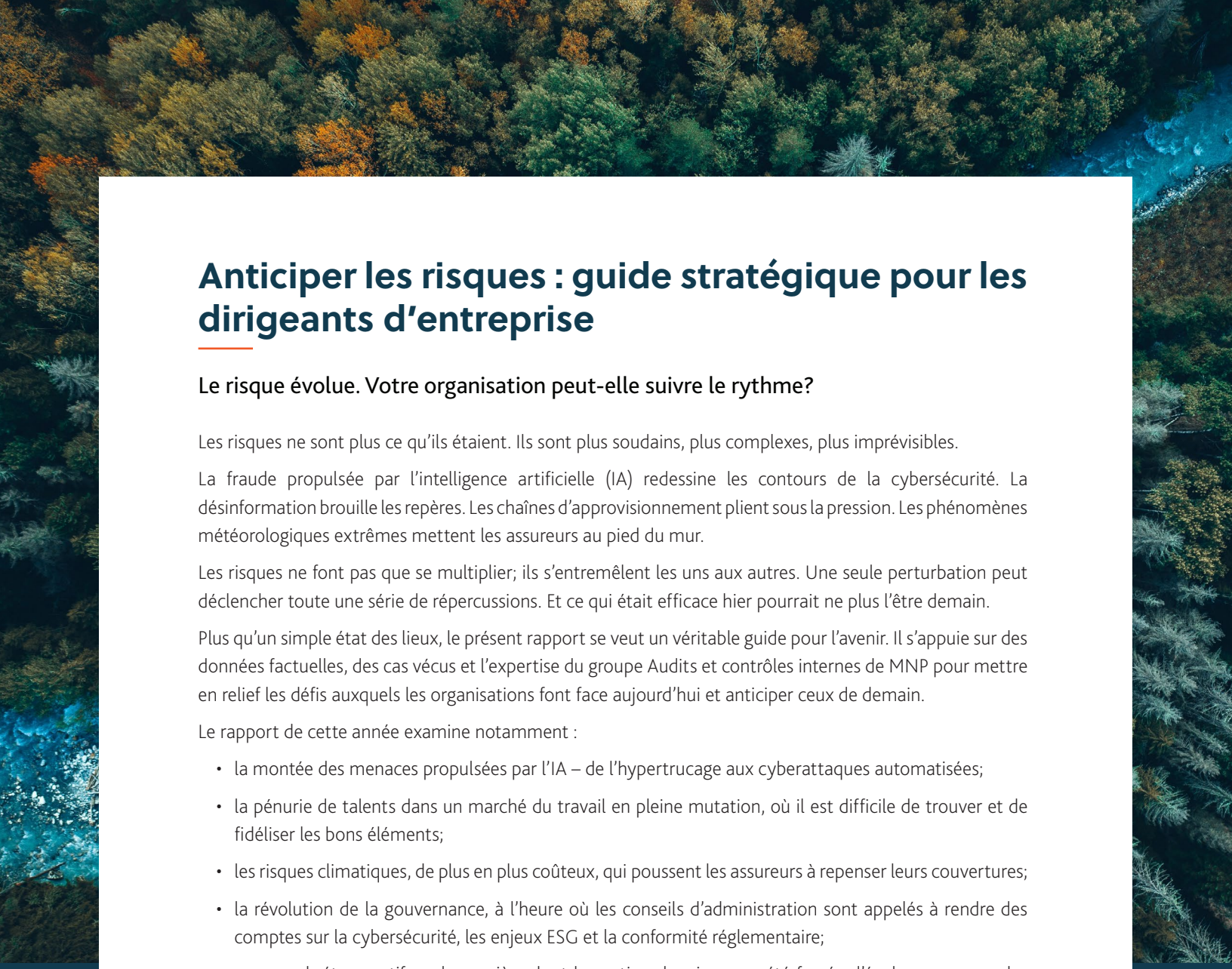
Les risques : tendances pour 2026 et par la suite

Comprendre les risques dans un monde d'incertitude et de changements sans précédent

MNP.ca

Table des matières



Anticiper les risques : guide stratégique pour les dirigeants d'entreprise

Le risque évolue. Votre organisation peut-elle suivre le rythme?

Les risques ne sont plus ce qu'ils étaient. Ils sont plus soudains, plus complexes, plus imprévisibles.

La fraude propulsée par l'intelligence artificielle (IA) redessine les contours de la cybersécurité. La désinformation brouille les repères. Les chaînes d'approvisionnement plient sous la pression. Les phénomènes météorologiques extrêmes mettent les assureurs au pied du mur.

Les risques ne font pas que se multiplier; ils s'entremêlent les uns aux autres. Une seule perturbation peut déclencher toute une série de répercussions. Et ce qui était efficace hier pourrait ne plus l'être demain.

Plus qu'un simple état des lieux, le présent rapport se veut un véritable guide pour l'avenir. Il s'appuie sur des données factuelles, des cas vécus et l'expertise du groupe Audits et contrôles internes de MNP pour mettre en relief les défis auxquels les organisations font face aujourd'hui et anticiper ceux de demain.

Le rapport de cette année examine notamment :

- la montée des menaces propulsées par l'IA – de l'hypertrucage aux cyberattaques automatisées;
- la pénurie de talents dans un marché du travail en pleine mutation, où il est difficile de trouver et de fidéliser les bons éléments;
- les risques climatiques, de plus en plus coûteux, qui poussent les assureurs à repenser leurs couvertures;
- la révolution de la gouvernance, à l'heure où les conseils d'administration sont appelés à rendre des comptes sur la cybersécurité, les enjeux ESG et la conformité réglementaire;
- un regard rétrospectif sur la manière dont la gestion des risques a été forcée d'évoluer au cours des dernières décennies.

Ces risques ne surviennent pas en vase clos : leurs effets se combinent, s'additionnent et mettent les entreprises au défi comme jamais. Les dirigeants qui s'en tireront ne seront pas ceux qui réagiront le plus vite, mais ceux qui seront les mieux préparés.

Chez MNP, nous aidons les organisations canadiennes, tant publiques que privées, à anticiper les risques émergents et à transformer l'incertitude en possibilité stratégique.

Ce rapport n'est pas un outil de peur, mais un exercice de prévoyance.

Voyons un peu ce qui nous attend.

Le groupe Audits et contrôles internes de MNP

Une incertitude persistante : pourquoi la gestion des risques doit suivre le mouvement

L'incertitude n'est pas un phénomène passager, mais une nouvelle réalité qui n'est pas près de disparaître.

Ce qui définissait les risques au Canada il y a 10 ou 20 ans n'a plus grand-chose à voir avec la réalité d'aujourd'hui. Et cette évolution exige une nouvelle façon d'aborder la gestion des risques. Des turbulences économiques aux catastrophes climatiques en passant par les cybermenaces, les tarifs douaniers et les tensions géopolitiques, les entreprises canadiennes affrontent une adversité incessante et impitoyable.

La gestion des risques organisationnels est un impératif qui s'est imposé progressivement au début des années 2000, au moment où les entreprises intégraient les technologies numériques et où les scandales financiers se succédaient à la une des médias. Avec l'arrivée des téléphones intelligents, de l'Internet des objets (IdO) et de l'infonuagique dans les années 2010, la prolifération des systèmes interconnectés a brouillé le portrait des risques et forcé l'adoption d'une approche plus agile.

Puis sont arrivées les années 2020

Les années 2020 ont vu naître des transformations d'une ampleur sans précédent. La pandémie de COVID-19 a forcé les organisations à accélérer leur virage numérique, à gérer les ruptures d'approvisionnement et à réorganiser le travail à distance. Le risque a de nouveau gagné en complexité et, tout d'un coup, l'incertitude est devenue la norme.

Les dynamiques à l'œuvre dans la gestion des risques ne cessent de changer et de s'intensifier. L'intelligence artificielle (IA) bouleverse la façon de brasser des affaires dans presque tous les secteurs. Dans ce contexte de changements générationnels – inflation persistante, tensions commerciales, transformation des marchés mondiaux –, la crise économique provoquée par la pandémie apparaît de plus en plus comme un simple prélude.

Dans l'intervalle, les changements climatiques accélèrent la fréquence des catastrophes naturelles. De fait, les 10 pires catastrophes naturelles jamais enregistrées au pays se sont produites au cours de la dernière décennie, selon les données du Bureau d'assurance du Canada. En 10 ans, ces catastrophes ont causé 30 milliards de dollars en pertes assurées, une hausse marquée par rapport à la moyenne annuelle de 2,2 milliards des 10 années précédentes.

Dans le même temps, les pressions sociales et économiques s'accentuent. Selon un rapport publié en 2024 par Banques alimentaires Canada, une personne sur quatre vit désormais sous le seuil de la pauvreté, soit plus du double que ce qu'estime officiellement Statistique Canada. À cela s'ajoute la crise du logement, aggravée par la croissance démographique et la hausse des loyers.

Parallèlement, les entreprises font face à un déferlement de cybermenaces. Selon l'Indice de risque de Travelers Canada, 65 % des dirigeants d'entreprises canadiennes considèrent les cyberrisques comme une préoccupation majeure. Près d'une organisation sur trois a déjà été victime d'une cyberattaque, les entreprises de taille moyenne étant plus vulnérables que les plus petites.

La planification de scénarios devient incontournable.

Des eaux troubles se profilent clairement à l'horizon, mais ces eaux restent navigables – à condition de renoncer aux approches réactives au profit d'une planification de scénarios continue et d'une gestion des risques agile. Cette capacité d'adaptation est déterminante dans un contexte où les risques se superposent : par exemple, une entreprise peut voir sa santé financière fragilisée par les tarifs douaniers au moment même où une cyberattaque paralyse ses systèmes. Pouvoir anticiper, s'adapter et réagir aux changements soudains de manière intégrée n'est plus un simple atout stratégique : c'est une question de survie. En anticipant les scénarios hypothétiques – les fameux « et si » –, les entreprises sont mieux outillées pour réagir plus prestement et avec plus de souplesse face aux risques.

Risques à surveiller

Ralentissement économique : devant les craintes d'une récession, alimentées par les tarifs imposés par les États-Unis, les tensions commerciales et l'incertitude sur les marchés mondiaux, les entreprises évoluent dans un climat d'extrême prudence.

Pénurie de main-d'œuvre : le vieillissement de la population active et l'évolution des attentes des salariés compliquent le recrutement et le maintien en poste des talents.

Cybermenaces : la fréquence et la complexité accrues des cyberattaques (comme l'hypertrucage) appellent à des mesures de cybersécurité renforcées afin de protéger les données sensibles et d'assurer la continuité des services.

Inflation : les effets prolongés de l'inflation se font sentir sur les coûts d'exploitation, le pouvoir d'achat des consommateurs et la compétitivité mondiale.

Perturbations de la chaîne d'approvisionnement : les pressions soutenues sur les chaînes logistiques mondiales, amplifiées par les tarifs douaniers, les tensions géopolitiques et les changements climatiques, menacent la fluidité des approvisionnements et le respect des calendriers.

Changements à la réglementation : les changements apportés aux règles touchant les facteurs ESG, l'intelligence artificielle (IA), les conflits commerciaux et la sécurité des données pourraient entraîner un durcissement des exigences à respecter.

Instabilité géopolitique : les tensions politiques internationales ébranlent les marchés et nuisent au bon déroulement des activités économiques.

Bouleversements technologiques : pour maintenir leur compétitivité dans une économie numérique, les entreprises doivent suivre le rythme soutenu des développements technologiques.

Risques environnementaux : les entreprises doivent intégrer des pratiques responsables et se préparer aux éventuelles transformations des cadres réglementaires et des dynamiques de marché.

Atteintes à la réputation : tout faux pas peut avoir de lourdes conséquences, tant sur le plan opérationnel que financier, d'où l'importance de maintenir une bonne réputation.

Signaux d'alarme

- Des secousses de marché aussi imprévisibles que sans précédent
- La perte de crédibilité de certains gouvernements étrangers, incapables de soutenir leur économie par des politiques fiscales cohérentes
- Des pics inhabituels d'activité cybercriminelle (par exemple, hameçonnage, attaques aux rançongiciels)
- Des mesures tarifaires agressives et d'incessants remaniements exacerbant l'incertitude mondiale

L'IA sans entrave : croissance fulgurante et risques insoupçonnés

L'intelligence artificielle n'est plus un concept futuriste; elle est bien présente et évolue à un rythme que la réglementation peine à rattraper.

Qu'on le veuille ou non, l'IA est là pour de bon : elle révolutionne les différents secteurs d'activité, transforme les processus décisionnels et s'infiltre dans nos vies, parfois même à notre insu. Et cette évolution fulgurante s'accompagne de risques sans précédent.

D'ici 2026, l'IA générera de nouveaux cas d'usage de minute en minute – influençant des domaines aussi variés que l'approbation de prêts hypothécaires, les admissions universitaires, les règlements d'assurance et les décisions d'embauche. Si ces technologies promettent une optimisation des processus et des gains d'efficacité, elles suscitent aussi de nombreuses inquiétudes.

Déjà, des fraudeurs exploitent l'IA pour orchestrer des cyberattaques perfectionnées, concevoir des arnaques par hypertrucage et lancer des campagnes de rançongiciels. Par ailleurs, une dépendance excessive aux décisions fondées sur l'IA soulève d'importants enjeux de transparence, de sécurité et de responsabilité professionnelle. Et les biais de ces systèmes sont déjà bien documentés. Souvent ancrés dans les données employées pour entraîner les modèles, ces biais ne sont pas toujours faciles à repérer ou à corriger une fois le problème détecté.

« Par ailleurs, une dépendance excessive aux décisions fondées sur l'IA soulève d'importants enjeux de transparence, de sécurité et de responsabilité professionnelle.

Comment les Canadiens perçoivent-ils l'IA?

Les entreprises, les travailleurs et les responsables politiques abordent l'IA avec un mélange d'optimisme et de prudence. Voici quelques données révélatrices :

- Un sondage du groupe Peninsula révèle que seulement 10 % des PME utilisent régulièrement des plateformes d'IA générative comme ChatGPT ou Gemini. Leur réserve tient notamment aux enjeux de confidentialité, à la qualité des réponses et aux risques juridiques.
- Selon un sondage mené par l'Autorité canadienne pour les enregistrements Internet (CIRA), 51 % des Canadiens craignent que l'IA propage des faussetés et des contenus hypertruqués.
- En novembre 2024, le gouvernement fédéral a lancé l'Institut canadien de la sécurité de l'intelligence artificielle (ICSIA), un organisme financé à hauteur de 50 millions de dollars, pour s'attaquer aux risques inhérents à l'IA et promouvoir un développement responsable.

Risques à surveiller

Biais et discrimination : les systèmes d'IA peuvent perpétuer certains biais et mener à des décisions discriminatoires dans des domaines comme le recrutement, l'octroi de prêts et les assurances.

Atteintes à la vie privée : les outils propulsés par l'IA peuvent recueillir et analyser d'énormes quantités de données personnelles ou organisationnelles, ce qui soulève de sérieux enjeux de confidentialité.

Cybermenaces : déjà, des cybercriminels se servent d'arnaques par hypertrucage et de logiciels malveillants propulsés par l'IA pour cibler les entreprises et les particuliers.

Suppression d'emplois : si l'IA permet d'automatiser certaines tâches, elle risque aussi d'entraîner des mises à pied, de causer des pénuries de compétences et de creuser les inégalités sociales.

Manque de compréhension : de nombreux modèles d'IA sont si complexes que même leurs concepteurs ne comprennent pas toujours comment ni pourquoi ils produisent certains résultats. Les utilisateurs et utilisatrices sont donc invités à faire preuve de scepticisme envers les mécanismes décisionnels de l'IA et le degré de fiabilité qu'on peut leur accorder.

Militarisation de l'IA : les systèmes d'armement autonomes et les outils de cyberguerre représentent une menace pour la sécurité mondiale, en raison des risques d'usage détourné ou d'escalade involontaire des tensions.

Incertitude réglementaire : des cadres de réglementation de l'IA flous ou changeants peuvent exposer les entreprises à des risques de non-conformité ou freiner leur capacité d'innovation. Les gouvernements peinent tant à suivre le rythme des progrès technologiques que la réglementation risque d'être dépassée avant même d'entrer en vigueur.

Dépendance excessive à l'IA : sans supervision humaine, les décisions prises par l'IA peuvent mener à des erreurs majeures en cas de défaillance technique ou de résultats inexacts. Il peut en résulter des conséquences dramatiques, surtout si la sécurité de certaines personnes est en jeu.

Enjeux liés à la propriété intellectuelle : la question de la titularité des contenus ou des innovations générés par l'IA, ainsi que l'utilisation de données protégées par le droit d'auteur lors de l'entraînement des modèles, soulève des enjeux de nature juridique et éthique.

Préoccupations éthiques et tollé public : le recours à l'IA à des fins éthiquement discutables, telles que la désinformation ou la surveillance de masse, peut porter gravement atteinte à la réputation de votre organisation et renforcer la méfiance du public envers ces technologies.

Signaux d'alarme

- Des biais inexpliqués dans les modèles de recrutement, de tarification ou d'octroi de prêts
- Des cyberincidents alimentés par l'IA, tels que l'hameçonnage, les escroqueries par hypertrucage et les violations de sécurité
- Des perturbations opérationnelles attribuables aux défaillances d'une plateforme d'IA menant à des pertes financières ou à des atteintes à la réputation
- Des allégations de fuite de données personnelles à la suite de la diffusion, volontaire ou non, de renseignements confidentiels par des membres du personnel

Stratégies d'atténuation des risques

- Renforcer la cyberrésilience
- Mettre en place des politiques de gouvernance et de gestion des risques liés à l'IA
- Élaborer des protocoles d'intervention en cas d'attaque par rançongiciel prévoyant notamment des formations et des stratégies de reprise après sinistre
- Renforcer la surveillance exercée par le conseil d'administration
- Procéder à des évaluations périodiques de la cybersécurité et des risques opérationnels liés aux fournisseurs externes et aux sous-traitants
- Améliorer la formation des équipes internes
- Tester en continu les modèles d'IA et valider leurs résultats
- Élaborer des protocoles de surveillance et de conformité liés à l'IA

Questions à se poser

- Vos contrats avec des fournisseurs externes précisent-ils clairement les usages de l'IA qui sont autorisés et ceux qui ne le sont pas?
- Quant à votre propre recours à l'IA, quelles pratiques internes devez-vous dévoiler pour maintenir la confiance du public?
- Quels risques concrets peuvent découler de l'utilisation que vous faites de l'IA?
- Utilisez-vous déjà l'IA pour prendre des décisions soulevant des risques importants? Devez-vous revoir ou cesser cette pratique?
- Comment pouvez-vous vérifier si les résultats produits par l'IA sont fiables ou même vraisemblables?

Cybersécurité 2.0 : gérer les risques critiques du monde numérique

Suivre l'évolution… ou se retrouver sans protection.

Tel est le paradoxe de la cybersécurité : on n'est jamais aussi vulnérable que lorsqu'on croit avoir enfin tout prévu. Si la cybersécurité est un objet de préoccupation constante, la tranquillité d'esprit, elle, demeure un but insaisissable. Car ce qui semblait sûr hier pourrait ne plus l'être aujourd'hui. De fait, les meilleures pratiques actuelles seront cruellement insuffisantes pour faire face aux menaces liées à l'IA qui se profilent à l'horizon.

La vérité, c'est que les cybercriminels ne s'attaquent plus seulement aux données : ils s'en prennent à la confiance même.

Imaginez-vous participer à une réunion virtuelle… pour découvrir ensuite que votre vis-à-vis n'était pas une personne réelle, mais une contrefaçon issue de l'hypertrucage. Comment savoir à qui – ou à quoi – on peut encore faire confiance? Telle est la question dérangeante que les fraudes propulsées par l'IA nous obligent à nous poser.

Qu'il s'agisse d'attaques par rançongiciel qui paralysent vos activités ou de tentatives d'hameçonnage capables de déjouer les filtres classiques, les cybermenaces n'ont jamais été aussi sophistiquées. Nous entrons dans une nouvelle ère : celle de la cybersécurité 2.0, un monde où la vigilance constante, la défense en amont et la détection avancée des menaces sont plus cruciales que jamais.

Évolution alarmante des cybermenaces

Ce que révèlent les chiffres est loin d'être rassurant :

- Selon le Centre de la sécurité des télécommunications Canada (CST), le programme cybernétique financé par la Chine représente la menace la plus sophistiquée et la plus active visant le Canada, et plus particulièrement les entreprises, les institutions publiques et les infrastructures essentielles.
- Selon la vérificatrice générale du Canada, les ménages canadiens ont essuyé plus de 500 millions de dollars de pertes en un an aux mains de cyberfraudeurs – pourtant, seulement 10 % des cybercrimes seraient signalés d'après les estimations des forces de l'ordre.
- Une étude menée par CDW Canada révèle que les cyberattaques sont moins nombreuses, mais de plus en plus efficaces. Selon les données, 43 % des entreprises considèrent la cybersécurité comme une priorité absolue et y consacrent de 5 % à 15 % de leur budget informatique.
- La même étude révèle que 82 % des entreprises disposent désormais d'une cyberassurance, contre 59 % en 2021.
- Le budget fédéral 2024 a alloué 917,4 millions de dollars sur cinq ans au renforcement des cyberopérations et des capacités de renseignement, ainsi qu'à l'établissement d'un Commandement Cyber au sein des Forces armées canadiennes afin de contrer les menaces croissantes.

Risques à surveiller

Évolution des rançongiciels : les cybercriminels recourent à des méthodes sophistiquées de chiffrement et d'extorsion pour cibler des infrastructures essentielles et gonfler le montant des rançons exigées.

Attaques visant la chaîne d'approvisionnement : les cybercriminels exploitent les failles des fournisseurs externes ou des sous-traitants pour infiltrer les systèmes interconnectés.

Cybercriminalité alimentée par l'IA : les pirates informatiques se servent de l'IA pour automatiser les attaques, créer des hypertrucages et concevoir des campagnes d'hameçonnage évoluées, qui sont plus difficiles à détecter.

Vulnérabilités de l'Internet des objets : les appareils connectés sont omniprésents, mais leur faible niveau de sécurité en fait des cibles de choix pour les cybercriminels à la recherche de failles faciles à exploiter.

Menaces internes : les actes malveillants ou involontaires commis à l'interne demeurent une source de préoccupation majeure, surtout dans un contexte de télétravail et de surveillance limitée.

Risques liés à l'infonuagique : la configuration inadéquate des environnements infonuagiques, notamment dans le contexte de la sécurité en nuage multiservice (ou sécurité multinuage), peut exposer les organisations à des fuites de données ou à des accès non autorisés.

Attaques contre les infrastructures essentielles : les cyberattaques visant les réseaux de distribution d'électricité, les systèmes de santé et les institutions financières peuvent entraîner des perturbations majeures à grande échelle.

Attaques du jour zéro : les pirates exploitent les failles sans correctif des logiciels grand public avant que les fournisseurs n'aient le temps d'y remédier.

Atteintes à la confidentialité des données : l'exfiltration de données personnelles ou organisationnelles dans le but de les revendre ou de faire pression demeure l'un des risques les plus répandus et les plus dommageables.

Menaces liées à l'informatique quantique : les percées dans ce domaine pourraient un jour rendre les systèmes de chiffrement traditionnels complètement obsolètes.

Signaux d'alerte

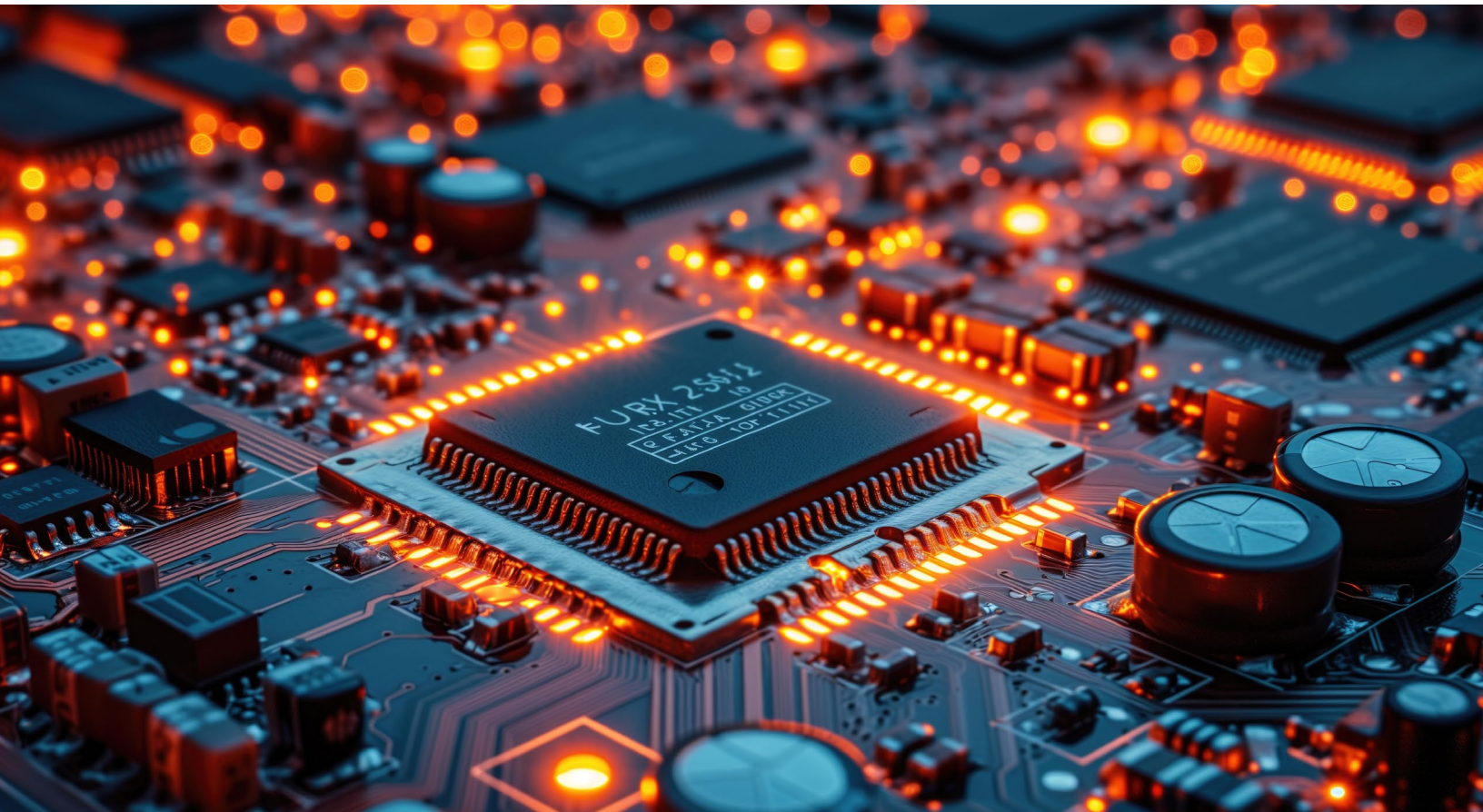
- Toute hausse des tentatives d'hameçonnage, notamment à l'aide de contenus générés par l'IA
- Des activités de connexion anormales ou des demandes d'accès suspectes, détectées depuis des emplacements inhabituels
- Des signalements de fuites internes ou d'activités suspectes de la part de membres du personnel
- Une multiplication des cyberattaques par rançongiciel, assorties de menaces de divulgation publique des données
- Des failles récemment découvertes dans des logiciels grand public, dont le correctif se fait attendre

Stratégies d'atténuation des risques

- Adopter une approche de cybersécurité fondée sur la vérification systématique
- Mettre en place des solutions avancées de détection des menaces
- Rendre l'authentification multifacteur (MFA) obligatoire
- Investir dans la formation continue du personnel
- Appliquer régulièrement les correctifs et mises à jour de sécurité
- Renforcer la gestion des risques liés aux fournisseurs externes
- Définir un plan d'intervention en cas de cyberincident
- Chiffrer les données et effectuer des sauvegardes régulières
- Se préparer à l'arrivée de la cryptographie post-quantique

Questions à se poser

- Votre organisation évalue-t-elle le niveau de confidentialité de chaque réunion? Appliquez-vous des mesures de sécurité accrues pour les rencontres à haut risque, comme le fait de vérifier l'identité des participants et participantes avant une visioconférence?
- Exigez-vous que les membres de votre équipe signalent au service des TI tout incident – professionnel ou privé – susceptible d'impliquer une usurpation d'identité ou une fuite de données personnelles?
- À quelle fréquence votre service des TI organise-t-il des séances de réflexion sur les nouveaux scénarios d'attaque possibles? Comment prévoit-il de renforcer les contrôles face à l'évolution des techniques utilisées par les cybercriminels?
- Votre organisation échange-t-elle ouvertement avec ses homologues du secteur pour rester au fait des nouvelles tactiques utilisées par les cybercriminels et s'accorder le temps nécessaire pour réagir?



Risques liés aux ESG : dompter l'incertitude pour un avenir durable

Il ne s'agit pas d'un simple enjeu de conformité, mais d'un défi d'affaires fondamental.

D'ici 2026, on s'attend à ce que votre entreprise fasse plus que jamais l'objet d'une surveillance étroite de ses efforts de durabilité, de son apport social et de sa transparence sur le plan de la gouvernance.

Même si les stratégies ESG étaient vues au départ comme un chemin vers la responsabilité des entreprises et la résilience à long terme, elles sont en réalité beaucoup plus complexes.

Les investissements ESG ne s'alignent pas toujours sur les rendements des actionnaires, ce qui peut causer de la frustration au sein des conseils d'administration devant des politiques contraignantes (comme le projet de loi C-59), des réglementations changeantes et des hausses de coûts. La transition vers la carboneutralité, un objectif de nombreuses organisations dans les dernières années, a grandement ralenti en raison de budgets plus serrés, de règles complexes et de contraintes liées aux obligations de conformité. À l'échelle mondiale, les maigres efforts de certains, en particulier des pays qui sont de grands émetteurs et qui ralentissent le progrès, ont ajouté à la frustration.

À la fois un risque et une occasion

Seulement en 2024, plus de 3,4 millions d'hectares ont été calcinés par des feux de forêt, celui de Jasper ayant entraîné près de 880 $ millions de dollars de dommages assurés. Des événements de ce type représentent des catastrophes environnementales, mais aussi financières.

Une bonne partie des plus grandes entreprises canadiennes sont toujours en mode rattrapage. Une revue de plus de 250 rapports d'entreprise sur le développement durable a permis de constater que la plupart d'entre elles ne quantifiaient pas financièrement leurs risques climatiques ou n'intégraient pas complètement les facteurs ESG à leurs stratégies.

La question à se poser est la suivante : y a-t-il un risque que les entreprises ne soient pas conformes à ce que propose le projet de loi C-59 ou y a-t-il là une occasion de réécrire ce projet de loi?

L'aspect social

La composante sociale des facteurs ESG constitue un impératif pour les entreprises. La façon dont les organisations répondent aux attentes du public, des communautés et de la société fait l'objet d'une surveillance de plus en plus serrée.

Les droits autochtones et la réconciliation demeurent un enjeu de grande importance au Canada. Les entreprises qui exercent leurs activités sur des terres autochtones ou à proximité de celles-ci doivent bien gérer les risques en lien avec l'utilisation des terres, la conservation de la culture et la confiance. Au-delà de la conformité, la concertation et les partenariats avec les communautés autochtones représentent une condition élémentaire aux yeux des organismes de réglementation, mais aussi du public.

Par ailleurs, les entreprises sont à la croisée des chemins en ce qui a trait à leurs efforts de DEI (diversité, équité et inclusion). Les États-Unis ayant renoncé à leurs engagements officiels de DEI, les organisations canadiennes se retrouvent aux prises avec des questionnements sur l'avenir de la DEI.

Cela étant dit, la DEI reste une attente fondamentale que le public, surtout les travailleurs et clients plus jeunes qui veulent voir d'authentiques progrès de la part des entreprises. Échouer dans la défense de ces valeurs peut miner votre réputation et la confiance que vous inspirez, en plus de limiter votre accès aux talents.

Une gouvernance de plus en plus dans la ligne de mire

À mesure que les obligations d'information ESG se resserrent, les risques de faible gouvernance augmentent.

Les organisations sont soumises à la pression de produire de l'information ESG uniforme et transparente. Celles qui n'y parviennent pas, que ce soit par omission, non-concordance ou écoblanchiment, encourent des sanctions réglementaires ou des atteintes à leur réputation.

Parallèlement, il faut que les conseils d'administration soient assujettis à un niveau d'imputabilité plus élevé que jamais. Le manque de surveillance ou d'engagement notable est inexcusable. Les conseils d'administration doivent non seulement comprendre les risques émergents, mais également participer activement aux choix de gestion de ces risques.

En outre, il y a augmentation du risque ou de la responsabilité en lien avec les obligations réglementaires ou juridiques. Qu'elles échouent à atteindre leurs cibles climatiques ou à fournir des indicateurs de diversité, les organisations sont tenues de rendre des comptes. Des structures de gouvernance solides, une attribution claire des responsabilités, une stratégie détaillée et un conseil jouant un rôle actif sont nécessaires pour contrer les difficultés financières et d'exploitation.

Les chefs de la direction canadiens semblent prendre les facteurs ESG plus au sérieux que leurs pairs à l'échelle mondiale : ils sont 29 % à les considérer comme une haute priorité, selon un sondage. Cela étant dit, le manque de préparation aux obligations d'information sur les facteurs ESG pourrait exposer les entreprises à des risques liés à la réglementation, à la réputation et à l'exploitation.

Malgré ces signaux d'alarme, il y a encore beaucoup d'optimisme. Les initiatives ESG ont déjà commencé à améliorer les choses au Canada, que l'on pense aux progrès en innovation ou en développement durable. Toutefois, pour que ces efforts débouchent sur de la valeur à long terme, les entreprises doivent traiter les facteurs ESG à la fois comme une occasion et un risque. Ce qui veut dire sensibiliser, améliorer la production d'information et prendre des mesures proactives pour aligner la stratégie sur l'action.

Risques à surveiller

Risques environnementaux

Conséquences des changements climatiques : une plus grande fréquence des phénomènes météorologiques extrêmes (comme des feux de forêt, des inondations et des canicules) perturbe les activités et les chaînes d'approvisionnement, particulièrement dans les secteurs exigeant énormément de ressources.

Risque de transition ratée vers la carboneutralité : une réglementation des émissions et un cadre d'établissement du prix du carbone plus contraignants pourraient hausser les coûts d'exploitation des entreprises qui échouent dans leurs efforts de décarbonisation.

Perte de la biodiversité et rareté des ressources : la diminution des ressources naturelles et la perte de la biodiversité entraînent des risques à long terme pour les secteurs qui dépendent de terres, de l'eau et de l'énergie.

Allégations d'écoblanchiment : les entreprises qui surévaluent ou donnent une image inexacte de leurs efforts ESG s'exposent à des atteintes à leur réputation, à des sanctions réglementaires et à une levée de boucliers de la part des consommateurs.

Risques sociaux

Droits autochtones et réconciliation : les entreprises qui exercent leurs activités sur des terres autochtones ou à proximité de celles-ci s'exposent à des risques liés à des revendications territoriales ou aux relations avec la communauté, ainsi qu'à une attention accrue du public et du milieu juridique.

Diversité, équité et inclusion (DEI) : des stratégies de DEI faibles et un non-respect des engagements peuvent occasionner un roulement de personnel, des difficultés à attirer les talents et des atteintes à la réputation.

Relations de travail et bien-être des effectifs : une mauvaise gestion des enjeux de salaires équitables, de santé mentale et de conditions de travail pourrait se révéler problématique pour les employeurs, surtout dans les secteurs à grand roulement.

Risques de gouvernance

Présentation d'information ESG et conformité : de l'information ESG erronée ou incohérente peut conduire à des pénalités en vertu des normes nationales et mondiales changeantes de présentation d'information.

Imputabilité du conseil d'administration : de faibles pratiques de gouvernance à l'égard des priorités ESG, comme un manque de supervision de la part du conseil ou d'engagement de la part des parties prenantes, peuvent mener à de l'activisme actionnarial ou à des atteintes à la réputation.

Responsabilités réglementaires ou juridiques : une augmentation du nombre de poursuites et une intensification de la surveillance des organismes de réglementation pour ne pas avoir rempli des engagements ESG pourraient accroître les risques financiers et d'exploitation.

Signaux d'alarme

- Modifications réglementaires menant à des exigences accrues de présentation d'information ESG et à des normes plus strictes.
- Activisme actionnarial et pression exercée par des investisseurs ou des groupes de défense d'intérêts à l'égard d'enjeux d'ordre social ou de développement durable.
- Contestations juridiques ou poursuites concernant le non-respect d'engagements ESG, particulièrement ceux de DEI et de réduction des émissions de carbone.
- Boycottage, mauvaise presse ou baisse de la fidélité à la marque en raison de manquements perçus envers les principes ESG.

Stratégies d'atténuation des risques

- Élaborer un plan d'adaptation aux changements climatiques
- Renforcer la présentation d'information ESG
- Travailler de concert avec les communautés autochtones
- Réaliser l'audit des chaînes d'approvisionnement
- Améliorer la surveillance exercée par le conseil d'administration
- Investir dans l'innovation écologique
- Se préparer à la gestion de crise
- Se concerter de façon proactive avec les parties prenantes
- Surveiller les risques juridiques et réglementaires

Questions à se poser

- Votre organisation a-t-elle établi ce qu'elle était en mesure de déclarer publiquement pour se conformer au projet de loi C-59 et quelles informations nécessitent une vérification plus poussée?
- Depuis que votre organisation s'est fixé des cibles ESG officielles, quels ont été les plus gros risques? Quels changements avez-vous faits pour atténuer ces risques?
- Où votre organisation se classe-t-elle quant à l'adoption de mesures pertinentes relatives aux facteurs ESG? Vos plus grandes forces ou faiblesses sont-elles susceptibles de devenir un avantage ou un désavantage concurrentiel?
- À quel point êtes-vous prêts à vous occuper des nouvelles politiques et réglementations gouvernementales sur les facteurs ESG? Un mandat officiel de suivi de ces exigences a-t-il été confié à quelqu'un?

Révolution numérique : la nouvelle ère de la transformation technologique

La transformation numérique ne ralentit pas, elle s'accélère.

L'année 2026 arrive à grands pas et l'innovation n'attend plus après vous. Les entreprises qui agiront rapidement pour adopter de nouvelles technologies et de nouveaux services mèneront la course.

L'innovation rapide est toutefois synonyme de risque. Nombreux sont les investissements en IA et en technologies numériques émergentes qui feront chou blanc. Des défis d'intégration, des cybermenaces, des lacunes dans les compétences d'employés et de l'incertitude réglementaire se profilent à l'horizon. D'ici là, les attentes pour des solutions numériques et la commodité ne cesseront de s'intensifier, forçant votre entreprise à repenser ses façons de faire dans la prestation de services.

L'économie numérique canadienne illustre bien ce virage. En 2023, le marché de la transformation numérique a généré 84,8 G$ US et les projections montrent qu'il pourrait atteindre près de 492 G$ US d'ici 2030, selon Grand View Research. Ce chiffre correspond à un taux de croissance annuel composé vertigineux de 30 %.

Cette croissance signifie que votre entreprise doit innover sans plus tarder, sans toutefois lésiner sur la stratégie et la sécurité.

> « Des défis d'intégration, des cybermenaces, des lacunes dans les compétences d'employés et de l'incertitude réglementaire se profilent à l'horizon.

La nouvelle réalité numérique

La technologie révolutionne nos façons de travailler, d'offrir des services bancaires et d'interagir avec le monde.

- **Effectif axé sur le numérique d'abord :** les attentes de compétence technologique deviendront la norme et redéfiniront les rôles et les exigences quant aux aptitudes.
- **Des sociétés de technologies financières bien établies :** les organisations comme Neo Financial et la Banque EQ changent les façons dont les Canadiens épargnent, dépensent et gèrent leur argent.
- **Utilisation du téléphone intelligent comme clé numérique :** d'après Nortal, 87 % des Canadiens s'attendent à pouvoir compter, d'ici 2026, sur des services publics entièrement numériques. Les activités couvertes par ces services sont variées : vérification de l'identité, déplacements, paiement de factures et accès à des espaces sécurisés.
- **IA et automatisation au travail :** les rapports de dépenses, les calendriers et la saisie de données seront gérés par les assistants propulsés par l'IA, qui libéreront du temps que les employés pourront consacrer à du travail à valeur plus élevée.

Risques à surveiller

Résistance au changement : les employés et les parties prenantes peuvent résister aux nouvelles technologies, ralentissant l'adoption de celles-ci et la productivité.

Difficultés d'intégration : intégrer de nouveaux outils aux systèmes d'origine peut occasionner des retards, des problèmes de comptabilité, des coûts imprévus et des temps d'arrêt.

Compétences manquantes : des lacunes dans le savoir-faire technique peuvent se solder par une mauvaise mise en œuvre et une dépendance envers les conseillers externes.

Attentes irréalistes : surestimer les avantages immédiats de la transformation numérique peut aboutir à des dépassements de budget, à des échecs de projets et à de la déception.

Risques à la sécurité et à la confidentialité des données : le recours de plus en plus fréquent aux outils numériques et aux services infonuagiques peut exposer les entreprises aux cybermenaces, à des violations de données et à des sanctions réglementaires pour non-respect des lois sur la protection des données.

Dépendance envers les fournisseurs : une dépendance excessive à un seul fournisseur de technologie peut nuire à une entreprise et limiter sa flexibilité et son pouvoir de négociation.

Risques liés à la réglementation et à la conformité : les entreprises qui ne respectent pas les réglementations propres à leur secteur pendant la transformation numérique peuvent subir des conséquences juridiques et financières.

Obsolescence technologique : le système dernier cri d'aujourd'hui peut devenir désuet en quelques années seulement. Vous devez rester à l'affût des mises à jour.

Non-concordance avec les objectifs d'affaires : l'adoption d'un outil numérique qui ne repose pas sur un objectif d'affaires clair peut gaspiller des ressources et ne pas ajouter de valeur.

Perturbation des activités : une transition mal gérée peut mener à des interruptions de service, à l'insatisfaction de la clientèle et à des pertes financières.

Signaux d'alarme

- Report des échéanciers de mise en œuvre et entraves fréquentes aux projets
- Résistance des employés ou d'intervenants clés aux changements technologiques
- Intrusions informatiques imprévues découlant de l'adoption des nouvelles plateformes
- Forte dépendance à un fournisseur en raison d'un choix limité d'autres options
- Surveillance accrue ou sanctions de la part des organismes de réglementation en lien avec des initiatives de transformation numérique
- Lourdeur de la gouvernance du numérique, laquelle complique l'innovation

Stratégies d'atténuation des risques

- Réaliser une gestion du changement rigoureuse
- Favoriser une cybersécurité robuste
- Planifier l'intégration de façon judicieuse
- S'assurer du perfectionnement continu des compétences et de la formation des employés
- Établir des objectifs réalistes et planifier en conséquence
- Élaborer une feuille de route technologique et la mettre à jour
- Réduire la dépendance envers les fournisseurs
- Mettre au point un plan de continuité des activités
- Aligner la transformation numérique sur la stratégie d'affaires
- Assurer la préparation à la conformité réglementaire

Questions à se poser

- Comment faites-vous place à l'innovation et avez-vous éliminé les obstacles en vous assurant d'optimiser vos investissements numériques?
- À quel point vos plans de transformation numérique sont-ils ambitieux (étendue, budget et échéancier)? Est-ce que votre organisation ou les tiers avec qui vous faites affaire avez déjà travaillé sur des projets d'une taille, d'un budget ou d'une étendue semblables?
- Quels seront les effets de cette nouvelle technologie numérique sur votre façon de faire des affaires? Aurez-vous besoin d'une structure organisationnelle et de descriptions de postes complètement nouvelles? Avez-vous les ressources et le modèle de gouvernance adéquats pour ressortir du lot dans cette nouvelle réalité?
- Quel niveau de risque la résistance au changement (de la part d'employés, de tiers ou de clients) provoquera-t-elle en lien avec cette transformation numérique?
- Quels seront les effets de la transformation numérique sur votre exposition aux cyberrisques? Êtes-vous prêt à gérer la situation?

Les fraudeurs innovent aussi : une occasion se présente à chaque seconde

À l'instar des outils numériques, la fraude évolue.

L'évolution numérique est rapide, mais les fraudeurs ont une longueur d'avance. Et le niveau d'ingéniosité ne fait qu'augmenter. D'ici l'an prochain, la vérification de l'identité, les opérations financières et les activités commerciales se feront plus en douceur que jamais. Imaginez-vous embarquer dans un avion sans passeport physique : lecture d'empreintes rétiniennes, pièces d'identité numériques et authentification biométrique permettront de vous identifier de façon transparente, sans aucun effort de votre part.

Malheureusement, les fraudeurs trouveront de nouvelles façons d'exploiter chaque avancée technologique sur le plan de la commodité. Des verres de contact pourront-ils imiter la rétine de quelqu'un? Des implants numériques pourraient-ils être copiés et utilisés pour usurper votre identité? Ces scénarios peuvent sembler tirés par les cheveux. Cependant, les techniques de fraude par vol d'identité, par hypertrucage et par identité synthétique existent déjà et vont s'affiner.

Selon Equifax, au deuxième trimestre de 2024, 48,3 % de toutes les demandes de crédit frauduleuses signalées étaient liées à une fraude par vol d'identité, comparativement à 42,9 % l'année précédente. Les cas de fraude par identité synthétique ont triplé en un an. Statista a révélé que les Canadiens avaient connu des pertes de 123 M$ en raison de fraudes au 1er trimestre de 2024 seulement, et que les pertes totales pour 2023 s'élevaient à 554 M$.

Et ce ne sont pas seulement les particuliers qui sont à risque : une étude de Paiements Canada indique qu'une entreprise canadienne sur cinq a été victime d'une fraude de paiement dans les six derniers mois, et que les grandes entreprises commerciales ont connu le taux de fraude le plus élevé, soit 26 %, comparativement à 16 % pour les petites entreprises. Les types de fraudes les plus courants ont été la fraude par usurpation d'identité (25 %), l'interception de virement Interac (22 %) et la fraude par carte de crédit (20 %).

La fraude évolue plus rapidement que la plupart des moyens de défense. Pour conserver une longueur d'avance, votre entreprise doit faire appel à la détection alimentée par l'IA, à la surveillance en continu de la fraude et à des contrôles de sécurité robustes, parce que c'est ce que font déjà les fraudeurs.

L'essor de la fraude par IA

La fraude ne se résume plus au vol de numéros de cartes de crédit. Elle vise à manipuler la confiance. L'IA et la technologie d'hypertrucage marquent le début d'une ère nouvelle où les criminels peuvent :

- cloner la voix et l'apparence pour usurper l'identité de dirigeants et approuver des opérations frauduleuses;
- utiliser des courriels d'hameçonnage générés par l'IA et de fausses factures pour duper des employés;
- utiliser des identités synthétiques, c'est-à-dire de fausses personnes créées à partir de données réelles volées, pour ouvrir des comptes, contracter des emprunts et commettre des fraudes à grande échelle;
- créer de fausses boutiques virtuelles et des plateformes d'investissement et se faire passer pour un organisme de bienfaisance afin de voler de l'argent et des données personnelles.

Risques à surveiller

Hameçonnage et piratage psychologique : de plus en plus astucieux, des courriels d'hameçonnage, des textos et du piratage psychologique incitent les employés et les consommateurs à révéler des données sensibles ou à effectuer des opérations non autorisées.

Compromission du courriel professionnel : les fraudeurs usurpent l'identité de dirigeants ou de fournisseurs et approuvent des paiements frauduleux.

Cyberfraude et rançongiciels : les criminels se servent du cryptage de données pour exiger une rançon, en ciblant souvent des PME disposant de moins de ressources de cybersécurité.

Vol d'identité et identités synthétiques : les fraudeurs combinent des données réelles et fausses pour créer des identités synthétiques, qu'ils utilisent pour commettre de la fraude financière, ouvrir des comptes frauduleux ou accéder à des prestations du gouvernement.

Commerce électronique et arnaques de paiement : la fraude par absence de carte, les fausses boutiques virtuelles et les arnaques par rétrofacturation font de plus en plus de ravages.

Stratagèmes de placement : ces fausses occasions de placement hautement profitables, notamment dans les cryptomonnaies, l'immobilier et les stratagèmes impliquant des rendements élevés, fourvoient de nombreuses victimes, surtout quand l'économie est volatile.

Fraude par délit d'initié : des employés ou des sous-traitants exploitent leur accès à des systèmes internes ou à des données sensibles pour leur gain personnel et le stratagème passe souvent inaperçu jusqu'à ce que des pertes considérables soient constatées.

Fraude liée aux impôts ou à des prestations : la fraude en lien avec les déclarations d'impôt et les prestations gouvernementales, comme celles de l'assurance-emploi et des programmes d'aide liés à la pandémie, demeure préoccupante.

Fraudes relatives aux dons et aux organismes de bienfaisance : les escrocs se font passer pour des organismes de bienfaisance légitimes ou en créent des faux pour exploiter la générosité du public, surtout à la suite d'une catastrophe naturelle ou dans un contexte de crises.

Produits de contrefaçon et vol de propriété intellectuelle : la distribution de produits de contrefaçon et l'utilisation non autorisée de marques de commerce ou de droits d'auteur causent du tort aux entreprises et induisent les consommateurs en erreur.

Signaux d'alarme

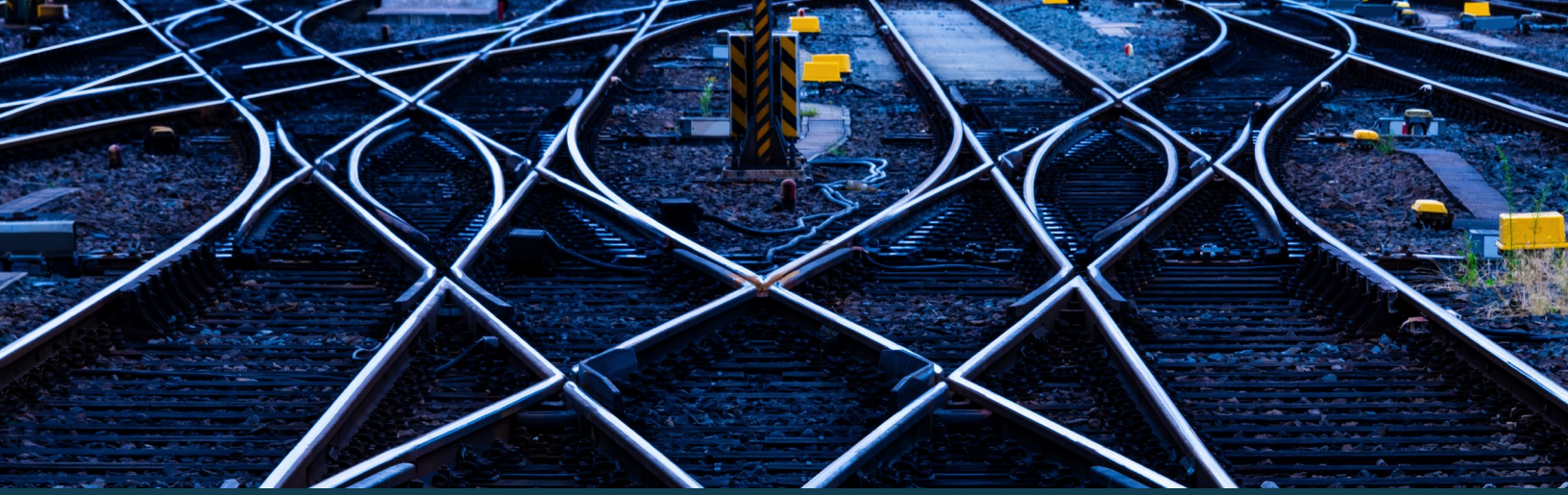
- Courriels inhabituels de demande de paiement urgent
- Hausses imprévues de la rétrofacturation, des opérations contestées ou des plaintes de clients
- Pannes de systèmes subites, messages de rançongiciels ou tentatives d'accès non autorisé
- Employés accédant à des données sensibles en outrepassant leurs fonctions
- Signalements de comptes frauduleux liés à des renseignements personnels ou commerciaux

Stratégies d'atténuation des risques

- Former son personnel
- Détecter les fraudes par l'IA et l'apprentissage automatique
- Mettre en place un système d'authentification à facteurs multiples
- Opter pour des systèmes de paiements sécurisés
- Renforcer la vérification des fournisseurs
- Instaurer des contrôles de cybersécurité avancés
- Protéger les données par le cryptage et le contrôle des accès
- Évaluer régulièrement les risques de fraude et surveiller les activités financières
- Organiser des campagnes de sensibilisation du public
- Collaborer avec les forces de l'ordre, les groupes sectoriels et les organismes de réglementation

Questions à se poser

- Avez-vous mis à jour la formation sur votre code de conduite et vos politiques connexes pour tenir compte des méthodes actuelles d'utilisation de la technologie à des fins de fraude?
- Vos contrôles de lutte contre la fraude sont-ils efficaces pour prévenir et détecter les techniques de fraude modernes?
- À quand remonte la dernière évaluation des risques de fraude que votre organisation a menée?
- Avez-vous une politique sur les conflits d'intérêts qui précise ceux qui sont acceptables?



Chaîne d'approvisionnement 2.0 : faire face aux enjeux d'un avenir hyperconnecté

Est-ce qu'il existe aujourd'hui des risques qui n'ont pas d'incidence sur les chaînes d'approvisionnement?

L'approvisionnement moderne nécessite des réseaux complexes et interdépendants.

Qu'il s'agisse de l'acquisition de matières premières, de la fabrication ou de la distribution, les risques associés au virage numérique, à la situation géopolitique, aux conflits de travail et aux questions environnementales remodèlent les flux transfrontaliers de marchandises. Les pressions grandissantes pour un approvisionnement éthique et durable viennent compléter la liste des ingrédients d'une complexité sans précédent.

La pandémie de 2020 a été un premier coup de semonce. Elle nous a appris qu'une chaîne d'approvisionnement peut rapidement s'effondrer. Les perturbations qui ont touché la main-d'œuvre, la fabrication et l'expédition ont causé des pénuries dans beaucoup de secteurs. Les faiblesses des modèles à fournisseur exclusif, des systèmes de logistique vétustes et des modèles de gestion juste-à-temps ont éclaté au grand jour.

> « La pandémie de 2020 a été un premier coup de semonce. Elle nous a appris qu'une chaîne d'approvisionnement peut rapidement s'effondrer.

Cinq ans plus tard, les chaînes d'approvisionnement font face à de nouveaux défis. Les mesures tarifaires sans précédent appliquées par le président Donald Trump sur les alliés de longue date des États-Unis bouleversent le paysage commercial pour les entreprises canadiennes. Force est de constater que l'existence d'un commerce transfrontalier bon marché n'est plus une certitude et que sa disparition poserait de graves problèmes économiques pour le Canada, qui s'est employé à l'optimiser depuis plus de 30 ans. Peu importe l'importance et la durée des tarifs, leurs répercussions seront assurément à la fois importantes et profondes.

Les conflits de travail dans le transport ferroviaire au Canada en 2024 ont été un nouveau rappel de la fragilité des chaînes d'approvisionnement. Le lock-out de plus de 9 000 ouvriers du Canadien National et du Canadien Pacifique Kansas City a mis en danger des millions de dollars d'échanges commerciaux quotidiens. Les exportations de céréales, la fabrication de produits chimiques et le transport de fret furent durement touchés. L'interruption du transport ferroviaire a occasionné des pertes quotidiennes de 55 M$ à 63 M$ dans le secteur des engrais selon Fertilisants Canada et aurait pu compromettre les exportations agricoles canadiennes sur l'échiquier mondial.

Dans le domaine des chaînes d'approvisionnement, l'avenir appartient à ceux qui sauront s'adapter, opérer un virage numérique et parer aux imprévus.

La réalité des chaînes d'approvisionnement modernes

La résilience des chaînes d'approvisionnement n'est plus seulement une question d'efficacité. Elle dépend dorénavant de facteurs clés comme l'agilité, la technologie et la gestion des risques.

Le numérique est en train de transformer le domaine de la logistique. Pour minimiser les contrecoups des perturbations, de grandes sociétés comme UPS et Walmart utilisent des systèmes de logistique et de gestion des stocks fondés sur des données. Or, les entreprises ne sont pas toutes capables d'une telle adaptation, et la conséquence pour les plus petits acteurs pourrait être de se voir exclus du marché.

On observe une intensification des pressions de nature réglementaire et éthique. Au Canada, la Loi sur la lutte contre le travail forcé et le travail des enfants dans les chaînes d'approvisionnement (2024) exige la production d'un rapport annuel sur les efforts déployés pour prévenir le risque de recours au travail forcé et au travail des enfants. Cette loi contribue à la transparence de ces chaînes, mais les entreprises qui ne réussissent pas à avoir un portrait clair des activités de leurs fournisseurs trouvent difficile de se conformer à ses dispositions.

On constate aussi une augmentation des risques mondiaux liés à la gouvernance. Les partenaires commerciaux du Canada doivent respecter des règles de gouvernance de plus en plus strictes, ce qui rend l'exercice d'un contrôle diligent à l'importation plus important que jamais pour éviter les fournisseurs malhonnêtes et assurer sa conformité aux lois et aux règlements.

Risques à surveiller

Phénomènes climatiques extrêmes : les feux de forêt, les inondations et les orages violents perturbent les installations manufacturières et les infrastructures de transport.

Instabilité géopolitique : les tarifs douaniers, les différends commerciaux et les conflits armés, entre autres, ont des répercussions sur la disponibilité et le prix des matières premières et des marchandises.

Perturbations du travail : les grèves et les conflits de travail peuvent interrompre la circulation des marchandises à l'échelle du pays.

Infrastructures de transport : les ports congestionnés, les réseaux ferroviaires vétustes et les autoroutes engorgées augmentent les coûts et les retards d'acheminement.

Menaces à la cybersécurité : les chaînes d'approvisionnement sont exposées à un risque accru de cyberattaques (logiciels de rançon, intrusions informatiques, etc.) qui visent les infrastructures et les systèmes informatiques essentiels.

Perturbations de nature technologique : les avancées technologiques et le virage numérique confrontent les chaînes d'approvisionnement à une complexité croissante et à des problèmes d'intégration.

Insolvabilité des fournisseurs : l'incertitude économique peut perturber les chaînes d'approvisionnement en rendant les fournisseurs insolvables ou en réduisant leur capacité de production.

Pénurie de matériaux : la hausse du coût des intrants et les questions environnementales rendent certains matériaux plus difficiles à obtenir.

Changements à la réglementation : les entreprises doivent respecter une reddition de comptes plus stricte au sujet de leurs émissions de carbone, du caractère éthique de leurs pratiques d'emploi et de l'impact écologique de leurs activités.

Perturbations causées par la pandémie : certains effets de la pandémie de COVID-19 continuent de jouer sur la disponibilité de la main-d'œuvre et les dynamiques du commerce mondial.

Signaux d'alarme

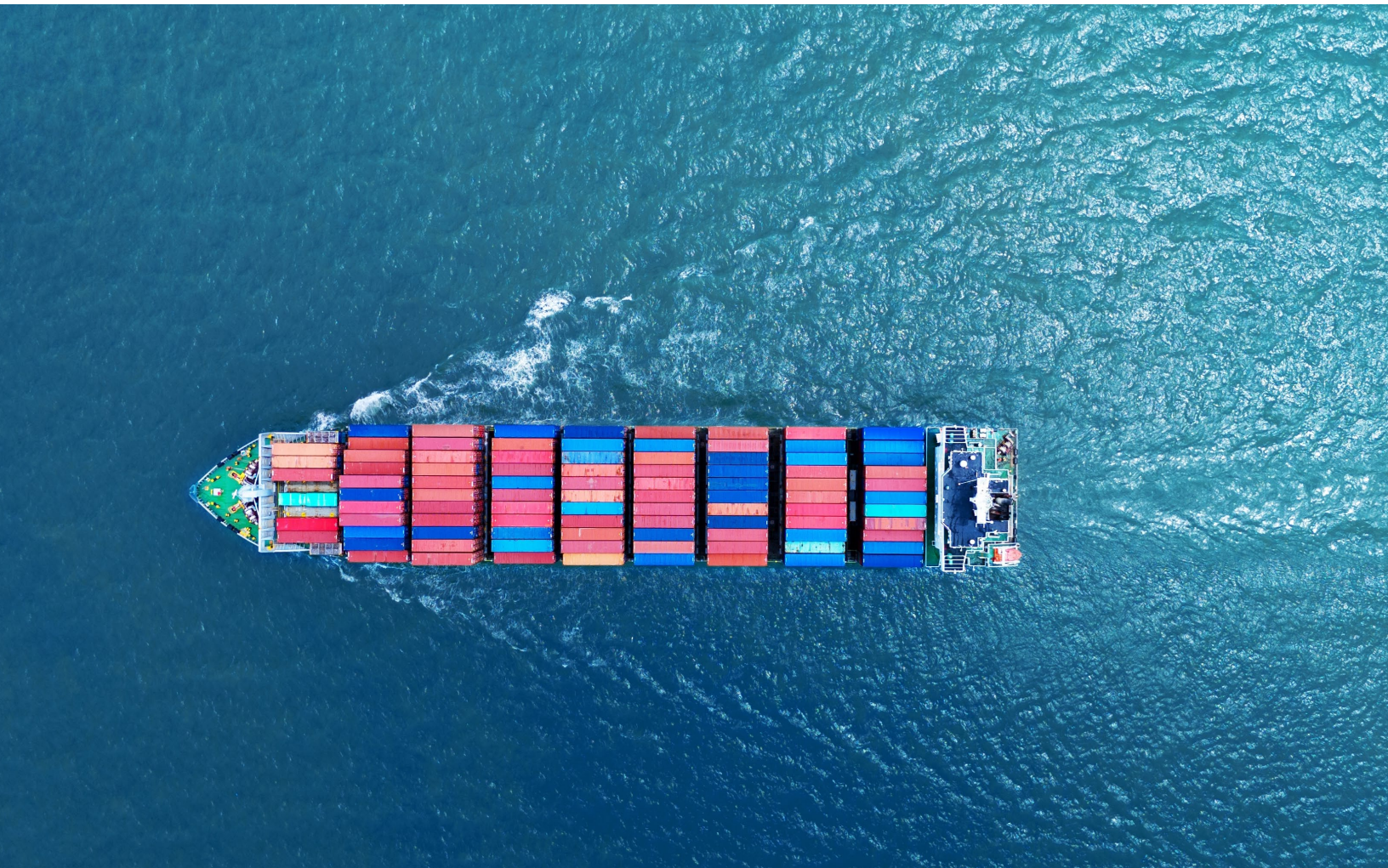
- Augmentation des délais d'approvisionnement ou de production, retards fréquents chez les fournisseurs
- Montée en flèche du coût de certains matériaux en raison de pénuries ou de tarifs douaniers
- Cyberattaques qui s'en prennent aux systèmes de logistique
- Conflits de travail, manifestations et non-respect de clauses contractuelles dans des secteurs névralgiques
- Cas signalés de recours au travail forcé et au travail des enfants par des fournisseurs internationaux
- Déclin de la fiabilité des infrastructures (ports congestionnés, transport ferroviaire perturbé, autoroutes vétustes, etc.)

Stratégies d'atténuation des risques

- Diversifier sa liste de fournisseurs
- Investir dans des outils d'analyse et des outils numériques pour cerner les problèmes et optimiser les ressources
- Renforcer les dispositifs de cybersécurité
- Envisager des scénarios et établir des plans de contingence
- Surveiller l'évolution du contexte réglementaire
- Renforcer ses relations et collaborer avec ses fournisseurs et ses partenaires commerciaux

Questions à se poser

- Quelles menaces au commerce mondial pourraient nuire à votre entreprise? Est-ce que vous effectuez des simulations pour déterminer le meilleur moyen d'atténuer les risques qui pèsent sur votre entreprise?
- Connaissez-vous bien vos fournisseurs? Est-ce que certains des risques auxquels ils sont exposés pourraient vous nuire directement ou indirectement?
- Quelles mesures d'atténuation des risques vos fournisseurs externes de confiance peuvent-ils mettre en œuvre au besoin?
- Dans quelle mesure vos chaînes d'approvisionnement reposent-elles sur des systèmes informatiques tiers? Les mesures de cybersécurité des entreprises responsables de ces systèmes sont-elles suffisantes?
- Votre chaîne d'approvisionnement est-elle assez souple pour s'adapter aux imprévus?



Valeur des données : gouvernance et protection des renseignements personnels à l'ère numérique

Les données : un actif à la fois précieux et vulnérable.

À une époque de transformations numériques sans précédent, les règles régissant la protection des renseignements personnels se resserrent, les cybermenaces s'intensifient et le public exige plus de transparence. La question n'est pas seulement de collecter et de stocker l'énorme quantité de données générée par l'intelligence artificielle, l'Internet des objets et les chaînes de blocs, mais également d'assurer la bonne gouvernance de cette information de même que sa protection et son utilisation conforme à des principes éthiques.

Le nouveau dilemme de la gouvernance des données

Normaliser la gouvernance des données devient de plus en plus complexe. Des initiatives comme le Collectif canadien de normalisation en matière de gouvernance des données tentent d'établir des cadres pour gérer les risques à leur sécurité et à leur confidentialité, mais la technologie continue de devancer les efforts déployés en ce sens. Résultat? Les normes diffèrent d'un secteur à l'autre, la gestion des données est loin d'être uniforme et les risques s'accroissent.

> « La question n'est pas seulement de collecter et de stocker l'énorme quantité de données générée par l'intelligence artificielle, l'Internet des objets et les chaînes de blocs, mais également d'assurer la bonne gouvernance de cette information de même que sa protection et son utilisation conforme à des principes éthiques.

On observe un resserrement de la réglementation. La Stratégie relative aux données de 2023-2026 pour la fonction publique fédérale met en lumière le besoin d'une gestion responsable des données et exige des entreprises qu'elles se montrent capables de respecter des règles plus strictes, sans quoi elles s'exposent à des conséquences de nature juridique ou à des atteintes à leur réputation.

Or, reconnaître que les renseignements personnels sont importants n'est pas la même chose qu'être prêt à les protéger. Bien qu'une proportion de 88 % des entreprises canadiennes connaisse leurs obligations de protection des renseignements personnels, seulement 47 % d'entre elles ont une politique officielle à cet effet, selon le Commissariat à la protection de la vie privée du Canada. Ces entreprises s'exposent à des intrusions et peuvent éveiller la méfiance du public, surtout à une époque où les consommateurs exigent que leurs informations soient mieux protégées.

Toutefois, les menaces auxquelles les organisations doivent faire face prennent de nouvelles formes. Les cybercriminels s'intéressent de plus en plus à la manipulation des données plutôt qu'au piratage des systèmes. Les fraudes utilisant les hypertrucages, les hameçonnages générés à l'aide de l'intelligence artificielle et les menaces internes rendent obsolètes les mesures de défense traditionnelles. Le Commissariat milite pour une intégration de la protection des renseignements personnels dès la conception, une approche fondée sur le risque qui détermine les contrôles nécessaires pour mettre à l'abri les informations sensibles. Une entreprise qui ne réalise pas d'investissements conséquents dans la sécurité des données et les efforts de conformité à la réglementation en vigueur risque de se retrouver à la traîne et de voir la confiance des consommateurs à son égard s'éroder.

Risques à surveiller

Intelligence artificielle et fournisseurs externes : le nombre d'atteintes à la vie privée pourrait augmenter à cause de l'intelligence artificielle et des fournisseurs externes ayant des cadres de gouvernance déficients.

Non-conformité réglementaire : les organisations qui peinent à suivre l'évolution des lois sur la protection des renseignements personnels peuvent se retrouver en situation de non-conformité et s'exposer à des sanctions juridiques.

Transfert de données transfrontalier : les lois régissant la souveraineté des données deviennent de plus en plus strictes, ce qui fait obstacle au stockage et au partage de données à l'international.

Menaces occasionnées par le travail à distance ou le travail hybride : hors de l'environnement sécurisé des locaux d'une entreprise, des employés pourraient mal utiliser des données sensibles.

Violations de données en raison de mauvais contrôles sécuritaires : des mesures de cybersécurité insuffisantes peuvent mettre en danger les renseignements personnels et organisationnels.

Gestion des préférences d'utilisateurs sur divers canaux : la gestion uniforme du consentement et des préférences d'un utilisateur sur une multitude de plateformes pose d'importantes difficultés et peut miner la confiance de celui-ci et la conformité de l'entreprise.

Incidences de la loi sur les jeux de données tierces : de nouvelles lois qui touchent les données tierces peuvent augmenter le risque de non-conformité pour les entreprises qui n'ont pas un cadre de gouvernance approprié.

Protection accrue des renseignements personnels des enfants : de nouvelles lois imposent des restrictions sur la collecte de données auprès de mineurs.

Encadrement de l'intelligence artificielle et questions d'ordre éthique : l'intelligence artificielle soulève des questions au sujet de la protection des renseignements personnels et de l'éthique. Les organisations doivent se doter de politiques détaillées pour les traiter.

Application plus stricte des règles de protection des renseignements personnels : les organismes de réglementation ont intensifié leurs efforts en ce sens, ce qui entraîne l'imposition de pénalités plus coûteuses et met en lumière le besoin pour des programmes de conformité.

Signaux d'alarme

- Fournisseur qui a des mesures de sécurité ou une politique de partage des données floues
- Adoption tardive de règles visant la protection des renseignements personnels ou non-respect des dates butoirs pour la conformité
- Accès fréquents et injustifiés à des données sensibles par des intervenants internes
- Lacunes dans les ententes pour le transfert transfrontalier de données, qui exposent à des risques de nature juridique
- Nombre grandissant de plaintes de clients au sujet de la transparence et de l'utilisation inappropriée de données
- Vigilance accrue des organismes de réglementation en raison du recours accru à l'intelligence artificielle dans la prise de décisions et des questions de nature éthique qui en découlent

Stratégies d'atténuation des risques

- Mettre en place un cadre de gouvernance des données rigoureux
- Renforcer les mesures de cybersécurité et les contrôles portant sur la gouvernance des données
- Offrir régulièrement de la formation sur la cybersécurité aux membres du personnel
- Créer des lignes directrices pour une utilisation éthique de l'intelligence artificielle
- Uniformiser la gestion du consentement et des préférences
- Améliorer le dispositif de détection des menaces internes
- Mettre l'accent sur la protection des données des enfants
- Surveiller l'évolution des cadres réglementaires
- Faire des préparatifs en vue d'une intervention des organismes de réglementation

Questions à se poser

- Comment une organisation peut-elle se conformer aux règles régissant la protection des renseignements personnels tout en favorisant l'innovation et l'efficacité de son exploitation?
- Quelles stratégies une organisation peut-elle mettre en œuvre pour combler le fossé entre la formation de ses équipes et leur participation active dans la gestion des risques visant la protection des renseignements personnels?
- Quelles mesures une entreprise peut-elle déployer pour rassurer le public et faire preuve de transparence dans l'utilisation et la protection des données recueillies?
- Avez-vous repéré les jeux de données qui sont essentiels à vos activités et mis en place des protections conséquentes?

Trouver une main-d'œuvre qualifiée : un défi majeur pour les entreprises

Les candidats de qualité font l'objet d'une concurrence plus féroce que jamais.

Dans un contexte où la croissance de l'économie canadienne repose de plus en plus sur la technologie, votre entreprise doit répondre à un besoin urgent, celui de trouver, de former et de fidéliser les professionnels du numérique dont elle a besoin pour prospérer.

Certains secteurs sont déjà aux prises avec une pénurie chronique de main-d'œuvre spécialisée, les attentes des travailleurs et la place grandissante de l'intelligence artificielle dans le recrutement. Ces tendances ne vont que s'accentuer dans les années à venir. En l'absence d'une stratégie pour les prendre en compte, elles pourraient étouffer l'innovation, nuire à la productivité et placer des entreprises dans une position désavantageuse sur les marchés mondiaux.

L'agrandissement du gouffre numérique

La demande en personnel qualifié demeure élevée dans les métiers technologiques. Malgré des compressions d'emploi très médiatisées dans ce domaine, une enquête menée par Equinix sur les tendances technologiques mondiales montre que 70 % des entreprises canadiennes sont d'avis que la pénurie de personnel compétent est une entrave majeure à leur prospérité. Les compétences les plus recherchées relèvent des domaines de l'infonuagique, de l'intelligence artificielle, de la cybersécurité et de l'analyse de données.

Or, le marché du travail ne réussit pas à répondre à la demande. Selon le Centre des compétences futures, 90 % des emplois nécessiteront dans la prochaine décennie des compétences en numérique que seulement 54 % des travailleurs possèdent à l'heure actuelle. S'il ne réalise pas des investissements pressants pour améliorer les compétences de sa main-d'œuvre et pour la requalifier, le Canada risque de se faire distancer dans l'économie mondiale du numérique.

La course au recrutement et à la rétention du personnel

La concurrence pour s'emparer de professionnels expérimentés en numérique n'a jamais été aussi rude. Les entreprises sont aux prises avec divers problèmes.

Difficulté à pourvoir des postes à temps plein : selon une étude réalisée en 2024 par la Society for Human Resource Management, plus de 75 % des organisations affirment avoir de la difficulté à embaucher du personnel à temps plein.

Manque de personnel compétent : les postes en cybersécurité, en intelligence artificielle et en science des données sont particulièrement difficiles à pourvoir.

Rétention du personnel : malgré la vigueur du marché de l'emploi, les entreprises peinent à conserver leurs employés les plus talentueux.

Le vieillissement de la main-d'œuvre au Canada exacerbe ce problème. Bon nombre de professionnels chevronnés prennent leur retraite et emportent avec eux un bagage de connaissances que leurs successeurs n'ont pas encore acquis.

Aussi, on remarque que les métiers qualifiés et les emplois dans les secteurs névralgiques, par exemple les mines et la fabrication, n'ont plus la cote. Malgré des salaires très concurrentiels et des emplois stables, les jeunes générations préfèrent occuper des postes dans le domaine des technologies.

Voici ce que nous réserve l'avenir : le Canada restera à la traîne sur les plans de l'innovation et de la productivité si les organisations ne font pas du perfectionnement de leurs effectifs une priorité.

Tout n'est pas noir pour autant. On déploie des efforts pour rectifier la situation. Le gouvernement canadien a par exemple mis en ligne une plateforme pour communiquer aux professionnels du numérique les possibilités d'emploi dans le secteur public. À la publication du présent rapport, plus de 14 000 personnes avaient soumis leur candidature.

Malgré les initiatives de ce genre, le recadrage des politiques et l'opinion publique pourraient avoir une incidence sur les stratégies d'embauche. Par conséquent, les organisations ne peuvent pas se fier uniquement sur de telles plateformes pour combler leurs besoins en personnel. Il est essentiel de se préparer à tout changement au droit du travail, aux quotas d'immigration ou aux mesures de financement pour le perfectionnement de la main-d'œuvre.

Intelligence artificielle et recrutement

L'intelligence artificielle transforme le domaine du recrutement. Les entreprises utilisent des solutions d'intelligence artificielle pour :

- accélérer le processus d'embauche grâce au filtrage des curriculum vitæ et à l'automatisation des évaluations;
- améliorer l'expérience des candidats grâce à des processus de recrutement personnalisés;
- repérer les candidatures d'après leurs compétences plutôt que par le titre des postes qu'ils ont occupés.

Le recours à l'intelligence artificielle n'est toutefois pas sans risque.

- En raison des préjugés sur lesquels ils pourraient reposer, les algorithmes d'embauche peuvent exclure involontairement des candidats qualifiés.
- Si l'on se fie trop à l'intelligence artificielle, on peut passer à côté de candidats prometteurs qui ont un parcours atypique.
- Tout manque de transparence au sujet du modèle d'entraînement et de la logique décisionnelle d'une intelligence artificielle peut soulever des préoccupations sur le plan de la conformité et de l'éthique.

Dans un contexte où l'intelligence artificielle et l'automatisation risquent de remplacer certains emplois, les entreprises doivent choisir entre la requalification et les mises à pied.

Votre organisation doit s'assurer que l'intelligence artificielle contribue à un recrutement efficace et à une expérience positive pour les candidats au lieu de nuire à une embauche axée sur la diversité des profils.

Risques à surveiller

Vieillissement de la main-d'œuvre et départs à la retraite : dans des domaines névralgiques comme les métiers manuels, le départ à la retraite des employés d'expérience rime avec perte de connaissances.

Pénurie chronique de main-d'œuvre qualifiée : les organisations peinent à pourvoir des postes clés, faute de candidats expérimentés, ce qui nuit à leur productivité et à leur croissance.

Incertitude économique et croissance des salaires : la volonté de limiter la hausse des salaires en raison de la conjoncture économique morose peut nuire au recrutement et à la rétention du personnel.

Pénurie de main-d'œuvre dans le secteur minier : dans un contexte de forte demande pour des minéraux essentiels à diverses technologies, le secteur minier fait face à une grave pénurie d'ouvriers.

Plafonnement des programmes de travailleurs étrangers temporaires : les secteurs qui dépendent d'une main-d'œuvre étrangère bon marché, par exemple le tourisme d'accueil et l'agriculture, devront composer avec des restrictions.

Difficultés d'intégration : le Canada n'arrive pas à créer suffisamment d'emplois pour répondre à la demande suscitée par une forte immigration, ce qui rend difficile l'intégration des nouveaux arrivants au marché de travail.

Amélioration des compétences et requalification : un nombre grandissant d'entreprises optent pour la formation de leurs employés actuels pour respecter leurs contraintes budgétaires et pour pallier des manques de compétences.

Avancées technologiques rapides et inadéquation des compétences : l'évolution de la technologie pousse sans cesse les travailleurs à acquérir des connaissances et à s'adapter.

Pénuries de compétences propres aux secteurs : certains domaines comme la construction, les services publics et les mines exigent des savoir-faire précis, et le manque de personnes qualifiées a des répercussions sur la productivité des entreprises qui en dépendent.

Opinion publique et recadrage des politiques : Le mécontentement du public et les pressions électorales entraînent un remaniement des programmes d'immigration et de travailleurs étrangers, qui a des répercussions sur la disponibilité d'une main-d'œuvre qualifiée.

Signaux d'alarme

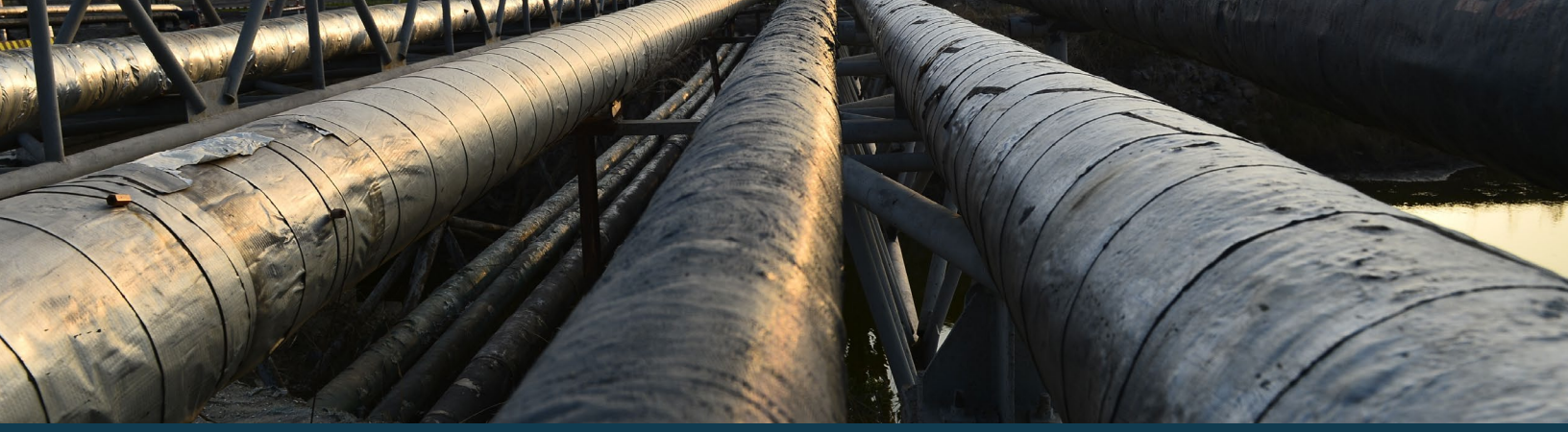
- Impossibilité d'embaucher le personnel requis
- Écart grandissant entre les compétences recherchées et le savoir-faire de la main-d'œuvre disponible
- Prolongation des délais d'embauche et augmentation des coûts de main-d'œuvre
- Recours accru aux sous-traitants et aux travailleurs temporaires
- Diminution de l'intérêt pour certains métiers essentiels et certains secteurs à forte intensité de main-d'œuvre

Stratégies d'atténuation des risques

- Investir dans l'amélioration des compétences et la requalification
- Multiplier les sources de recrutement et améliorer les stratégies d'embauche
- Faire la promotion d'une carrière dans les métiers spécialisés
- Améliorer la souplesse des conditions de travail
- Militer pour un soutien des pouvoirs publics

Questions à se poser

- Quels sont les besoins actuels et anticipés de votre organisation pour des professionnels qualifiés en numérique? Est-ce que la main-d'œuvre disponible sur le marché de l'emploi permet de combler ces besoins? Quelles solutions novatrices peuvent vous permettre de pourvoir tous vos postes?
- Quels effets ont les politiques d'immigration et la concurrence mondiale sur la capacité de votre organisation à attirer et à retenir des professionnels qualifiés en numérique?
- Quel rôle vos programmes de formation jouent-ils dans l'acquisition par votre personnel des compétences numériques dont votre organisation a besoin? Croyez-vous que ces programmes sont en mesure de répondre à vos besoins futurs?
- Quels sont les effets de facteurs comme le télétravail, l'automatisation et l'incertitude économique sur la disponibilité et l'affectation des professionnels spécialisés en numérique au sein de votre entreprise?



Convergence stratégique : prévenir les risques émergents liés à la gouvernance des TI et de la TO

Chevauchement des TI et de la TO

Plus l'infrastructure numérique du Canada évolue, plus les technologies de l'information (TI) et la technologie opérationnelle (TO) tendent à se chevaucher. Les entreprises utilisent aujourd'hui des systèmes qui intègrent à leurs activités concrètes des informations fondées sur des données, ce qui contribue à cette convergence. Celle-ci favorise les gains d'efficience, mais crée également des sources de vulnérabilité, notamment dans les secteurs de l'énergie, de la fabrication et des transports.

Les systèmes de TO étaient par le passé à l'abri des menaces externes, mais ils sont maintenant des cibles de choix pour les cybercriminels. Les attaques par rançongiciel ont le potentiel de faire cesser la production, perturber les réseaux d'énergie et paralyser les réseaux de transport.

En 2021, le réseau de pipelines de Colonial aux États-Unis a été victime d'une attaque par rançongiciel ayant compromis son réseau de technologies de l'information (TI) via un réseau privé virtuel. Par mesure préventive, l'organisation a interrompu ses opérations de transport afin d'éviter que l'attaque ne touche ses systèmes de technologies opérationnelles (TO). Au bout du compte, Colonial Pipeline a payé une rançon de 4,4 M$ pour reprendre le contrôle de ses systèmes et s'assurer que l'incident n'affecte pas ses infrastructures critiques.

En même temps, l'IA générative redéfinit la cybersécurité en offrant à la fois des moyens de protection et des outils pour lancer des attaques. Face à l'augmentation des risques, les organisations doivent revoir leur stratégie de gouvernance, et trouver le point d'équilibre entre innovation et sécurité.

> « Les attaques par rançongiciel ont le potentiel de faire cesser la production, perturber les réseaux d'énergie et paralyser les réseaux de transport.

Hausse des incidents liés à la TO

Les fraudeurs ciblent de moins en moins les réseaux de TI pour viser plutôt les environnements de TO, dont les pannes peuvent paralyser complètement une organisation. Et une fréquence à la hausse des attaques par rançongiciel et des coûts qu'elles engendrent appelle un resserrement des mesures de cybersécurité. Les organisations doivent miser sur leur résilience en favorisant une meilleure planification des interventions en cas d'incident, une formation plus poussée de leur personnel et des investissements plus importants dans des technologies de détection.

L'IA, et particulièrement l'IA générative, constitue à la fois un outil de cybersécurité et une menace à vos systèmes de TI et de TO. En fait, selon l'Autorité canadienne pour les enregistrements Internet, 70 % des professionnels en cybersécurité ont exprimé des inquiétudes quant aux cybermenaces posées par l'IA générative, en raison notamment des données qui sont collectées par les outils d'IA (61 %) et les tactiques d'hameçonnage perfectionnées qu'elle permet d'utiliser (56 %).

Pour se prémunir contre la multiplication des menaces liées à l'IA, les organisations doivent adopter des mesures de surveillance plus poussées, resserrer le contrôle des données et élaborer des politiques d'utilisation éthique de cette technologie.

Risques à surveiller

Attaques par rançongiciel : elles s'imposent comme la plus grande cybermenace pouvant perturber directement les infrastructures et services essentiels.

Cybermenaces parrainées par des États : des acteurs d'États-nations mènent des activités d'espionnage ou de vol de propriété intellectuelle.

Hameçonnage et piratage psychologique : les attaques par hameçonnage sont toujours d'actualité. Elles exploitent la vulnérabilité humaine pour obtenir un accès non autorisé aux systèmes de TI ou de TO.

Lacunes des systèmes existants : des infrastructures désuètes de TI et de TO posent des risques à la sécurité et freinent l'adoption de technologies modernes.

Menaces internes : des membres du personnel malintentionnés posent toujours des risques importants pour la sécurité organisationnelle.

Vulnérabilités de la chaîne d'approvisionnement : la hausse des risques associés aux fournisseurs tiers et aux chaînes d'approvisionnement peut compromettre la sécurité des organisations.

Défis de la conformité à la réglementation : le resserrement des exigences réglementaires entraîne des ajustements constants aux stratégies de conformité, ce qui a des répercussions sur les activités liées aux TI et à la TO.

Menaces plus persistantes et plus perfectionnées : les cyberattaques perfectionnées et ciblées dont l'objectif est de voler des données ou de perturber les activités sont de plus en plus fréquentes.

Vulnérabilités de l'Internet des objets (IdO) : l'augmentation du nombre d'appareils d'IdO étend la cible des attaques et présente de nouveaux défis liés à la sécurité pour les TI et la TO.

Perturbations des activités liées à des cyberincidents : les cyberincidents perturbent les activités en nuisant à la productivité et à la prestation de services.

Signaux d'alarme

- Indisponibilité des infrastructures et services essentiels
- Pannes de systèmes inexpliquées ou chiffrement soudain des données
- Hausse des tentatives d'hameçonnage et des demandes d'accès non autorisées
- Signalement de fuites à l'interne ou d'activités suspectes de membres du personnel
- Retards dans les mises à jour de logiciels et de correctifs de sécurité
- Défaillance ou pannes subites des systèmes de TO

Stratégies d'atténuation des risques

- Renforcer la cyberdéfense
- Mettre à niveau les systèmes existants
- Offrir régulièrement de la formation sur la cybersécurité aux membres du personnel
- Évaluer la sécurité de la chaîne d'approvisionnement
- Créer des programmes pour contrer les menaces internes
- Assurer la conformité à la réglementation
- Surveiller les menaces plus persistantes et plus perfectionnées
- Appliquer des mesures de sécurité aux appareils de l'IdO
- Élaborer des plans d'intervention en cas d'incident
- Tenir compte de l'aspect global de la sécurité en fonction des environnements des TI et de TO

Questions à se poser

- Comment votre organisation peut-elle se prémunir contre les menaces à la cybersécurité des TI et de la TO, alors que les infrastructures essentielles sont des cibles de choix?
- Quelles mesures votre organisation a-t-elle prises pour harmoniser la gouvernance des TI et de la TO, compte tenu de leurs différentes priorités opérationnelles et exigences de sécurité?
- Quelle sera l'incidence de la réglementation canadienne et des normes internationales sur la gouvernance des TI et de la TO, et sur la stratégie de votre organisation à cet égard?
- Quelles stratégies sont mises en œuvre pour parfaire les compétences en lien avec la convergence des TI et de la TO, surtout dans le contexte de technologies émergentes comme l'IA et l'IdO?

Prolifération de la désinformation : distinguer le vrai du faux dans un monde numérique

Une menace de plus en plus grave à la démocratie.

La désinformation, soit le fait de propager délibérément de fausses informations pour tromper les autres ou leur causer du tort, constitue l'une des plus grandes menaces actuellement à la société canadienne ainsi qu'à la démocratie et aux entreprises du pays. L'omniprésence des plateformes numériques fait que les fausses informations se répandent plus rapidement et sont plus convaincantes que jamais, ce qui mine la confiance envers les institutions et déforme dangereusement l'opinion publique.

Selon Statistique Canada, en 2023, 59 % des Canadiens exprimaient de grandes inquiétudes à l'égard de la mésinformation en ligne, et 43 % admettaient avoir de la difficulté à distinguer le vrai du faux. Même si ces statistiques font référence à la mésinformation, cette inquiétude croissante illustre la conscientisation du public à l'égard des enjeux posés par la désinformation et l'urgence d'y remédier efficacement.

Le problème va bien au-delà du manque de jugement de tout un chacun. Il s'agit d'un enjeu systémique qui ébranle la stabilité politique, la réputation des entreprises et la sécurité publique.

La désinformation est une nuisance, mais également une attaque directe contre le processus démocratique. Selon l'enquête de 2024 intitulée Survey of Online Harms in Canada, 38 % des Canadiens croient de fausses nouvelles au moins quelques fois par mois, ce qui révèle le degré de perfectionnement du contenu trompeur. L'ingérence étrangère, les fausses nouvelles générées par l'IA et les technologies d'hypertrucage constituent des armes pour manipuler la perception du public, polariser les communautés et influencer les résultats d'élections.

Incidence sur les entreprises et l'économie

Le monde des affaires n'est pas immunisé contre la désinformation, qui s'étend aux mèmes et médias sociaux, à la contrefaçon, à l'hypertrucage et aux plateformes de désinformation. Pour lutter contre cette tendance, les entreprises canadiennes disent avoir adopté des solutions (article en anglais seulement) comme des campagnes de marketing (afin de prévenir la prolifération d'informations fausses ou trompeuses par la conscientisation), des poursuites judiciaires, de meilleures communications avec leurs clients, la formation du personnel, et la mise en œuvre de nouvelles mesures de cybersécurité.

Les campagnes de désinformation peuvent détruire des réputations, éroder la confiance des clients et ébranler les marchés.

Selon le Global Risks Report de 2024 publié par le Forum économique mondial, la mésinformation et la désinformation restent les principaux risques à court terme à l'échelle mondiale. Des marchés financiers aux conflits géopolitiques, la distorsion de la réalité est un outil utilisé par des acteurs malintentionnés pour déstabiliser des pans entiers de la société.

Risques à surveiller

Désinformation générée par l'IA : les outils d'IA créent du faux contenu hyperréaliste et peuvent le diffuser à grande échelle, ce qui complique de plus en plus la distinction du vrai du faux.

Technologie d'hypertrucage : les attaques par hypertrucage sont fondées sur du contenu audio et vidéo très réaliste, mais faux, ce qui pose des risques importants à la confiance du public et à la sécurité.

Ingérence étrangère dans le processus démocratique : des pirates informatiques de l'étranger peuvent mener des campagnes de désinformation visant à affaiblir la démocratie canadienne en exploitant des sujets controversés.

Désinformation ciblant des étudiants internationaux : les étudiants internationaux au Canada pourraient être victimes de mésinformation liée à l'immigration, ce qui peut susciter de la confusion et même mener à de l'exploitation.

Désinformation dans les médias sociaux : les plateformes de médias sociaux sont un terreau fertile pour la désinformation, altérant la perception du public et suscitant la polémique.

Manipulation de l'opinion publique par de fausses nouvelles : la prolifération délibérée de fausses informations ou fausses nouvelles peut servir à manipuler l'opinion du public sur divers sujets.

Conflits internationaux : lors de conflits internationaux, des fraudeurs peuvent utiliser des campagnes de désinformation sophistiquées ciblant des groupes particuliers pour faire basculer l'opinion publique.

Préjudices en ligne et contenu haineux : on constate une multiplication du contenu haineux et des préjudices en ligne, souvent alimentée par la désinformation, qui nuit au bien-être des individus et divise les sociétés.

Exploitation de théories complotistes : la désinformation peut contribuer à une certaine légitimation des théories complotistes, et ainsi entraîner une perte de confiance du public envers les institutions et les experts.

Détection de la mésinformation et lutte contre celle-ci : malgré tous les efforts déployés, la détection de la mésinformation et la lutte contre celle-ci constituent d'énormes défis qui soulignent la nécessité de créer des outils et d'établir des stratégies pour aider les Canadiens à identifier les fausses informations en ligne.

Signaux d'alarme

- Prolifération de contenu viral véhiculant des affirmations non vérifiées
- Campagnes de désinformation coordonnées en lien avec des élections ou des événements mondiaux, ou ciblant des personnes ou de grandes entreprises
- Nouvelles ou enregistrements vidéo ou vocaux générés par l'IA et imitant des sources réelles
- Comptes de médias sociaux d'origine étrangère amplifiant les discours polémiques

Stratégies d'atténuation des risques

- Conscientiser les membres du public et améliorer leur culture médiatique
- Créer de meilleurs outils de vérification des faits et de détection de fausses informations
- Renforcer les cadres réglementaires, l'imputabilité et l'application des politiques
- Promouvoir la communication transparente
- Collaborer avec des partenaires mondiaux pour vérifier l'exactitude des informations

Questions à se poser

- Quelles mesures proactives avez-vous mises en place pour identifier et surveiller les sources possibles de désinformation?
- Comment votre organisation répond-elle à la désinformation après l'avoir identifiée?
- Quelle formation ou quelles ressources fournissez-vous aux membres de votre personnel pour les aider à reconnaître les fausses nouvelles et à y réagir?
- Comment votre organisation prévoit-elle renforcer ses moyens de défense contre la désinformation afin de protéger ses parties prenantes et son auditoire?

Risques liés aux tiers : les défis d'un monde interrelié

La dépendance : une menace grandissante

Les entreprises comptent sur des fournisseurs tiers pour une panoplie de services : de l'infonuagique à la cybersécurité, en passant par le soutien informatique pour des services administratifs. Or, cette dépendance n'est pas sans risques.

Même s'il appartient généralement aux intervenants de la chaîne d'approvisionnement de prendre contact avec des fournisseurs et de les gérer, les tiers jouent un rôle de plus en plus important dans la sphère des TI et de la TO. De nombreuses organisations peinent à trouver l'expertise technologique nécessaire pour faire fonctionner leurs systèmes et en faire la maintenance. Leur dépendance envers des tiers s'accroît donc d'année en année. Certaines organisations, particulièrement celles à l'extérieur des grands centres, risquent de perdre l'accès à leurs outils technologiques à défaut de trouver un fournisseur fiable.

Un seul maillon faible dans une chaîne d'approvisionnement ou un réseau de fournisseurs peut entraîner une interruption des activités, des pertes financières ou une atteinte à la réputation. Il est important de bien protéger votre organisation contre les cybermenaces, les manquements à la réglementation et les lacunes opérationnelles. Toutefois, vos partenaires externes doivent également avoir l'assurance d'être bien protégés.

Un rapport de 2024 de MNP souligne un accroissement marqué de la dépendance des entreprises canadiennes envers des tiers pour les services technologiques. Cette tendance souligne l'importance de revoir régulièrement les ententes conclues avec des tiers, les droits d'accès pour vérifier l'intégrité des contrôles de sécurité, et les clauses de responsabilité des tiers pour déterminer de façon réaliste la responsabilité qu'un tiers peut assumer.

De plus, un rapport comparatif de 2024 a révélé que 62 % des organisations ont connu des perturbations de leur chaîne d'approvisionnement en raison d'incidents de cybersécurité, une hausse de 13 % par rapport à l'année précédente.

En 2024, certaines institutions canadiennes, particulièrement dans le secteur financier, ont fait l'objet d'un contrôle plus serré en lien avec les risques posés par leurs fournisseurs tiers. Le Bureau du surintendant des institutions financières (BSIF) a exprimé des inquiétudes à propos des risques de concentration et a averti qu'une dépendance excessive envers une poignée de fournisseurs de services peut créer une vulnérabilité systémique.

Plus les entreprises ont recours à des tiers, plus la gestion des risques inhérents devient une question de survie.

Risques à surveiller

Atteinte à la cybersécurité : les fournisseurs tiers constituent une source importante d'atteinte à la sécurité des données.

Non-conformité réglementaire : le défaut de s'aligner aux nouvelles exigences réglementaires, y compris celles de vos fournisseurs tiers, pose des risques associés à la conformité technologique et à la gestion des cyberrisques.

Perturbation des activités : la dépendance de tiers envers des services essentiels augmente le risque de perturbation des activités en raison de manquements ou de la faillite d'un fournisseur.

Atteinte à la sécurité des données : toute négligence dans le traitement des données sensibles par vos fournisseurs peut poser un risque à leur confidentialité et entraîner des conséquences graves pour vous, comme des poursuites judiciaires ou une atteinte à votre réputation.

Instabilité financière des fournisseurs : la santé financière des fournisseurs tiers a une incidence directe sur la prestation de leurs services.

Vulnérabilités de la chaîne d'approvisionnement : des perturbations à l'échelle mondiale témoignent de la fragilité des chaînes d'approvisionnement, alors que les manquements possibles de la part des tiers peuvent avoir une incidence sur la disponibilité des produits et les activités d'une organisation.

Atteinte à votre réputation : la collaboration avec des tiers présentant des lacunes en fait d'éthique ou de conformité peut ternir la réputation d'une organisation et miner la confiance de ses parties prenantes.

Obligations juridiques : la gestion inadéquate des risques liés à des tiers expose les organisations à des poursuites judiciaires, surtout en présence de cas de violation de données et de non-conformité.

Décalage stratégique : l'établissement d'un partenariat avec un fournisseur externe dont les objectifs diffèrent de ceux de votre organisation peut engendrer des conflits et des pertes d'efficacité.

Trop grande dépendance envers des fournisseurs clés : le risque de concentration augmente lorsque des entreprises dépendent dans une trop grande mesure d'un petit nombre de fournisseurs.

Signaux d'alarme

- Interruptions fréquentes de services ou retards de fournisseurs clés
- Rapports d'audit réglementaire soulignant des lacunes dans la conformité des fournisseurs
- Hausse des incidents de cybersécurité liés à des partenaires externes
- Augmentation des litiges portant sur des contrats avec des fournisseurs
- Couverture médiatique négative à l'égard de problèmes d'éthique ou de manquements à la sécurité d'un fournisseur

Stratégies d'atténuation des risques

- Évaluer régulièrement les fournisseurs
- Mettre en œuvre un programme de gestion des risques liés aux tiers
- Diversifier les partenariats avec les fournisseurs
- Rédiger les contrats pour qu'ils précisent clairement les obligations de conformité et les autres protections
- Surveiller la santé financière et la stabilité des principaux fournisseurs

Questions à se poser

- Comment votre organisation procède-t-elle pour évaluer les fournisseurs tiers avant de faire affaire avec eux?
- Quels mécanismes avez-vous mis en place pour surveiller le rendement de fournisseurs tiers et leur conformité au fil du temps?
- Quels sont les protocoles de votre organisation pour répondre aux incidents ou aux atteintes à la sécurité chez un fournisseur tiers?
- Vos contrats avec des fournisseurs tiers comprennent-ils des clauses visant à gérer ou à limiter le risque?

Répondre aux besoins de demain : votre structure organisationnelle repose-t-elle sur vos infrastructures technologiques et de données?

Êtes-vous prêt pour demain?

Nous assistons actuellement à une profonde transformation du monde du travail qui force les organisations à revoir leurs structures, les méthodes de leur équipe de direction et leurs stratégies de ressources humaines.

Cependant, au moment où elles adoptent de nouvelles structures organisationnelles, les entreprises sont confrontées à des défis majeurs, comme la pénurie de main-d'œuvre, la résistance culturelle, des infrastructures désuètes et des menaces à la cybersécurité. Elles doivent définir clairement leur vision et leur stratégie pour composer avec ces nouvelles réalités. Sinon, elles risquent de prendre du retard face à la concurrence.

Risque de déconnexion

La plupart des organisations peinent à s'adapter au changement, non par manque de ressources, mais par manque de vision à l'égard de leur transformation. En l'absence d'un leadership fort, d'une ouverture aux nouvelles idées et à l'innovation, et d'une communication claire et franche, les nouvelles technologies et structures ainsi que les nouveaux modèles d'affaires risquent de sembler lourds et compliqués, plutôt que bénéfiques.

> « Elles doivent définir clairement leur vision et leur stratégie pour composer avec ces nouvelles réalités. Sinon, elles risquent de prendre du retard face à la concurrence.

Les projets de changement échouent souvent en raison d'un manque d'adhésion de l'équipe de direction. Les leaders qui n'encouragent pas activement la transformation créent de l'incertitude et de la résistance au sein de leurs équipes. Les membres du personnel ont tendance à ne pas déroger de leur petite routine, ce qui renforce le besoin d'une bonne communication et d'une gestion efficace du changement.

L'incapacité des leaders à bien expliquer les raisons et les bénéfices d'une transformation peut démotiver le personnel et même ralentir ou compromettre la mise en œuvre des nouvelles initiatives.

De plus, en raison de l'évolution des outils numériques, les membres du personnel doivent constamment parfaire leurs compétences et s'adapter aux mises à jour des systèmes. Mais de nombreuses entreprises négligent d'investir dans la formation, laissant leurs équipes dépourvues face aux nouvelles exigences.

Même si les effectifs sont bien formés et ouverts au changement, une infrastructure numérique désuète ne peut répondre aux besoins d'une entreprise d'aujourd'hui. À défaut d'investissements stratégiques dans la technologie, beaucoup d'entreprises s'exposent à des pertes d'efficacité, à des risques pour la sécurité et à une baisse de productivité.

Risques à surveiller

Défis liés à l'acquisition et à la rétention de talents : à la suite d'un important projet de transformation numérique, les organisations peuvent avoir de la difficulté à redéfinir leur structure, ainsi qu'à attirer et à garder des professionnels qualifiés, ce qui restreint leur capacité à mettre en œuvre leurs priorités.

Transformation inadéquate de la main-d'œuvre : la résistance au changement et une culture trop rigide peuvent freiner les transformations nécessaires de la main-d'œuvre et avoir une incidence sur la préparation générale des entreprises.

Vulnérabilité aux menaces à la cybersécurité : les cybermenaces posent un risque important aux organisations qui négligent de transformer leurs systèmes et qui se retrouvent démunies en cas d'attaque.

Incertitude économique et financière : les taux d'intérêt élevés et l'inflation peuvent, à long terme, créer de l'incertitude économique et mettre à l'épreuve la résilience financière.

Changements réglementaires et conformité : dans le contexte de resserrement des exigences réglementaires, les organisations doivent s'adapter rapidement ou se préparer à faire face aux conséquences financières ou juridiques possibles.

Évolution technologique et compétences de la main-d'œuvre : la technologie évolue plus rapidement que les compétences de la main-d'œuvre, ce qui accentue le besoin de formation continue et d'adaptation.

Dépendance envers des tiers : une dépendance accrue envers des fournisseurs externes peut causer des perturbations imprévues et des risques pour la sécurité, ce qui a une incidence sur la capacité de l'organisation à utiliser la technologie mise en œuvre durant la transformation.

Perturbation des activités : les perturbations de la chaîne d'approvisionnement, les ralentissements économiques ou toute autre crise peuvent provoquer le chaos au sein des organisations les mieux structurées.

Faiblesse des cadres de gestion des risques : l'absence de stratégies claires de gestion des risques peut rendre une organisation vulnérable aux nouvelles menaces et aux nouveaux défis.

Résistance culturelle au changement : les cultures organisationnelles résistantes au changement peuvent nuire à l'adhésion aux nouveaux modèles d'affaires et à l'adaptation aux nouvelles exigences du marché.

Signaux d'alarme

- Taux de roulement élevés
- Recours à des outils désuets et application de flux de travail dépassés
- Résistance des membres du personnel à de nouveaux processus et à la formation
- Atteinte fréquente à la cybersécurité ou manquements à la conformité
- Adoption lente de la technologie en raison de l'hésitation de la direction
- Sanctions réglementaires ou surveillance accrue par des organes de direction

Stratégies d'atténuation des risques

- Investir dans la gestion des talents et la formation
- Promouvoir une culture agile
- Renforcer les protections en cybersécurité
- Améliorer la résilience financière par la diversification
- S'assurer de la conformité aux changements dans la réglementation
- Gérer les risques liés aux tiers
- Élaborer des plans de continuité des activités
- Mettre en œuvre un programme complet de gestion des risques
- Lancer des initiatives de gestion du changement

Questions à se poser

- Comment votre organisation évalue-t-elle sa stratégie et les capacités de sa main-d'œuvre et comment les aligne-t-elle aux nouvelles exigences liées à la technologie et aux tendances du marché?
- Quelles stratégies avez-vous mises en place pour parvenir à un point d'équilibre entre souplesse et stabilité dans votre structure organisationnelle?
- Comment votre organisation parvient-elle à intégrer ses principes de gouvernance et son processus de prise de décisions à des structures novatrices?
- Quels mécanismes avez-vous établis pour surveiller et adapter votre structure organisationnelle en réponse aux changements internes et externes?

Risque d'assurance : le diable se cache dans les détails

Les clauses en petits caractères n'ont jamais été aussi importantes.

Comme bon nombre d'autres secteurs d'activité, le secteur canadien de l'assurance est aux prises avec des risques sans précédent, qui vont des incidences des changements climatiques à la montée des taux de criminalité, en passant par une dynamique de marché en mutation et une réglementation changeante. Au moment où les assureurs, les organisations et les autorités tentent de retrouver leurs marques dans cette nouvelle ère, il est devenu essentiel de lire et de comprendre les clauses en petits caractères des contrats.

De plus en plus fréquents et coûteux, les phénomènes météorologiques extrêmes exercent d'immenses pressions sur le secteur de l'assurance. En effet, au cours de la dernière décennie, les pertes assurées découlant de catastrophes naturelles se sont élevées en moyenne à 2,2 M$ par année, un seuil trois fois plus élevé par rapport à la moyenne mobile sur 10 ans, selon le Bureau d'assurance du Canada. À lui seul, le feu de forêt à Jasper, en 2024, a causé des pertes assurées de 880 millions de dollars.

En réponse à cela, les assureurs révisent leurs modèles de risque, augmentent les primes pour les secteurs à risque élevé et resserrent les modalités des couvertures offertes. Les entreprises canadiennes doivent se préparer à une montée des coûts, à un accroissement de la surveillance et à la non-couverture de certains éléments

> « Les entreprises canadiennes doivent se préparer à une montée des coûts, à un accroissement de la surveillance et à la non-couverture de certains éléments.

Conditions de marché en mutation

Malgré les difficultés mentionnées ci-dessus, le marché de l'assurance continue de faire preuve de résilience. Selon CMB Insurance Brokers, la baisse de un pour cent des primes d'assurance commerciale enregistrée au troisième trimestre de 2024 est le signe d'une intensification de la concurrence entre assureurs. Cela dit, étant donné que les catastrophes telles que les feux de forêt à Jasper et en Colombie-Britannique font grimper le nombre de réclamations, plusieurs assureurs choisissent d'appliquer des processus de souscription et de sélection des risques plus stricts.

Les organismes de réglementation accentuent également leur surveillance. Le Bureau du surintendant des institutions financières (BSIF) a indiqué que les taux d'intérêt élevés, l'instabilité des marchés et les risques climatiques figuraient au nombre de ses principales préoccupations pour 2024 et 2025. Les institutions financières, telles les banques, doivent maintenant envisager d'intégrer des évaluations des risques climatiques et de renforcer leur gestion du capital pour préserver leur résilience.

Étant donné que, collectivement, les catastrophes naturelles, les vols de voitures et la volatilité des marchés façonnent l'avenir de l'assurance au Canada, les parties prenantes doivent miser davantage sur l'innovation et la collaboration. Pour les assureurs, la gestion de ces défis passe par l'amélioration de la modélisation des risques, l'adoption de nouvelles technologies et la prise de mesures réglementaires proactives.

Pour les entreprises, cela signifie qu'il faut comprendre les risques et adopter des mesures préventives pouvant aider à en atténuer les incidences financières et à assurer un accès continu à une couverture d'assurance à prix abordable.

Risques à surveiller

Pour l'assuré

Accroissement de la fréquence et de la gravité des catastrophes naturelles : la montée des dommages causés par les feux de forêt, les inondations et les orages violents se traduira par une hausse des réclamations.

Risques géopolitiques : les tensions politiques et les conflits à l'échelle mondiale créent des incertitudes qui ont des effets sur la stabilité des marchés et les stratégies de placement.

Inflation médicale : l'augmentation des coûts des soins de santé entraîne un accroissement des dépenses liées aux réclamations et pousse les assureurs de soins médicaux à revoir leurs primes et limites de couverture.

Risques liés aux biens : la hausse de la valeur des biens immobiliers et des coûts de construction, de concert avec des catastrophes naturelles plus fréquentes, augmente le nombre de réclamations, ainsi que la complexité et le coût des activités de souscription.

Verdicts de responsabilité : une augmentation des verdicts de responsabilité importants, influencée par l'inflation sociale, peut se traduire par une hausse du montant des règlements et des ajustements à la couverture pour l'assurance responsabilité.

Pour les assureurs

Cybermenaces : la hausse du nombre de cyberattaques, y compris les interruptions technologiques à l'échelle mondiale, pose de sérieux problèmes et force les assureurs à se préparer à une vague de réclamations et à réévaluer les normes de souscription.

Percées technologiques : l'IA et les innovations technologiques créent à la fois des possibilités et des défis; les outils numériques qu'utilisent les assureurs doivent continuellement évoluer pour que ces derniers demeurent concurrentiels.

Incertitude économique : les fluctuations des taux d'intérêt et de la conjoncture ont une incidence sur les rendements des placements ainsi que sur la stabilité financière globale des assureurs.

Acquisition et fidélisation des talents : le secteur de l'assurance éprouve des difficultés à attirer et à fidéliser des professionnels compétents, ce qui influe sur l'efficience opérationnelle et l'innovation.

Évolution de la réglementation : l'évolution de la réglementation pousse les assureurs à s'adapter rapidement pour remplir leurs obligations, à défaut de quoi ils seront aux prises avec des cas de non-conformité susceptibles d'entraîner des répercussions juridiques et financières.

Signaux d'alarme

- Hausse des coûts de réassurance et couverture limitée pour les éléments à risque élevé
- Augmentation des surprimes d'assurance automobile
- Retards dans la souscription d'assurance cybersécurité en raison de préoccupations relatives aux risques
- Taux de roulement élevé des employés au sein des compagnies d'assurance, ayant des incidences sur l'efficience de la souscription et du traitement des réclamations

Stratégies d'atténuation des risques

- Élaborer une évaluation des risques climatiques
- Renforcer les mesures de cybersécurité
- Surveiller l'environnement géopolitique
- Mettre en place des mesures de contrôles des coûts des soins de santé
- Réévaluer les pratiques de souscription pour les biens immobiliers
- Identifier et traiter les expositions en matière de responsabilité
- Assurer la conformité réglementaire
- Investir dans les technologies avancées et la formation
- Accroître la résilience financière par l'entremise de la diversification
- Mettre en place des programmes pour attirer, former et fidéliser les employés compétents

Questions à se poser

- Quels types de couvertures d'assurance sont essentielles pour votre organisation compte tenu de son secteur, de ses activités et de ses obligations légales?
- À quelle fréquence votre organisation examine-t-elle et met-elle à jour ses polices d'assurance pour tenir compte des changements survenus dans ses activités, ses actifs ou son exposition aux risques?
- Quelles stratégies sont en place pour réduire les réclamations éventuelles, comme la mise en œuvre de programmes de gestion des risques, de séances de formation à l'intention des employés ou de protocoles de sécurité?
- De quelle façon votre organisation maintient-elle sa conformité avec les exigences des polices et les obligations réglementaires afin d'éviter les refus de couverture ou les pénalités?

Résilience à l'épreuve du temps : être audacieux et agile

L'agilité est l'avantage concurrentiel par excellence.

De nos jours, il faut être proactif pour exploiter une entreprise. Pour garder une longueur d'avance, votre organisation doit penser plus intelligemment, agir plus rapidement et anticiper les défis émergents.

La montée des coûts continue d'être un défi majeur pour les entreprises canadiennes. En effet, selon Statistique Canada, 62,5 pour cent des entreprises anticipent d'avoir à surmonter des obstacles liés aux coûts pendant le premier trimestre de 2025.

De plus, l'incidence à long terme des taux d'intérêt et des coûts d'emprunt pèse sur les organisations. Ces pressions financières limitent les investissements dans la croissance, les technologies et le perfectionnement de la main-d'œuvre et font de la résilience financière une priorité.

Le marché du travail continue d'être sous pression et de représenter un enjeu important pour les entreprises modernes. En fait, d'après la même étude de Statistique Canada, le coût de la main-d'œuvre est l'obstacle auquel les entreprises s'attendent le plus au deuxième trimestre de 2025. Sans accès à des talents, une organisation risque de perdre du terrain au chapitre de la productivité, de l'innovation et de la prestation des services. Elles sont donc nombreuses à se tourner vers l'automatisation, l'amélioration des compétences et les nouvelles stratégies de recrutement.

> « Sans accès à des talents, une organisation risque de perdre du terrain au chapitre de la productivité, de l'innovation et de la prestation des services.

Même si un plus petit nombre d'entre elles mentionnent les perturbations de la chaîne d'approvisionnement parmi leurs principales préoccupations, environ 16 pour cent des entreprises continuent de s'y attendre. Les retards, les pénuries de stocks et la hausse des coûts de transport continuent de peser sur les activités. Pour garder une longueur d'avance, les entreprises doivent diversifier leurs fournisseurs, renforcer la logistique et investir dans une gestion plus intelligente de leurs stocks.

Le BSIF a souligné que les cybermenaces, une dépendance excessive à l'égard de certains fournisseurs, la fraude et les vulnérabilités technologiques constituent des risques pressants pour les entreprises. Comme elles s'appuient de plus en plus sur l'infrastructure numérique, elles seront plus exposées à des fuites de données, à des attaques au rançongiciel et à des cybermenaces visant la chaîne d'approvisionnement, ce qui ne manquera pas de mettre à l'épreuve leur résilience opérationnelle.

Malgré ces difficultés, bon nombre d'entreprises sont prudentes, mais continuent de voir le bon côté des choses. Statistique Canada a indiqué que près des trois quarts (73,1 %) des entreprises sont très optimistes ou plutôt optimistes quant à leurs perspectives pour 2025. La proportion d'entre elles ayant fait état de projections optimistes demeure supérieure à 70 pour cent, et ce, depuis le deuxième trimestre de 2024.

Risques à surveiller

Interruption des activités : des cyberincidents, des catastrophes naturelles ou des défaillances de la chaîne d'approvisionnement pourraient perturber les activités.

Cybermenaces : l'augmentation de la fréquence et du degré de complexité des cyberattaques représente une menace substantielle pour la continuité des activités.

Catastrophes naturelles : des inondations, des feux de forêt et des orages violents pourraient endommager des biens et perturber la chaîne d'approvisionnement, mettant du même coup la résilience opérationnelle à l'épreuve.

Perturbations de la chaîne d'approvisionnement : des problèmes d'envergure mondiale ou régionale touchant la chaîne d'approvisionnement pourraient influer sur la livraison des biens et la prestation des services.

Changements dans la réglementation : l'évolution de la réglementation force les entreprises à s'adapter rapidement pour pouvoir demeurer conformes.

Acquisition et fidélisation des talents : les difficultés liées à l'attrait et à la fidélisation de travailleurs compétents affectent l'efficience opérationnelle et l'innovation.

Incertitude économique : l'inflation, les taux d'intérêt, les coûts d'emprunt et la volatilité des marchés continueront de créer de l'instabilité financière pour les entreprises.

Risques liés aux tiers : le recours à des fournisseurs entraîne des vulnérabilités liées à la continuité des services et à la conformité.

Percées technologiques : puisque les changements technologiques nécessitent une adaptation continue, les entreprises qui veulent rester concurrentielles doivent faire preuve d'agilité dans l'intégration des nouvelles technologies.

Incertitude géopolitique : les tensions mondiales créent une incertitude qui pourrait avoir des incidences sur la stabilité des marchés et les activités commerciales.

Signaux d'alarme

- Arrêt imprévu des activités en raison de cyberattaques, de phénomènes météorologiques ou de défaillances des fournisseurs
- Augmentation des primes d'assurance et de la surveillance réglementaire liée aux risques climatiques et au risque de non-conformité dans certains secteurs d'activité, à moins que les organisations adoptent des technologies de prédiction plus poussées
- Retards dans l'embauche pour les postes clés, qui ralentissent la productivité
- Perturbations fréquentes dans la performance des fournisseurs ou problèmes de conformité éprouvés par des partenaires externes
- Mentions de retards dans les mises à niveau relatives à la cybersécurité

Stratégies d'atténuation des risques

- Élaborer un plan complet de continuité des activités
- Renforcer les mesures de cybersécurité
- Mettre en place des cadres de gestion des risques
- Effectuer une vigie des tendances économiques
- Diversifier les stratégies relatives aux talents
- Rehausser la résilience de la chaîne d'approvisionnement
- Gérer les risques liés aux tiers
- Surveiller la conformité réglementaire
- Adopter des technologies émergentes
- Rester au fait de l'évolution de la scène géopolitique

Questions à se poser

- De quelle façon votre organisation favorise-t-elle l'adaptabilité et l'apprentissage continu au sein de sa main-d'œuvre?
- Quels systèmes et stratégies sont en place pour assurer que la prise de décisions est agile et fondée sur des données en temps réel?
- De quelle façon votre organisation favorise-t-elle une culture de l'innovation tout en respectant ses valeurs fondamentales et en assurant sa stabilité?
- Quelles mesures prenez-vous pour évaluer et atténuer les risques causés par des facteurs externes, comme les ralentissements économiques, l'instabilité politique ou les cybermenaces?

L'avenir de la gouvernance : des conseils d'administration à l'affût des risques

Les conseils du futur devront être tout aussi diversifiés et qualifiés que les personnes qu'ils régissent.

Le rôle des conseils d'administration est en voie de subir des bouleversements sismiques alimentés par les percées technologiques, la volatilité économique, les changements dans la réglementation et les attentes des parties prenantes. Pour continuer d'être des gardiens efficaces, les conseils doivent s'adapter en même temps que les entreprises, élargir leur expertise et affiner continuellement leurs stratégies de gouvernance.

Au fil de l'évolution des risques, certaines organisations se poseront les questions suivantes : est-ce qu'un programme de perfectionnement continu devrait être obligatoire pour les membres du conseil? Est-ce qu'une meilleure connaissance de l'IA, des cyberrisques et de la durabilité améliorerait la prise de décisions et la veille stratégique?

Acquérir un avantage concurrentiel

La diversité au sein du conseil n'est plus un impératif de nature éthique; c'est un atout. Les Autorités canadiennes en valeurs mobilières (ACVM) ont relevé que 29 % des postes d'administrateurs des plus importantes sociétés cotées du Canada sont actuellement occupés par des femmes. De plus, les nouvelles lignes directrices d'Institutional Shareholder Services exigent que les sociétés comprises dans l'indice composé S&P/TSX aient au moins un administrateur qui soit d'une origine ethnique diverse.

Bien qu'on observe des progrès sur ce plan, il vaut la peine de rappeler à quel point il est important que les organes de direction aient des perspectives diversifiées pour favoriser l'innovation, la résilience et la confiance du public. Ils doivent élargir leur champ d'action traditionnel et ne pas se limiter à la stabilité financière de l'organisation et la capacité de la direction à réaliser le plan stratégique. Les administrateurs et les membres de la direction qui encouragent l'agilité et l'innovation seront valorisés et essentiels pour pousser l'organisation à être plus progressive face à l'incertitude mondiale et économique.

> « Est-ce qu'une meilleure connaissance de l'IA, des cyberrisques et de la durabilité améliorerait la prise de décisions et la veille stratégique?

Les conseils sont également aux prises avec une montée des inspections réglementaires. Les ACVM ont proposé le Règlement 51-107 dans le but de standardiser l'information liée aux questions climatiques. Si ce règlement est adopté, les entreprises devront intégrer d'emblée les risques climatiques dans la gouvernance, à défaut de quoi elles s'exposeront à des pénalités et à un ternissement de leur réputation.

De plus, les agences de conseil en vote comme Glass Lewis ont relevé qu'une piètre surveillance de la cybersécurité peut se traduire par des recommandations négatives relativement aux administrateurs, en particulier dans le cas des organisations qui ont été considérablement touchées par des cyberincidents. Les conseils doivent collaborer avec la direction pour améliorer les mesures de cybersécurité et s'assurer de demeurer résilients devant les menaces numériques.

Risques à surveiller

Activisme actionnarial : étant donné que les actionnaires engagés exercent d'importantes pressions sur les conseils, ces derniers se doivent d'être transparents et activement mobilisés.

Diversité et inclusion : les changements à la réglementation et aux politiques relatives aux conseils en vote qui sont en vigueur soulignent l'importance de la diversité au sein des conseils.

Cybermenaces : la montée des cyberattaques et des attaques au rançongiciel met à l'épreuve la surveillance exercée par le conseil.

Conformité réglementaire : les changements à la réglementation, en particulier ceux qui se rapportent aux facteurs ESG, exigent qu'on leur accorde plus d'attention et qu'on y consacre plus de ressources.

Perfectionnement des talents et planification de la relève : les conseils doivent se concentrer sur l'évaluation des dirigeants actuels et l'identification des lacunes dans le pipeline de talents afin de guider l'entreprise dans un environnement d'affaires dynamique.

Incertitude économique : l'inflation, les taux d'intérêt et la volatilité des marchés des capitaux pourraient affecter la stabilité financière et nécessiter une orientation de la part du conseil.

Intégration des technologies : les nouvelles technologies permettant d'améliorer les activités peuvent représenter à la fois une possibilité et un obstacle et nécessitent une surveillance accrue.

Gestion de la réputation et de l'image de marque : l'accroissement de la surveillance dans les médias sociaux et des attentes du public signifie que les conseils doivent régler rapidement les crises.

Risques liés aux tiers : la gestion des risques associés aux fournisseurs externes est un élément qui gagne en importance au chapitre de la résilience opérationnelle.

Signaux d'alarme

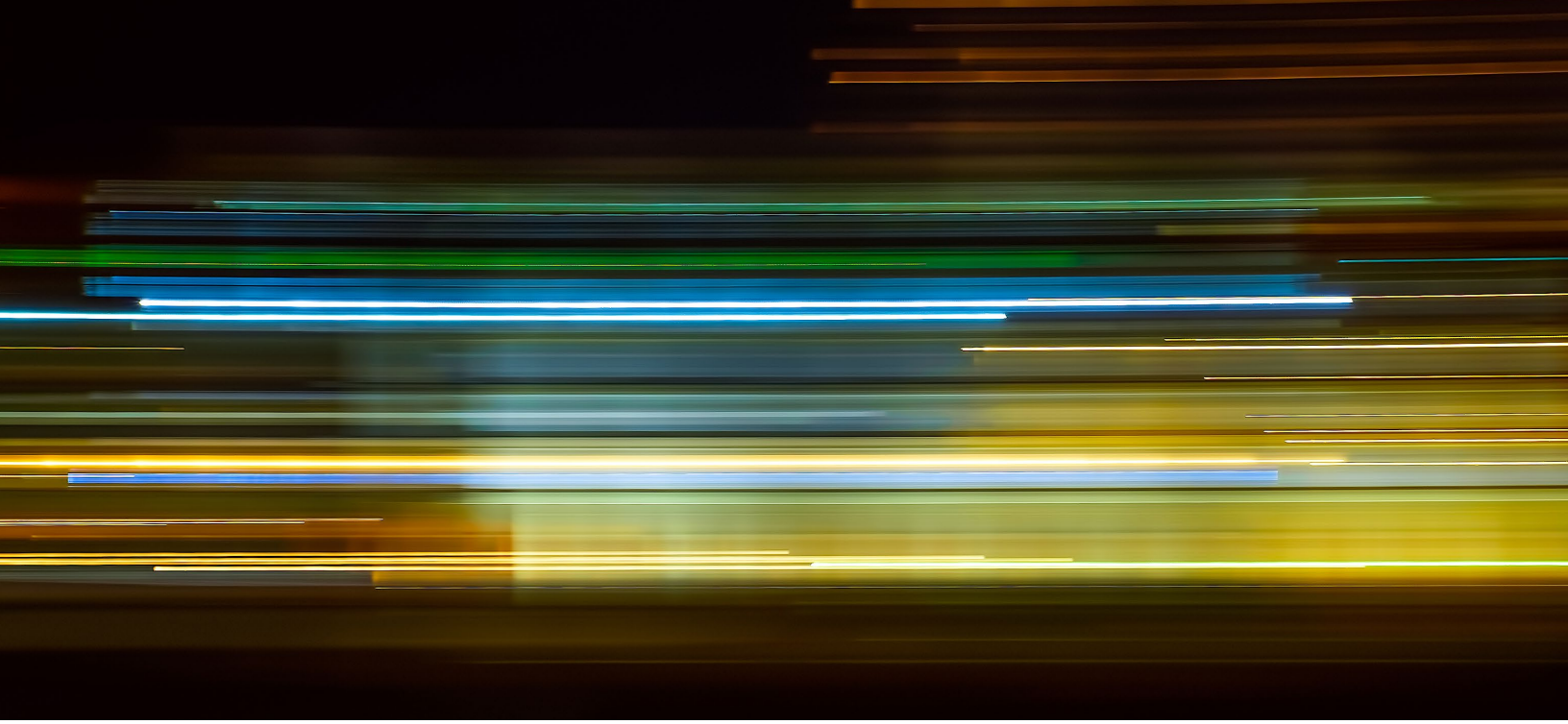
- Accroissement de la fréquence des plaintes d'actionnaires et des courses aux procurations
- Augmentation de la gravité des cyberincidents en raison du manque de surveillance
- Identification de cas de non-conformité au cours d'audits réglementaires
- Baisse de la confiance des investisseurs, qui se traduit par des fluctuations du cours de l'action ou des critiques ouvertes
- Retard dans l'adoption des technologies émergentes en raison de l'hésitation ou du manque d'expertise du conseil
- Taux de roulement élevé au sein de la haute direction
- Atteinte à la réputation découlant de bévues en matière d'environnement, d'éthique ou de gouvernance

Stratégies d'atténuation des risques

- Mettre en place une formation continue en gouvernance
- Maintenir des communications transparentes et des relations proactives avec les investisseurs
- Évaluer régulièrement les cyberrisques et offrir de la formation à ce sujet
- Accroître la diversité
- Rester à l'affût des lois touchant les facteurs ESG et autres règlements connexes
- Effectuer une vigie des tendances économiques
- Adopter des technologies évolutives pour répondre aux besoins changeants de l'entreprise
- Identifier tôt les futurs dirigeants et mettre en place des pipelines de membres éventuels de la haute direction
- Aligner les stratégies commerciales sur les initiatives visant la durabilité et la résilience
- Gérer les relations avec les tiers
- Gérer activement l'intégrité de la réputation et de l'image de marque

Questions à se poser

- Quels sont les processus en place pour faire en sorte que votre conseil dispose de la bonne combinaison de compétences, d'expertise et de diversité?
- Comment votre conseil reste-t-il au fait de l'évolution des exigences réglementaires et des exigences de gouvernance?
- Quels cadres ou pratiques de gouvernance votre conseil utilise-t-il pour faire le suivi de la gestion des risques?
- De quelle façon votre organisation évalue-t-elle la performance et la reddition de compte du conseil? Comment l'améliore-t-elle?



C’est à vous de jouer

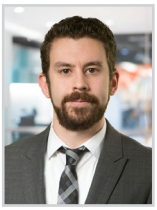
La nature des risques a changé, et notre réponse à ceux-ci doit aller dans le même sens. Aujourd’hui, les menaces sont plus soudaines, complexes et interreliées que jamais auparavant. Toutefois, si votre organisation dispose des bons conseils et se dote d’une stratégie proactive, elle pourra transformer l’incertitude en possibilité.

L’avenir appartient à ceux qui sont prêts.

Voyons ensemble comment votre organisation peut anticiper ce que demain lui réserve.

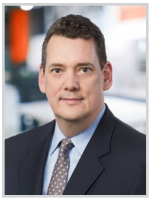
Collaborateurs

Richard Arthurs
Associé | Leader national, Audit interne



Drew Buhr
Associé | Leader national, Bilan de cybersécurité, Solutions numériques

Craig Burkart
Associé | Leader national, Services-conseils en assurances



Gord Chalk
Associé | Leader, Consultation, Énergie et services publics

Caitlin Crowley
Associée | Leader nationale, Transformation d'entreprise, Solutions numériques

Catharine Dutt
Associée | Gestion des risques d'entreprise

James Dyack
Associé | Évaluations et soutien en litige

Johnny Earl
Directeur général, Financement d'entreprises

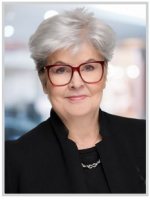
Mariesa Fett
Associée | Leader nationale, Gestion des risques d'entreprise

Soumya Ghosh
Associé | Solutions numériques

Denise Gigova
Associé | Leader nationale, Transformation numérique, Solutions numériques

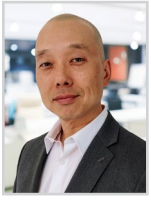
Adriana Gliga-Belavic
Associée | Confidentialité et gouvernance des données

Wendy Gnenz
Associée | Solutions numériques

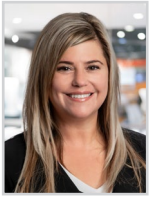


Mary Larson
Associée | Consultation stratégique et services-conseils

Chris Law
Associé | Solutions numériques



Jason J. Lee
Associé | Solutions numériques



Lisa Majeau-Gordon
Associée | Leader nationale, Juricomptabilité et soutien en litige

Eugene Ng
Associé | Leader, Cybersécurité, Gestion des risques d'entreprise

Collaborateurs

Cameron Ollenberger
Associé | Gestion des risques d'entreprise

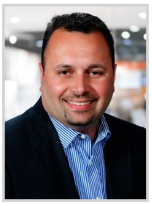
Edward Olson
Associé | Leader ESG, Gestion des risques d'entreprise

Hash Qureshi
Associé | Gestion des risques d'entreprise

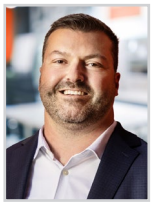
Phil Racco
Associé | Gestion des risques d'entreprise et gestion des risques liés aux tiers

Mark Reynolds
Directeur général, Financement d'entreprises

Mike Reynolds
Directeur général, Financement d'entreprises

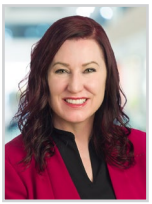


Geoff Rodrigues
Associé | Gestion des risques d'entreprise

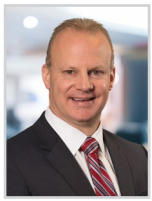


Adam Taylor
Associé | Gestion des risques d'entreprise

Lee Thiessen
Associé | Vice-président, Immobilier et construction



Gina Thornton
Associée | Gestion des risques d'entreprise



Cliff Trollope
Associé | Leader national, Résilience organisationelle

Colin Wenngatz
Associé | Données et analyses

Lanny Westersund
Associé | Consultation

Giovanni Worsley
Associé | Fiscalité foncière

Un cabinet bien d'ici

D'envergure nationale et d'intérêt local, MNP est l'un des principaux cabinets de services professionnels du Canada, fièrement au service des particuliers, des entreprises et des organisations depuis 1958. Grâce au développement de relations solides, nous fournissons des services de comptabilité, de services-conseils, de fiscalité et des services numériques axés sur le client. Nos clients bénéficient de stratégies personnalisées et d'une perspective locale qui leur permettent de réussir partout où les affaires les mènent.

Pour obtenir plus de renseignements, veuillez vous adresser à :

Richard Arthurs, FCPA, FCMA, MBA, CFE, CIA, CRMA, QIAL
Leader national, Audit interne
richard.arthurs@mnp.ca

Mariesa Fett, CPA, CA, ABCP, CRMA, IAS.A
Leader nationale, Gestion des risques d'entreprise
mariesa.fett@mnp.ca

PRAXITY®
A member of the Praxity Global Alliance