



BAC
Bureau d'assurance
du Canada

Le marché canadien de la cyberassurance

**Assurer les cyberrisques
dans une économie
interconnectée**



iStock™
Credit: sankai

Octobre 2026

FPO

Résumé

Le présent rapport établit que le marché canadien de la cyberassurance continue de se développer, les assureurs portant une attention accrue à la gravité des pertes, à l'interconnexion croissante des systèmes numériques et à l'écart persistant dans le recours à la cyberassurance par les petites et moyennes entreprises (PME).

Trois constats principaux y sont présentés.

1

Les conditions du marché se sont stabilisées. À l'issue d'une période marquée par la hausse des demandes de règlement et les ajustements de souscription, la performance des assureurs s'est nettement améliorée ces dernières années. Les données de l'industrie laissent entrevoir une accalmie de la période de rapports sinistres/primes élevés, les résultats récents témoignant d'un retour à des conditions de marché plus habituelles.

2

Les demandes de règlement individuelles demeurent importantes. Les cyberincidents peuvent être dispendieux et perturbateurs, et engendrent souvent plusieurs coûts simultanés, dont des pertes d'exploitation, des pertes liées à la fraude, des coûts d'intervention et des obligations liées à la protection de la vie privée. Malgré l'amélioration de la performance du marché, les cyberattaques de grande ampleur continuent d'influer sur les statistiques des sinistres et sur la souscription.

3

Les technologies partagées influencent de plus en plus les cyberrisques. Nombre d'organisations utilisent les mêmes serveurs infonuagiques, plateformes logicielles et fournisseurs d'accès Internet. Par conséquent, elles sont nombreuses à être simultanément touchées par la perturbation d'une technologie partagée, ce qui entraîne un risque de pertes à grande échelle.

En plus d'offrir une protection financière, de nombreuses polices de cyberassurance donnent aux entreprises l'accès à des services spécialisés d'intervention en cas d'incident, notamment une expertise juridique, judiciaire et en rétablissement.

Il est à noter que de nombreuses PME n'ont souscrit aucune cyberassurance. Selon un sondage mené par le Bureau d'assurance du Canada (BAC), en 2025, seuls 22 % des PME détenaient une cyberassurance et à peine 12 % disposaient d'une cyberassurance autonome¹.

Dans l'ensemble, le marché canadien de la cyberassurance est plus stable qu'il ne l'était entre 2019 et 2021, années où les pertes liées aux rançongiciels ont atteint un sommet. Pour le marché, l'enjeu fondamental n'est plus de s'attaquer uniquement aux incidents cybernétiques individuels, mais plutôt de comprendre comment les sinistres graves, les dépendances technologiques partagées et l'interconnexion numérique croissante influencent le cyberrisque dans l'ensemble de l'économie.

L'importance croissante de la cyberassurance

Les cyberincidents ont des conséquences financières et réputationnelles immédiates et importantes. Une violation grave peut entraîner une perte d'exploitation, des coûts de récupération des données, des frais juridiques et judiciaires, des obligations liées à la protection de la vie privée, des pertes liées

à la fraude et une atteinte à la réputation. Les organisations canadiennes sont de plus en plus nombreuses à subir ces conséquences^{2,3}.

La cyberassurance ne se limite pas à couvrir les pertes liées à un incident. Les assureurs participent de plus en plus à l'intervention en cas d'incident. Ils offrent un accès rapide à une expertise judiciaire, juridique et en rétablissement. Une intervention précoce permet de contenir rapidement les incidents et d'en atténuer les conséquences financières^{4,5}.

L'intervention précoce des assureurs est particulièrement importante, car les cyberincidents ne se limitent plus aux entreprises individuelles : ils peuvent se propager à de vastes réseaux, ce qui perturbe les activités en plus d'avoir des répercussions sur les fournisseurs, les clients et les fournisseurs de services. La participation des assureurs est d'autant plus pertinente au Canada, où les PME jouent un rôle de premier plan dans les chaînes d'approvisionnement et les économies locales⁶.

En raison de ses exigences de souscription (p. ex. veiller à ce que les organisations offrent à leur personnel une formation en cybersécurité et qu'elles mettent régulièrement à jour leurs logiciels de sécurité), la cyberassurance favorise également la préparation.

1 Bureau d'assurance du Canada, [Sondage sur la cybersécurité 2025](#).

2 IBM Canada, [IBM Report: Canadians' Data Security Under Increased Threat, While Breach Costs Surge](#), IBM Newsroom Canada, 30 juillet 2025.

3 Maude St-Georges et coll. ["Tendances en matière de cyberassurance : Perspectives 2026 sur les incidents de confidentialité – Partie 5"](#), McCarthy Tétrault, 7 mai 2026.

4 *Ibid.*

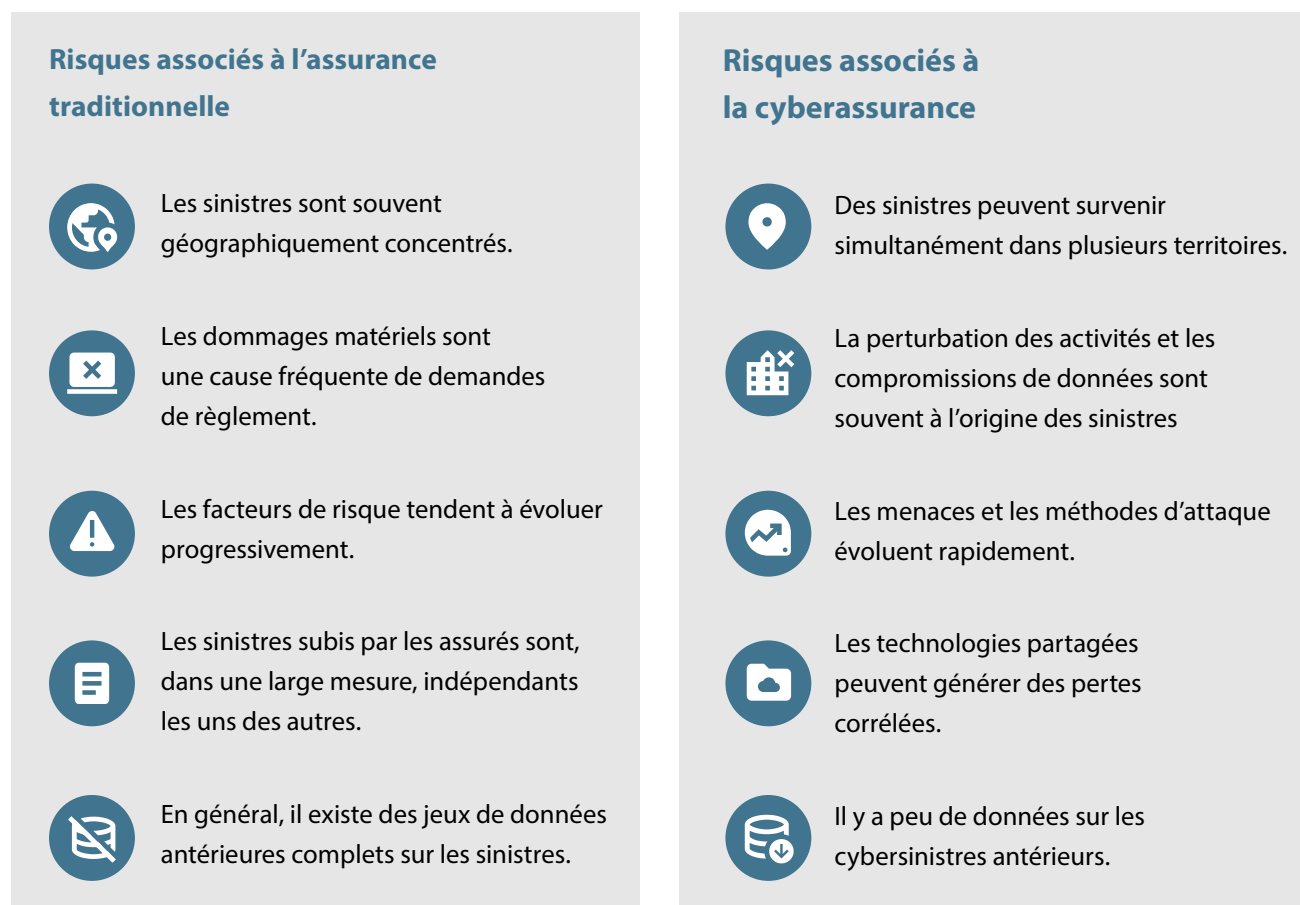
5 Coalition, ["Coalition 2025 Cyber Claims Report Finds Ransomware Stabilized but Remains Costly for Businesses"](#), Coalition, May 7, 2025.

6 *Ibid.*

En quoi le cyberrisque est-il différent à assurer?

La cyberassurance partage certes de nombreuses caractéristiques communes avec d'autres formes d'assurance des entreprises, mais elle présente des défis distincts. La figure 1 dresse une comparaison des risques associés à l'assurance traditionnelle et à la cyberassurance.

Figure 1. Comparaison des risques associés à l'assurance traditionnelle et à la cyberassurance

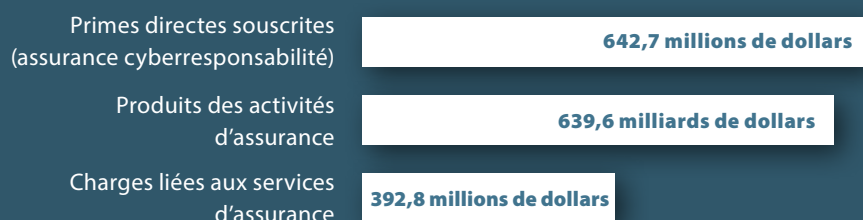


L'observabilité et la vérifiabilité des risques sont d'autres différences importantes entre l'assurance traditionnelle et la cyberassurance. Dans l'assurance des biens traditionnelle, de nombreux facteurs de risque de souscription, comme les mesures de protection incendie, la construction du bâtiment et son occupation, sont tangibles et relativement faciles à évaluer. De nombreux contrôles en matière de cybersécurité, pratiques de gouvernance et dépendances à l'égard de tiers peuvent évoluer rapidement; ils ne sont pas nécessairement directement observables ni indépendamment vérifiables au moment de la souscription.

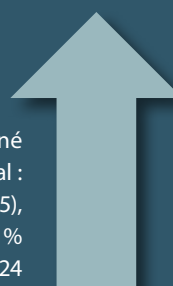
Vue d'ensemble du marché

Les entreprises canadiennes sont de plus en plus nombreuses à souscrire une cyberassurance, mais les résultats récents pointent vers une phase plus mature, caractérisée par une performance stable, une pression persistante exercée par les demandes de règlement et une garantie inégale.

Performance du marché (2025)



Ratio combiné
global :
72,6 % (2025),
contre 57,4 %
en 2024



Environnement de risque

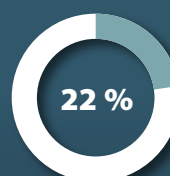
Coût moyen d'une fuite de données au Canada :
\$7.11 million in 2026⁷

↑ **\$6,98 millions de dollars (2025)⁸**

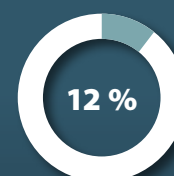
Entreprises visées par des incidents de
cybersécurité : **16 % (2023)⁹**

Pertes liées à la fraude déclarées au Canada :
plus de 704 millions de dollars (2025)¹⁰

Écarts en matière de garanties et de protection



PME ayant
souscrit une
cyberassurance



PME ayant souscrit
une cyberassurance
autonome¹¹

FPO

⁷ IBM, 2026. *Cost of a Data Breach Report 2026*.

⁸ IBM, 2025. *IBM Cost of a Data Breach Report*.

⁹ Statistique Canada, 2024. *L'incidence du cybercrime sur les entreprises canadiennes, 2023*.

¹⁰ CAEC.

¹¹ IBC 2025 Cyber Security Survey.

Rendement du marché

Les conditions du marché demeurent stables, mais les résultats récents laissent entrevoir une modération de la performance alors que la pression exercée par les demandes de règlement refait surface.

Pendant la pandémie de COVID-19, de nombreuses entreprises ont adopté le télétravail; les cybercriminels ont profité des possibilités accrues d'attaquer les systèmes informatiques, comme la plus grande dépendance des employés aux appareils mobiles et les réseaux Wi-Fi moins sécurisés. La fréquence élevée des cyberattaques et

des attaques par rançongiciel a entraîné une période de forte correction, s'accompagnant d'importantes pertes techniques.

Les données probantes semblent désormais indiquer une stabilisation. Les conditions du marché demeurent plus favorables qu'au cours de la période de fortes pertes, mais l'amélioration linéaire de la performance a cessé.

Les données antérieures illustrent l'ampleur du cycle de souscription et la correction subséquente du rendement du marché.

Figure 2. Résultats de la norme IFRS 4¹³

Année	Primes directes (en millions de dollars)	Coûts des demandes de règlement en millions de dollars)	Ratio combiné des pertes
2018	92	42	79 %
2019	136	118	130,9 %
2020	224	600	402,1 %
2021	329	322	146,6 %
2022 ¹²	477	(135)	3,3 %

Accounting system for insurance contracts before January 1, 2023.

¹² Les provisions pour sinistres constituées par les cyberassureurs canadiens se sont avérées plus importantes que prévu et ont été débloquées, ce qui s'est traduit par des coûts de sinistres agrégés négatifs pour l'année.

¹³ This ratio is a key profitability measure of insurance service result and represents the relationship between claims costs and insurance service result that are directly attributable to insurance contracts and insurance revenue.

Figure 3. Résultats de la norme IFRS 17¹⁴

Année	Produits des activités d'assurance (en millions de dollars)	Charges afférentes aux activités d'assurance (en millions de dollars)	Ratio combiné global
2023	550	458	93,6 %
2024	650	252	49,2 %
2025	639	392	66,0 %

Source : Données de MSA Research transmises au BAC, 2026.

Après des années de sinistres record, les résultats se sont nettement améliorés sur le marché, l'année 2025 témoignant de la stabilisation du marché du point de vue de la tarification et des sinistres, ainsi que de la normalisation de la performance.

Ces résultats donnent à penser que le marché ne se durcit pas et qu'il ne retombe pas dans la grave détérioration observée pendant les années de pertes record. L'année 2025 traduit plutôt un ralentissement par rapport à des conditions exceptionnellement favorables. Concrètement, le marché s'est stabilisé tout en demeurant sensible aux variations dans la gravité des sinistres¹⁵.

Les déclarations des courtiers viennent confirmer cette interprétation. Les conditions concurrentielles ont persisté jusqu'en 2025, bien que la baisse des tarifs ait commencé à ralentir au début de 2026, les assureurs se concentrant davantage sur la stabilité de

leurs portefeuilles. Les acteurs du marché continuent de faire état d'une capacité de souscription adéquate, mais notent également un contrôle accru des souscriptions dans les secteurs où les statistiques des sinistres et les inquiétudes liées au cyberrisque systémique sont élevés^{16,17}.

La tarification, les conditions et les capacités de souscription semblent plus étroitement liées à la robustesse des contrôles, de la gouvernance et des capacités d'intervention en cas d'incident d'une organisation¹⁸.

Ces tendances indiquent un marché plus mature, plus stable et plus sélectif. La phase de correction a permis de restaurer, dans une large mesure, la rigueur en matière de souscription. La performance actuelle du marché témoigne d'une attention constante portée à la gravité des sinistres, à la rigueur dans la souscription et à l'accumulation des risques.

¹⁴ La Norme internationale d'information financière 17 (IFRS 17), entrée en vigueur le 1^{er} janvier 2023, a modifié certains concepts fondamentaux, ainsi que le mode de présentation des indicateurs financiers. Par conséquent, les résultats financiers antérieurs à 2023 sont similaires, mais pas exactement comparables.

¹⁵ MSA Research, données agrégées sur les demandes de règlement soumises aux assureurs, transmises au BAC, 2026.

¹⁶ Willis Towers Watson, 2026. ["Cyber Risk: A Look Ahead to 2026."](#)

¹⁷ Gallagher, 2026. ["2026 Cyber Insurance Market Outlook."](#)

¹⁸ Willis Towers Watson, 2025. ["Insurance Marketplace Realities 2026: Cyber Risk."](#)

Structure du marché

Le marché canadien de la cyberassurance est devenu plus spécialisé et plus sensible aux risques, la rigueur en matière de souscription et le soutien de la réassurance jouant un rôle central dans les conditions du marché.

Le marché de la cyberassurance comprend les assureurs traditionnels, les agents généraux délégués, les fournisseurs spécialisés en cybersécurité, les réassureurs et les courtiers, qui collectivement offrent des capacités et apportent une expertise dans un univers des risques qui évolue à un rythme effréné.

Les polices de cyberassurance demeurent largement accessibles à de nombreuses organisations, notamment celles qui ont adopté des pratiques rigoureuses en matière de cybersécurité. Les courtiers font état de la stabilité des prix des polices et de la tolérance constante des assureurs à l'égard des risques bien gérés, même si plusieurs misent davantage sur la stabilité du portefeuille et sur la rigueur en matière de souscription¹⁹.

De ce fait, la cyberassurance se démarque de plus en plus par la qualité du risque plutôt que par les grands cycles du marché. Les assureurs accordent une importance considérable à des facteurs comme l'authentification multifacteur, la détection des terminaux, les procédures de

sauvegarde, la planification de l'intervention en cas d'incident, les pratiques de gouvernance et la gestion des risques liés aux tiers.

La réassurance demeure une composante centrale du marché. Les rapports de l'industrie révèlent que les réassureurs en cyberassurance continuent de fournir une capacité de souscription tout en maintenant le risque d'accumulation, la concentration technologique et les cyberévénements systémiques au centre de leurs priorités. Par exemple, Gallagher Re a fait état d'une capacité de souscription excédentaire lors des renouvellements de janvier 2026, ce qui a contribué à une amélioration de la tarification et des conditions structurelles pour de nombreux acheteurs²⁰.

Prises conjointement, ces dynamiques donnent à penser que le marché canadien de la cyberassurance est concurrentiel, mais pas aveuglé. La capacité de souscription est globalement disponible; toutefois, la rigueur en matière de souscription, les contrôles en matière de cybersécurité et la gestion des risques continuent de jouer un rôle central dans l'évaluation des risques et la tarification^{21,22}.

¹⁹ Willis Towers Watson, 2026. ["Insurance Marketplace Realities 2026 Spring Update: Cyber Risk."](#)

²⁰ Gallagher Re, 2026. [Gallagher Re Cyber Risk Adjusted Rating \(RAR\) Index: 2026 update.](#)

²¹ *Ibid.*

²² Guy Carpenter, 2026. ["Cyber 2025—A Year in Review."](#)

Sinistres et assurabilité

Les cybersinistres sont influencés par la fréquence des incidents et les coûts associés à la survenue simultanée de plusieurs facteurs de pertes.

Les statistiques des sinistres offrent le portrait le plus clair de ce qui compte le plus sur le marché actuel. L'enjeu principal est de savoir à quelle vitesse les sinistres peuvent s'aggraver lorsque plusieurs facteurs de coûts interviennent au cours d'un même événement.

Les données actuelles font entrevoir un environnement marqué par l'augmentation de la fréquence des événements, une évolution de la composition des sinistres et une exposition constante à des événements de faible fréquence, mais de forte gravité.

Les données publiques confirment cette tendance. IBM révèle que le coût moyen d'une fuite de données au Canada a atteint 7,11 millions de dollars en 2026²³. Marsh laisse entendre que les atteintes à la protection des renseignements personnels restent la cybermenace la plus fréquente, tandis que les rançongiciels continuent de générer les sinistres les plus importants et les plus complexes²⁴.

À l'heure actuelle, les statistiques des sinistres illustrent deux pressions qui interagissent :

1. Les sinistres les plus fréquents, dont la fraude, les atteintes à la protection des renseignements personnels et les perturbations opérationnelles, qui génèrent un volume constant de demandes de règlement.
2. Les événements peu fréquents, mais très graves, notamment ceux impliquant des rançongiciels ou une interruption prolongée des activités, qui peuvent avoir des conséquences financières démesurées.

Ensemble, ces deux dynamiques créent un environnement de gestion des sinistres qui risque de compromettre la rentabilité, même dans des conditions de marché stables.

Le piratage psychologique est au cœur de cet environnement. Les incidents liés à la fraude comptent pour une part importante du volume des sinistres et demeurent l'un des facteurs les plus persistants des sinistres assurés. Ces événements exploitent les vulnérabilités humaines et dans les processus plutôt que les défaillances techniques des systèmes²⁵.

²³ IBM, 2025.

²⁴ Marsh, 2026. [US & Canada Cyber Claims 2025: Data Privacy Remains a Challenge While Ransomware Lingers.](#)

²⁵ Coalition, 7 mai 2025. ["Coalition 2025 Cyber Claims Report Finds Ransomware Stabilized but Remains Costly for Businesses."](#)

Les rançongiciels demeurent le principal risque de gravité. Malgré la fluctuation de la fréquence des attaques par rançongiciel au fil des ans, le risque de sinistres importants demeure. Les agents malveillants ont de plus en plus recours à l'exfiltration et à l'extorsion de données, ce qui amplifie les conséquences financières, réglementaires et réputationnelles. Le Centre canadien pour la cybersécurité considère les rançongiciels comme une menace persistante et évolutive dans tous les secteurs²⁶.

Ces dynamiques de sinistres influent directement sur l'assurabilité. La souscription tient de plus en plus compte de la présence de contrôles de base en matière de cybersécurité et de leur efficacité. L'authentification multifacteur, la détection des terminaux, les sauvegardes sécurisées, la correction de programme et la planification des interventions en cas d'incident sont au nombre des mesures auxquelles s'attendent généralement les assureurs. Par conséquent, l'assurabilité est de plus en plus liée aux contrôles en matière de cybersécurité, aux pratiques de gouvernance et aux capacités d'intervention en cas d'incident plutôt qu'à l'exposition seule.

Les statistiques des sinistres demeurent un facteur important qui influe sur la tarification, la sélection des risques et les conditions du marché. Ils influencent activement la tarification, la sélection des risques et la structure même du marché de la cyberassurance.

Étude de cas : Indigo victime d'un rançongiciel

Une seule atteinte à la cybersécurité peut engendrer des pertes financières et opérationnelles qui se chevauchent au sein de plusieurs secteurs d'une organisation.

En février 2023, Indigo Books & Music est victime d'une attaque par rançongiciel qui perturbe ses activités numériques et de vente au détail. Les systèmes de transactions aux points de vente, les activités internes et le commerce électronique sont visés; l'entreprise voit sa capacité à mener ses activités commerciales habituelles restreinte. Selon les renseignements diffusés publiquement, les magasins sont momentanément dans l'incapacité de traiter les paiements par carte et les ventes en ligne sont indisponibles pendant une période prolongée^{27,28}.

Dans la foulée de l'incident, les données des employés sont également compromises. Les renseignements personnels d'employés actuels et anciens ont été consultés. Heureusement, les données de paiement des clients ne sont pas compromises²⁹.

Indigo déclare que la cyberattaque lui a fait perdre quelque 50 millions de dollars, soit les coûts liés à l'intervention directe et à la perturbation de ses activités^{30,31}.

Cette étude de cas est importante non seulement par son ampleur, mais aussi parce qu'elle illustre bien les cybersinistres d'aujourd'hui. Les atteintes à la cybersécurité

26 Centre canadien pour la cybersécurité, 2026. [Vue d'ensemble des menaces par rançongiciel de 2025 à 2027](#).

27 CBC News, 2023. ["Indigo lost \\$50M last year, in large part due to February cyberattack."](#)

28 Indigo Books & Music, 2023.

29 CBC News, 2023. ["Indigo won't pay ransom for stolen employee data."](#)

30 *Ibid.*

31 Indigo Books & Music, 2023.

peuvent perturber simultanément les systèmes numériques et les activités physiques, notamment lorsque les paiements, les activités de vente au détail et la logistique sont tous tributaires de plateformes technologiques intégrées. Les mesures prises pour contenir l'incident, notamment la mise hors ligne des systèmes, permettent certes d'atténuer les dommages supplémentaires, mais peuvent également prolonger l'interruption des activités.

Un seul événement peut entraîner de multiples sinistres, notamment une perte d'exploitation, une fuite de données, des coûts liés à l'intervention en cas d'incident et une atteinte à la réputation. En cyberassurance, l'interaction de ces facteurs est un élément déterminant de la gravité des risques.

Dépendance numérique et cyberrisques systémiques

Lorsque les dépendances numériques sont partagées, le cyberrisque n'est pas toujours indépendant d'une organisation à l'autre. La perturbation d'une technologie utilisée par beaucoup peut nuire à plusieurs entreprises en même temps.

Il n'est donc plus possible d'appréhender le cyberrisque sous le seul angle des organisations individuelles. De nombreuses entreprises qui semblent indépendantes du point de vue de l'assurance (en raison de leur emplacement géographique, de leur secteur d'activité ou de leur taille) sont tributaires des mêmes fournisseurs infonuagiques, plateformes

logicielles, fournisseurs de services gérés et infrastructures numériques. Par conséquent, la perturbation d'une technologie largement utilisée peut nuire à de nombreuses organisations en même temps.

Dans le domaine de la cyberassurance, des organisations de secteurs d'activité, emplacements géographiques ou taille divers peuvent avoir des dépendances technologiques communes. Des sinistres peuvent donc émerger d'une source commune.

La numérisation croissante de l'économie est venue amplifier ces interconnexions. L'informatique en nuage, les plateformes de logiciels-services, les fournisseurs de services gérés, les systèmes de paiement et les logiciels d'entreprise font désormais partie intégrante des activités commerciales. Si ces technologies offrent des avantages considérables en matière d'efficacité et de sécurité, elles peuvent également concentrer les risques lorsque de nombreuses organisations y ont recours.

La numérisation et la connectivité croissantes des foyers, des véhicules, des équipements et des entreprises créent des voies supplémentaires par lesquelles un incident cybernétique peut entraîner des dommages matériels, des vols, des dommages corporels, une perte d'exploitation, une atteinte à la protection des renseignements personnels ou la responsabilité civile. Il peut s'ensuivre des interactions complexes entre la cyberassurance spécialisée et les polices d'assurance traditionnelles (biens, dommages, vols et détournements, automobile et responsabilité civile). La garantie dépendra du libellé de la police applicable, notamment de la nature et de l'étendue de l'assurance, des définitions, des exclusions, des avenants et des dispositions relatives à la causalité.

Des incidents survenus récemment illustrent bien les répercussions importantes que ces dépendances peuvent avoir.

CrowdStrike (2024)

Une mise à jour logicielle défectueuse, publiée par le fournisseur de cybersécurité CrowdStrike, a entraîné des perturbations informatiques généralisées à l'échelle mondiale, touchant des compagnies aériennes, des institutions financières, des établissements de santé, des détaillants et des organismes gouvernementaux. S'il n'a pas été causé par une cyberattaque malveillante, l'incident a tout de même démontré comment des milliers d'organisations peuvent être simultanément touchées par la perturbation d'une technologie utilisée par beaucoup.

MOVEit (2023)

L'exploitation d'une vulnérabilité dans le logiciel de transfert de fichiers MOVEit a ciblé des milliers d'organisations dans le monde entier par l'intermédiaire d'une plateforme technologique couramment utilisée. Cet incident démontre qu'une simple vulnérabilité logicielle peut exposer des organisations qui, autrement, n'ont aucun lien entre elles.

SolarWinds (2020)

La faille de sécurité chez SolarWinds illustre comment une attaque de la chaîne d'approvisionnement peut se propager par l'intermédiaire de fournisseurs de logiciels de confiance, touchant un grand nombre d'organisations des secteurs public et privé ayant une dépendance communée.

Ces incidents n'ont pas commencé au sein des organisations touchées. Ils se sont plutôt propagés par l'intermédiaire de technologies, de fournisseurs de services ou d'une infrastructure numérique partagés reliant de nombreuses organisations.

Les conséquences pour les assureurs sont importantes. L'assurance traditionnelle repose,

en partie, sur la diversification. Bien souvent, les sinistres subis par un assuré sont, pour l'ensemble, indépendants de ceux subis par un autre. Les dépendances numériques partagées viennent ébranler cette idée. Lorsque plusieurs organisations assurées dépendent de la même plateforme technologique, du même fournisseur de services ou du même logiciel, une seule perturbation peut entraîner des sinistres simultanés pour de nombreux assurés.

La concentration des fournisseurs est un élément central de ce risque. De nombreuses organisations dépendent d'un nombre relativement restreint de fournisseurs pour l'informatique en nuage, le stockage de données, les services de cybersécurité, les logiciels d'entreprise et le traitement des paiements. Bien souvent, ces fournisseurs consacrent d'importantes sommes à la cybersécurité et à la résilience opérationnelle, mais l'adoption généralisée peut venir accentuer l'ampleur potentielle des perturbations en cas d'incident.

Les dépendances à des tiers viennent complexifier le portrait. Les organisations modernes sont actives dans de vastes écosystèmes numériques qui comprennent des fournisseurs, des sous-traitants, des fournisseurs de services gérés et des partenaires technologiques externes. Par conséquent, les cyberincidents peuvent avoir un effet domino dans les réseaux d'entreprises, engendrant des conséquences opérationnelles et financières qui transcendent la première organisation touchée.

Ces préoccupations sont palpables sur les marchés de la réassurance. Selon les rapports industriels, lors de l'évaluation des portefeuilles de cybersécurité, les réassureurs continuent d'accorder la priorité au risque d'accumulation, à la concentration technologique et aux dépendances numériques partagées. Si les capacités de souscription demeurent largement disponibles, le risque de pertes corrélées reste un élément central de la cyberassurance à ne pas ignorer au moment de constituer les portefeuilles et de gérer les risques.

L'écart de protection : les PME et le marché de la cyberassurance

L'écart de cyberprotection des PME crée des vulnérabilités qui peuvent se propager par les chaînes d'approvisionnement et les réseaux d'entreprises.

L'écart de cyberprotection des PME demeure l'un des enjeux structurels les plus manifestes du marché canadien. Un sondage mené par le BAC révèle que, en 2025, seuls 22 % des PME disposaient d'une cyberassurance et à peine 12 %, d'une couverture autonome. Parallèlement, moins de la moitié des PME ont déclaré avoir mis en place des mesures de cybersécurité de base³².

Il ne s'agit pas que d'un problème de garantie. Cet écart influe sur la façon dont l'économie dans son ensemble absorbe les cybersinistres. En tant qu'employeurs, fournisseurs de services et acteurs des chaînes d'approvisionnement essentielles, les PME jouent un rôle de premier plan au sein de l'économie canadienne. Faute d'assurance ou de préparation, les incidents cybernétiques sont moins susceptibles d'être absorbés par des mécanismes structurés tels que l'assurance.

Ce sont plutôt les entreprises, les clients et les partenaires commerciaux qui risquent d'assumer les pertes. Ces effets sont souvent moins visibles et moins prévisibles, notamment lorsqu'ils se propagent à travers les chaînes d'approvisionnement ou les relations commerciales.

L'écart de protection reflète une combinaison de facteurs liés à l'offre et à la demande. Du côté de la demande, les PME sont souvent confrontées à des contraintes liées à la sensibilisation, à l'accessibilité financière et à des priorités commerciales concurrentes. Du côté de l'offre, les exigences de souscription liées à des contrôles de base en matière de cybersécurité peuvent créer des barrières à l'entrée pour les entreprises disposant de ressources limitées.

Ces facteurs peuvent se renforcer mutuellement. Les entreprises qui n'ont pas les moyens d'instaurer des contrôles de base peinent parfois à obtenir une garantie, ce qui, à son tour, peut freiner les améliorations apportées aux pratiques et à la préparation en matière de cybersécurité. Il s'ensuit un cercle vicieux dans lequel une préparation moindre entraîne une couverture moindre et une plus grande vulnérabilité.

La cyberassurance joue un rôle dans la réduction de cet écart. Les exigences en matière de souscription peuvent contribuer à améliorer les contrôles de base, tandis que les courtiers et les conseillers en gestion des risques peuvent aider à traduire le cyberrisque en décisions commerciales concrètes.

Les conséquences transcendent les entreprises individuelles. Les PME sont souvent intégrées aux chaînes d'approvisionnement et aux économies locales. Compte tenu du

³² BAC, 2025.

rôle que jouent les PME dans les chaînes d'approvisionnement et dans la prestation de services, les cyberincidents peuvent avoir des répercussions qui dépassent de loin l'organisation où l'incident a commencé.

Les cyberincidents ciblant des PME sous-assurées peuvent avoir des conséquences financières et opérationnelles pour les fournisseurs, les clients et les partenaires commerciaux. Pour combler l'écart de cyberprotection des PME, il ne suffit donc pas d'augmenter le recours à l'assurance. Il faut également améliorer la préparation aux cyberattaques et la capacité des entreprises à absorber les pertes liées aux cyberattaques et à s'en remettre.

Politique et réglementation

Les politiques de cybersécurité et les cyberassurances fonctionnent de plus en plus dans le même environnement de risque. L'évolution de la réglementation, des déclarations, de la gouvernance et de la coopération internationale peut influencer la manière dont les cyberrisques sont appréhendés, gérés et assurés.

Face à l'importance économique croissante des cyberincidents, les gouvernements accordent une attention accrue à la cybersécurité, à la protection des infrastructures essentielles, à la déclaration des incidents et à la gouvernance numérique. Si la plupart de ces initiatives ne sont pas

destinées à l'industrie de l'assurance, elles peuvent influencer les conditions dans lesquelles les cyberrisques sont mesurés, gérés et transférés.

Les avancées suivantes sont particulièrement pertinentes pour le marché de la cyberassurance:

Renforcement des infrastructures essentielles pour la cybersécurité

Le Canada continue d'accorder une place importante à la protection des infrastructures essentielles contre les cybermenaces. La Loi sur la protection des cybersystèmes essentiels, qui a force de loi depuis juin 2026, mais qui est en attente d'une réglementation pour entrer pleinement en vigueur, renforcera les exigences en matière de cybersécurité pour les opérateurs désignés dans les secteurs réglementés par le gouvernement fédéral et améliorera les pratiques de déclaration des incidents, de gouvernance et de gestion des risques.

C'est pertinent dans le contexte de la cyberassurance, car les organisations qui soutiennent les infrastructures essentielles représentent souvent les expositions aux cyberrisques les plus complexes et potentiellement les plus graves de l'économie. Les perturbations dans les secteurs des télécommunications, de l'énergie, des transports ou des services financiers peuvent avoir des conséquences qui dépassent le cadre des organisations individuelles et nuisent à l'activité économique dans son ensemble.

Du point de vue des assurances, les exigences réglementaires relatives à la gouvernance cybernétique, à la gestion des incidents et aux contrôles en matière de cybersécurité peuvent également influencer les attentes en matière de souscription. À l'heure où les assureurs accordent une importance de plus en plus grande à l'efficacité des contrôles et à la préparation organisationnelle, les normes réglementaires peuvent accroître l'uniformité dans la gestion et l'évaluation des cyberrisques.

Déclaration d'incidents et données sur les cyberrisques

Dans le domaine de la cyberassurance, la disponibilité de données fiables sur les incidents et les pertes est un défi de longue date. Comparativement à de nombreuses branches d'assurance traditionnelles, les statistiques des sinistres sont plutôt récentes dans le domaine de la cyberassurance et les renseignements sur les sinistres y sont moins uniformisés.

Au Canada et à l'étranger, les nouvelles politiques mettent davantage l'accent sur l'obligation de déclarer les incidents, sur les exigences de divulgation et sur la mise en commun des renseignements. Ces efforts témoignent d'une reconnaissance croissante de l'importance d'améliorer les données pour mieux comprendre les cyberrisques.

Une déclaration améliorée des incidents offre aux assureurs des renseignements plus précis sur les tendances en matière de sinistres, les activités des menaces et les nouveaux risques. Des données améliorées peuvent faciliter la souscription, la tarification, l'évaluation de

l'accumulation et la modélisation des risques au fil du temps.

C'est particulièrement pertinent sur un marché où les préoccupations transcendent de plus en plus les organisations individuelles pour englober des sources de risques corrélés telles que les technologies partagées et les fournisseurs de services communs.

Coopération internationale et menace posée par les rançongiciels

Par sa nature même, le risque cybernétique dépasse les frontières. Les agents malveillants travaillent à l'échelle internationale, les campagnes de rançongiciels ciblent des organisations dans plusieurs territoires et de nombreux services numériques reposent sur une infrastructure interconnectée à l'échelle mondiale.

Le Canada participe à plusieurs initiatives internationales en matière de cybersécurité, notamment l'Initiative de lutte contre les rançongiciels internationale, qui vise à renforcer la collaboration entre les gouvernements par la mise en commun de renseignements, la perturbation des activités cybercriminelles et les efforts déployés pour réduire les flux financiers liés aux rançongiciels.

Le Canada est récemment devenu signataire de la Convention des Nations Unies contre la cybercriminalité, qui prévoit des mesures pour prévenir la cybercriminalité grâce à une sensibilisation accrue du public, une collaboration renforcée entre les secteurs public et privé et un soutien ciblé aux petites entreprises, reconnaissant leur importance

pour la résilience économique et les communautés locales.

Cet accord s'inscrit dans la tendance plus vaste d'une participation croissante du Canada aux cadres et accords internationaux en matière de cybersécurité, tels que le Groupe des cinq, qui visent à renforcer la cyberdéfense et la coopération.

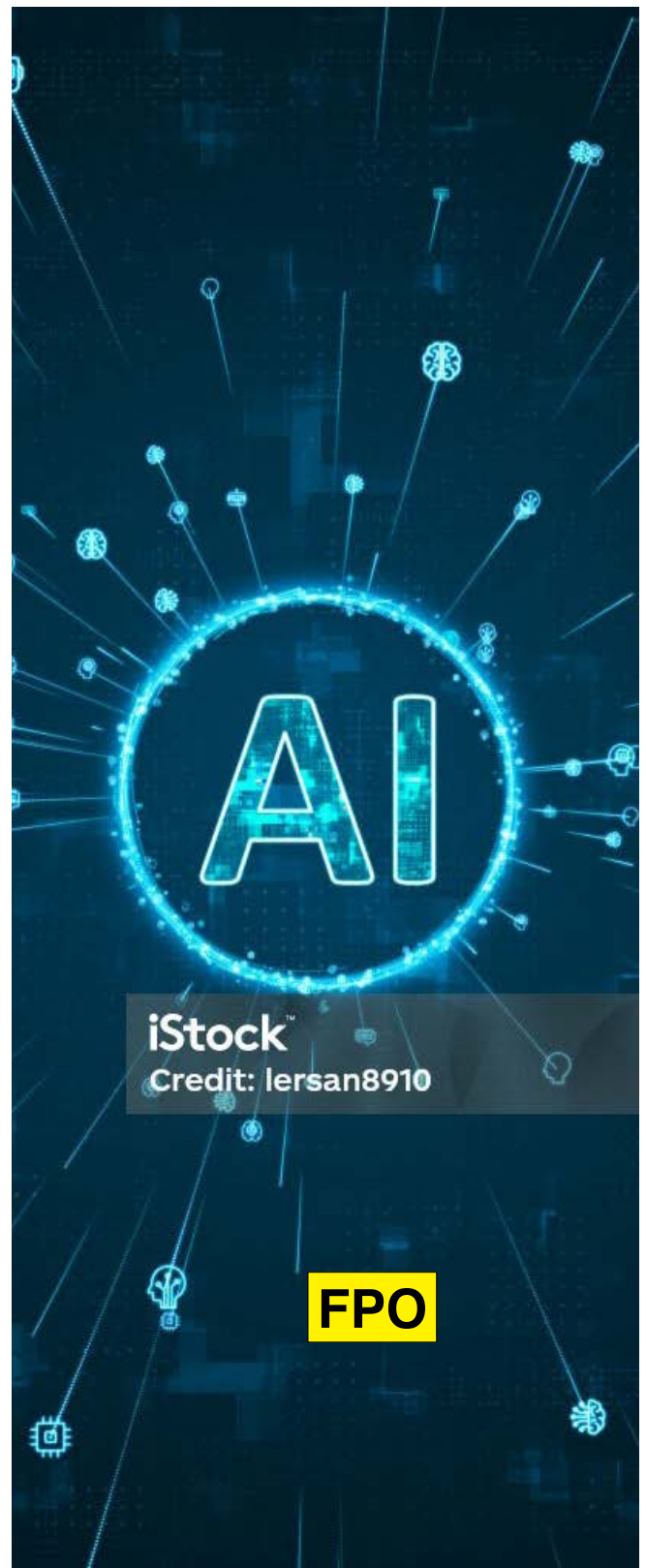
Intelligence artificielle et risques émergents

L'intelligence artificielle (IA) est une composante de plus en plus importante de la cybersécurité.

Des outils basés sur l'IA sont utilisés pour améliorer la détection des menaces, la surveillance et l'intervention en cas d'incident. Parallèlement, ces outils peuvent servir à perfectionner les techniques de piratage psychologique, d'hameçonnage, d'usurpation d'identité et de détection des vulnérabilités informatiques et à en accroître la portée.

L'incertitude persiste quant aux effets à long terme de l'IA. Toutefois, c'est un sujet qui prend de plus en plus de place dans les discussions plus générales sur les politiques de cybersécurité, la gouvernance numérique et la gestion des risques organisationnels.

Les assureurs doivent surtout comprendre l'influence que les technologies émergentes peuvent avoir sur les cyberincidents. L'IA peut certes renforcer les capacités de cyberdéfense, mais elle peut aussi modifier l'univers des menaces de façons que nous ne comprenons pas encore pleinement.



Pourquoi c'est important pour le marché de la cyberassurance

La politique publique et les cyberassurances fonctionnent de plus en plus dans le même environnement de risque.

Les avancées politiques gouvernementales les plus importantes sont celles qui améliorent la visibilité des cyberincidents, renforcent les pratiques de cybersécurité, contribuent à la mise en commun des renseignements et permettent de mieux comprendre les risques émergents. Ces facteurs orientent les décisions de souscription, influencent les attentes en matière de gestion des risques et permettent une évaluation plus éclairée des cyberrisques dans l'ensemble de l'économie.

Si les mesures politiques gouvernementales et les mécanismes d'assurance jouent des fonctions différentes, ils répondent tous deux aux défis communs associés aux cyberrisques.

Conséquences principales

Pour les gouvernements : La dépendance numérique, l'écart persistant dans la couverture des PME et l'importance croissante du cyber risque systémique sont autant de caractéristiques notables de l'univers des cyberrisques canadien.

Pour l'industrie de l'assurance de dommages : Malgré la stabilité des marchés, la gravité des sinistres et le risque d'accumulation demeurent des aspects essentiels. La rigueur en matière de souscription, la gravité des sinistres et la gestion des risques continuent d'influer sur la performance. Les dépendances numériques partagées sont un facteur important, et les assureurs se doivent d'en tenir compte.

Pour les entreprises : Les pratiques en matière de cyberassurance et de cybersécurité sont de plus en plus interreliées. La cyberassurance est de plus en plus liée aux pratiques de cybersécurité, à la préparation opérationnelle et à la gestion des risques liés aux tiers. Dans un contexte où les organisations dépendent de plus en plus des systèmes numériques, le risque cybernétique dépasse les limites des fonctions informatiques traditionnelles.

Conclusion

Le marché canadien de la cyberassurance s'est certes développé, mais l'environnement des risques s'est complexifié.

Après les importantes pertes subies entre 2019 et 2021, le marché s'est, dans une grande mesure, stabilisé. Le cyberrisque est de plus en plus influencé par les interdépendances numériques partagées et par la concentration des services technologiques essentiels.

De ce fait, on ne cherche plus à savoir si la cyberassurance peut fournir la capacité de souscription et la couverture nécessaires. La question centrale est de savoir comment les assureurs, les entreprises et les stratégies comprennent et gèrent les risques qui peuvent être graves, interdépendants et difficiles à diversifier.



Sources

- **Centre canadien pour la cybersécurité.** *Vue d'ensemble des menaces par rançongiciel de 2025 à 2027.* Gouvernement du Canada, 2026.
- **CBC News.** *Indigo lost \$50M last year, in large part due to February cyberattack*, 28 juin 2023.
- **CBC News.** *Indigo won't pay ransom for stolen employee data*, 1^{er} mars 2023.
- **Coalition.** *Cyber Claims Report*. 2025.
- **Gallagher Re.** *Cyber Market Outlook*. 2026.
- **Gallagher Re.** *Cyber Risk Adjusted Rating (RAR) Index: 2026 Update*. Janvier 2026.
- **Guy Carpenter.** *Cyber 2025—A Year in Review*. 2026.
- **IBM.** *Rapport 2026 sur le coût d'une violation de données : Canada*. 2025.
- **Indigo Books & Music Inc.** Information financière publiée et divulgations liées à l'attaque par rançongiciel de février 2023.
- **Bureau d'assurance du Canada.** *Sondage sur la cybersécurité*. 2025.
- **Bureau d'assurance du Canada.** *Le marché canadien de la cyberassurance*. Octobre 2025.
- **McCarthy Tétrault.** *Tendances en matière de cyberassurance : Perspectives 2026 sur les incidents de confidentialité*. 2026.
- **Marsh.** *Réclamations liées aux cyberrisques en 2025*. 2026.
- **MSA Research Inc.** Données sur l'industrie de la cyberassurance analysées par le Bureau d'assurance du Canada, 2026.
- **Statistique Canada.** *Cyber security and cybercrime survey data*, 2023.
- **Willis Towers Watson.** *Cyber Risk: A Look Ahead to 2026*. 2026.
- **Willis Towers Watson.** *Insurance Marketplace Realities 2026 Spring Update – Cyber Risk*. Mai 2026.
- **Willis Towers Watson.** *Insurance Marketplace Realities 2026 – Cyber Risk*. Octobre 2025.

Remarque : Sauf indication contraire, les statistiques du marché canadien de la cyberassurance se basent sur une analyse du Bureau d'assurance du Canada reposant sur les données de MSA Research pour les assureurs de dommages privés exerçant leurs activités au Canada.



bac.ca

