BAC
Bureau d'assurance du Canada

Le marché canadien de la cyberassurance

Octobre 2025

Résumé

En 2025, le marché canadien de la cyberassurance est entré dans une phase de stabilisation prudente. Après plusieurs années marquées par l'instabilité, les assureurs constatent une amélioration des résultats en matière de souscription, tandis que la concurrence revient progressivement, soutenue par une capacité accrue (voir la figure 1). Parallèlement, les cybermenaces continuent d'évoluer. Les pirates informatiques tirent désormais parti de l'intelligence artificielle (IA) pour mener des attaques plus convaincantes, plus efficaces et à plus grande échelle, ce qui souligne la nécessité d'une vigilance constante. Bien que la législation fédérale attendue en matière de cybersécurité ne soit toujours pas adoptée, le secteur de la cyberassurance et les gouvernements poursuivent leurs efforts concertés pour renforcer la résilience numérique du Canada. Les petites et moyennes entreprises (PME) demeurent largement sous-assurées, ce qui met en lumière la nécessité d'une sensibilisation accrue et de solutions de couverture plus accessibles. Le présent rapport examine les principaux développements et les principales tendances de 2025 et met l'accent sur les dynamiques du marché, l'évolution du paysage des risques, les avancées réglementaires et la résilience numérique des PME.

Ce rapport est destiné aux représentants gouvernementaux, **aux organismes de réglementation, aux assureurs ainsi qu'aux chefs d'entreprise** qui souhaitent contribuer au renforcement de la cybersécurité au Canada. Il insiste sur l'urgence d'une action coordonnée entre les secteurs public et privé afin de protéger les consommateurs, de soutenir les entreprises vulnérables et d'assurer la pérennité du marché de la cyberassurance. Il propose également des recommandations importantes qui prémuniront la population du Canada contre les menaces grandissantes en ligne.

Le rapport couvre les thèmes suivants :

- **Les tendances du marché de la cyberassurance et les perspectives du secteur**
- **Un paysage des cyberrisques en pleine mutation au Canada**
- **Les développements législatifs et le cadre réglementaire**
- **Le fossé en matière de cyberassurance pour les PME : enjeux et occasions**

Principaux constats et recommandations

Les tendances du marché de la cyberassurance et les perspectives du secteur

Croissance rapide du marché : Les primes émises de cyberassurance sont passées de 18 millions de dollars canadiens en 2015 à environ 650 millions en 2024, portées par une demande croissante dans tous les secteurs.

Pertes de souscription et marché dur : L'épidémie de rançongiciels (2019–2021) a entraîné de lourdes pertes, avec des rapports sinistres-primes combinés moyens de 155 %, ce qui a eu des répercussions sur le prix et la couverture des garanties offertes.

Stabilisation du marché : En 2025, le resserrement des critères de souscription et l'application d'une plus grande rigueur dans la sélection des risques ont permis un retour à la rentabilité, avec des ratios ramenés à 49 %. Cela a contribué à stabiliser les tarifs pour les risques bien gérés.

Renforcement des pratiques de souscription : De nombreux assureurs exigent des contrôles de base en cybersécurité (par exemple, authentification multifacteur, sauvegardes, formation), ce qui améliore la qualité des portefeuilles.

Augmentation des capacités et maturité du marché : Le retour des réassureurs permet d'offrir une couverture plus étendue et des limites plus élevées. L'arrivée de nouveaux acteurs et d'agents généraux principaux diversifie l'offre, signe d'un marché plus prévisible et durable.

Concurrence plus saine : Les entreprises dotées d'une bonne hygiène numérique peuvent obtenir de meilleures conditions et des rabais, ce qui renforce le lien vertueux entre gestion des risques et tarification.

Incertitude persistante : Malgré ces progrès, le risque d'événements systémiques reste présent. La pression concurrentielle pourrait inciter à des pratiques de souscription imprudentes si elle n'est pas bien encadrée.

Nouveaux produits et innovations : La cyberassurance personnelle se développe et offre une protection contre le vol d'identité, les rançongiciels et les atteintes à la réputation. Les contrats d'assurance titrisés (CAT) permettent d'élargir l'accès aux capitaux et d'accroître la résilience face aux événements catastrophiques.

L'évolution du paysage des cyberrisques au Canada

Menaces facilitées par l'IA

- L'intelligence artificielle générative permet de concevoir des courriels d'hameçonnage convaincants et des hypertrucages, et ainsi des attaques par piratage psychologique plus difficiles à détecter.
- Les logiciels malveillants améliorés par l'IA font leur apparition; ils sont en mesure d'adapter leur comportement en fonction des dispositifs de défense de la victime.
- Les rançongiciels sont de plus en plus automatisés et pourraient bientôt exploiter l'IA pour cibler les données de façon plus stratégique.
- Les outils d'IA en tant que service réduisent les obstacles, ce qui permet à des pirates informatiques peu expérimentés de lancer des attaques sophistiquées.

Risque croissant lié aux rançongiciels

- Les rançongiciels demeurent la principale cause des réclamations majeures en matière de cyberassurance au Canada; leur fréquence, leur complexité ainsi que le coût qui y est associé ne cessent de prendre de l'ampleur.
- En 2023, les incidents dans le monde ont augmenté de 74 % et les paiements de rançons ont dépassé 1 milliard de dollars américains. Au Canada, les incidents se sont accrus de 26 % par année depuis 2021 et le paiement moyen de rançon s'élève à 1,13 million de dollars canadiens.
- Les modèles, de plus en plus professionnels, de rançongiciel en tant que service adoptent désormais des tactiques d'extorsion double et triple.
- Les entreprises de taille moyenne, les municipalités, les hôpitaux et les PME sont de plus en plus ciblés en raison de leurs systèmes de défense plus faibles.

Autres menaces persistantes

- Les fraudes du président, les cyberattaques sur les chaînes d'approvisionnement et les intrusions dans les infrastructures essentielles continuent d'augmenter, souvent amplifiées par les outils d'IA.
- Les pirates informatiques utilisent des canaux chiffrés et des horaires décalés; le temps de présence des cybercriminels a chuté à 10 jours dans le monde en 2023, ce qui est encore suffisant pour causer des dégâts considérables.

Conséquences pour les assureurs

- La fréquence et l'importance des réclamations s'intensifient.
- L'évolution rapide des cybermenaces met à l'épreuve les clauses des polices et pousse les assureurs à proposer des couvertures plus adaptées ainsi que des services proactifs.

Les développements législatifs et le cadre réglementaire

- **Les progrès réglementaires sont inégaux**
  Le projet de loi C-26, qui visait à moderniser le cadre canadien de cybersécurité pour les infrastructures essentielles, a franchi plusieurs étapes législatives en 2024, mais n'a pas été adopté après la prorogation du gouvernement fédéral, en janvier 2025. Son successeur, le projet de loi C-8, a été déposé plus tard en 2025, mais demeure à l'étude.

- **La réforme de la protection de la vie privée est aussi au point mort**
  Le projet de loi C-27, qui devait moderniser la législation relative à la protection de la vie privée et établir un cadre pour l'IA, est mort au feuilleton, ce qui a laissé le cadre canadien de protection des données désuet et fragmenté.

- **Le Canada ne dispose toujours pas d'un cadre national sur la cybersécurité des infrastructures essentielles**
  Cette lacune législative prive des secteurs vitaux (comme l'énergie, les télécommunications et les services financiers) de normes uniformes et exécutoires, ce qui accroît le risque systémique.

- **La stratégie intérimaire du Canada mise sur la collaboration**
  La nouvelle stratégie nationale de cybersécurité du gouvernement fédéral met l'accent sur les partenariats, et le Collectif canadien pour la cyberdéfense (CCCD) joue notamment un rôle clé pour coordonner la collaboration intersectorielle et la communication des renseignements.

Recommandations pour les décideurs afin de réduire le risque de cybermenaces au Canada

- **Produire un cadre national sur la cybersécurité des infrastructures essentielles**
  Mettre en place un cadre national de cyberrésilience pour les infrastructures essentielles qui exige des exploitants d'infrastructures essentielles nationales (selon la définition donnée par le gouvernement fédéral) qu'ils respectent des normes minimales en matière de cybersécurité, avec des directives de mise en œuvre adaptées à chaque secteur.

- **Soutenir la collaboration intersectorielle**
  Soutenir l'élargissement d'initiatives comme le CCCD afin d'améliorer la diffusion d'information, la réponse aux incidents et la compréhension des risques systémiques.

- **Harmoniser les règlements avec les normes internationales**
  Harmoniser les règlements canadiens avec les cadres mondiaux en matière de cybersécurité afin de renforcer la résilience du pays et d'attirer une plus grande capacité d'assurance internationale.

- **Envisager un moyen de garantie contre les catastrophes de cybersécurité**
  Envisager la mise en place d'un dispositif d'assurance soutenu par l'État, semblable aux fonds de mutualisation des risques liés au terrorisme, afin de prévenir les incidents de cybersécurité de grande ampleur.

Le fossé en matière de cyberassurance pour les PME

- **Les PME sont très vulnérables et demeurent sous-assurées**
  Bien qu'elles soient confrontées à des cybermenaces croissantes, seules 12 % des petites entreprises canadiennes disposent d'une cyberassurance autonome.
- **La sensibilisation demeure faible et les idées fausses persistent**
  De nombreux propriétaires de PME sous-estiment leur exposition aux cyberrisques ou croient à tort que leur assurance commerciale de dommages ou leurs fournisseurs de services de TI leur offrent une protection suffisante.
- **Les produits offerts ont longtemps été mal adaptés aux besoins des PME**
  Les polices de cybersécurité traditionnelles ne répondaient pas aux réalités des PME, avec des protections et des plafonds conçus pour les grandes entreprises.
- **La préparation en cybersécurité est inégale parmi les PME**
  Beaucoup de PME n'ont pas de personnel TI dédié ni de protections de base, ce qui complique le travail de souscription et l'évaluation des risques.
- **Les conditions du marché s'améliorent progressivement**
  Avec la stabilisation des prix en 2024 et 2025, les assureurs commencent à offrir des produits plus adaptés, abordables et modulaires pour les PME.

Recommandations pour un environnement plus serein en matière de cyberrisques pour les PME

- **Élargir les activités de sensibilisation et de formation**
  Les gouvernements devraient collaborer avec les assureurs, les courtiers et les associations professionnelles afin d'aider les PME à comprendre que la cybersécurité constitue un enjeu central pour leurs affaires et à clarifier ce que couvre une cyberassurance.
- **Créer un programme incitatif à l'état de préparation en matière de cybersécurité**
  Le gouvernement fédéral devrait mettre en place des aides financières ciblées (par exemple, des crédits d'impôt, des subventions ou des mesures de partage des coûts) afin d'aider les PME à miser sur des outils essentiels en cybersécurité, de la formation et des pratiques de gestion des risques.

Les tendances du marché de la cyberassurance et les perspectives du secteur

Les tendances du marché et les perspectives du secteur

Croissance et stabilisation du marché

La cyberassurance s'est solidement imposée comme un élément clé du paysage de l'assurance des entreprises au Canada. Le marché a connu une croissance spectaculaire, alors que les petites et grandes entreprises cherchent à se protéger financièrement contre les incidents de cybersécurité. Les primes émises sont passées d'environ 18 millions de dollars de primes émises en 2015 à environ 650 millions en 2024[1,2]. Cette expansion s'est toutefois accompagnée d'une augmentation tout aussi rapide de la fréquence et de la gravité des sinistres, en particulier lors de l'épidémie de rançongiciels[3,4] de 2019 à 2021. Les assureurs ont subi des pertes sans précédent : entre 2019 et 2023, les rapports sinistres-primes combinés des cyberassureurs canadiens ont atteint en moyenne 155 %, ce qui témoigne d'importantes pertes de souscription[5]. Cette situation a culminé en un marché dur en 2021-2022, marqué par la hausse des primes, le resserrement des limites de couverture et le retrait de certains assureurs de certaines lignes de risque.

Figure 1.

Résultats financiers selon la norme IFRS 4[6]	Primes directes (en millions de dollars)	Coûts des sinistres (en millions de dollars)	Ratio combiné des pertes[7]
2019	119	118	130,9 %
2020	162	600	402,1 %
2021	279	322	146,6 %
2022[8]	472	(135)	3,3 %
Résultats financiers selon la norme IFRS 17	**Produits des activités d'assurance**	**Charges afférentes aux activités d'assurance**	**Ratio des activités d'assurance[9]**
2023	550	458	94 %
2024	650	252	49 %

1. BAC, 2024.
2. Une nouvelle norme internationale d'information financière applicable à la comptabilité des contrats d'assurance, l'IFRS 17, est entrée en vigueur le 1er janvier 2023. Cette nouvelle norme mondiale remplace la norme IFRS 4, instaurée en 2004.
3. Axios, 17 mai 2021. The new digital extortion.
4. Marsh, Ransomware: A persistent challenge in cyber insurance claims.
5. BAC, 2024.
6. Système comptable applicable aux contrats d'assurance avant le 1er janvier 2023.
7. Le rapport sinistre-primes correspond au rapport entre le total des indemnités versées (y compris les frais de règlement) et le total des primes encaissées. Il s'exprime généralement en pourcentage.
8. En 2022, les assureurs en cyberassurance au Canada ont constitué des réserves supérieures aux besoins réels pour couvrir les réclamations, en raison de l'incertitude des conditions macroéconomiques. Cela a entraîné des coûts de réclamations agrégés négatifs, ce qui a faussé le ratio des pertes pour cette catégorie d'assurance.
9. Ce rapport constitue un indicateur clé de la rentabilité des activités d'assurance. Il exprime le rapport entre les coûts de sinistres et les charges directement attribuables aux contrats d'assurance, et les produits des activités d'assurance.

Les tendances du marché et les perspectives du secteur

Amélioration des rapports sinistres-primes

En 2025, des signes clairs montrent que ce cycle tend à se stabiliser. Grâce à des critères de souscription plus stricts, à une meilleure sélection des risques et aux hausses de primes des années précédentes, les rapports sinistres-primes se sont sensiblement améliorés[10]. En 2024, le ratio des activités d'assurance[11] était de 94 %, ce qui signifie que les assureurs ont versé environ 0,94 $ en sinistres et en frais pour chaque dollar de prime souscrite. Ce résultat marque une nette amélioration par rapport aux pertes importantes enregistrées en 2020-2021[12]. En 2025, ce ratio s'est encore amélioré, atteignant 49 %. Bien que les changements comptables consécutifs à la mise en œuvre de la norme IFRS 17 aient une incidence sur la comparabilité d'une année à l'autre [13], le consensus est que la cyberassurance au Canada est redevenue rentable pour les souscripteurs. Cette reprise a renforcé la confiance des assureurs et des réassureurs. Même si la rentabilité reste fragile, elle a permis une stabilisation des conditions du marché. Dans certains cas, les tarifs de renouvellement se sont maintenus ou ont diminué pour les risques bien gérés, ce qui contraste fortement avec les augmentations à deux chiffres observées il y a quelques années.

Perfectionnement des pratiques de souscription

Un facteur clé de la stabilisation du marché a été le perfectionnement des critères de souscription. Certains assureurs ont modifié les modalités de couverture pour mieux gérer les risques émergents, notamment en introduisant des sous-limites ou des exclusions pour certains périls à forte gravité, comme les cyberattaques soutenues par l'État ou les pannes généralisées. De nombreux souscripteurs exigent désormais couramment que les titulaires de polices maintiennent des mesures minimales de cybersécurité (par exemple, l'authentification multifacteur, les sauvegardes régulières de données et la formation du personnel) comme condition de couverture. Ces mesures ont permis d'écarter les risques mal protégés et de réduire les pertes évitables. Grâce à cette approche plus rigoureuse, la concurrence s'est améliorée après la phase corrective. En effet, si certains assureurs limitaient leurs produits de cyberassurance il y a quelques années, de nouveaux acteurs sur le marché élargissent désormais leur offre, profitant d'un secteur d'activité devenu plus prévisible d'un point de vue actuariel.

Capacité accrue et maturité du marché

L'accroissement de la capacité se traduit par une augmentation des limites disponibles et un appétit plus large pour le risque. Les réassureurs, en particulier, ont retrouvé un intérêt pour la cyberassurance après avoir observé une amélioration du rendement en matière de sinistres. Cela a permis aux assureurs principaux d'obtenir plus facilement une réassurance à moindre coût, ce qui leur permet de développer davantage leurs activités. Certains assureurs spécialisés et agents généraux principaux augmentent également leurs portefeuilles de cyberassurance au Canada. Dans l'ensemble, ces évolutions témoignent d'un marché qui arrive à maturité : assureurs et investisseurs considèrent désormais les cyberrisques comme un péril gérable et assurable exigeant toutefois une attention constante.

Concurrence plus saine

Avec le retour de la capacité sur le marché, les clients commencent à ressentir un certain soulagement. Alors que les limites de couverture avaient été fortement réduites lors du marché dur (certaines entreprises ne pouvant souscrire qu'une assurance de 5 à 10 millions de dollars), des limites plus élevées sont désormais disponibles à des tarifs plus stables. Dans certains cas, les entreprises disposant de solides mesures de cybersécurité obtiennent même des rabais sur les primes ou des conditions plus favorables, les assureurs cherchant à attirer les risques les mieux protégés. Cette tendance à récompenser une bonne hygiène numérique crée une boucle vertueuse : elle incite les assurés à investir dans la cybersécurité pour obtenir de meilleurs tarifs, ce qui contribue à réduire les pertes pour les assureurs. Le consensus pour 2025 est que le marché se réajuste : la tarification est plus alignée sur les risques, les couvertures sont mieux définies et la capacité croît à un rythme durable.

10. Le rapport sinistre-primes correspond au rapport entre le total des indemnités versées (y compris les frais de règlement) et le total des primes encaissées. Il s'exprime généralement en pourcentage.
11. Ce rapport constitue un indicateur clé de la rentabilité des activités d'assurance. Il exprime le rapport entre les coûts de sinistres et les charges directement attribuables aux contrats d'assurance, et les produits des activités d'assurance. Un ratio supérieur à 100 % indique généralement une perte dans le résultat des activités d'assurance.
12. BAC, 2024.
13. Une nouvelle norme internationale d'information financière applicable à la comptabilité des contrats d'assurance, l'IFRS 17, est entrée en vigueur le 1er janvier 2023. Cette nouvelle norme mondiale remplace la norme IFRS 4, instaurée en 2004.

Les tendances du marché et les perspectives du secteur

Incertitudes persistantes

Malgré ces signes positifs, les assureurs restent prudents. En effet, la rentabilité future de la cyberassurance demeure incertaine. Les cyberrisques évoluent rapidement, et un seul événement majeur (par exemple, une violation massive de services infonuagiques ou une propagation étendue de logiciels malveillants) pourrait générer des pertes corrélées mettant à l'épreuve le capital du secteur. De plus, à mesure que la concurrence s'intensifie, la pression pour assouplir les exigences de souscription ou réduire les prix pourrait, si cela n'est pas exercé avec prudence, conduire à une nouvelle période d'instabilité du marché. Le sentiment général reste donc celui d'un optimisme réservé : le secteur est désormais plus expérimenté et repose sur des bases plus solides, mais une gestion prudente des risques et l'innovation (tant en souscription qu'en atténuation des risques) restent essentielles pour maintenir cette dynamique.

Nouveaux produits et offres

Parallèlement à la stabilisation du marché, les assureurs diversifient leurs offres de produits de cybersécurité. Une tendance notable est le développement de la cyberassurance personnelle. Traditionnellement, la cyberassurance était presque exclusivement commerciale, mais la multiplication d'incidents médiatisés (comme le vol d'identité, le piratage de comptes financiers et les extorsions en ligne) a fait croître la demande de protection personnelle. En réponse, les assureurs canadiens ont commencé à proposer des polices ou avenants de cyberassurance pour les particuliers. Ces produits couvrent généralement les individus et les familles pour les frais liés à la restauration après un vol d'identité, le paiement de rançons (par exemple lorsqu'un ordinateur personnel est bloqué), la récupération de données et, dans certains cas, le cyberharcèlement ou les atteintes à la réputation. Bien que ce marché en soit encore à ses débuts, la cyberassurance personnelle transpose la gestion des cyberrisques au niveau du consommateur, et les premières souscriptions témoignent d'une sensibilisation croissante aux menaces informatiques, au-delà du cadre des entreprises. Cette tendance représente également une nouvelle voie de croissance pour les assureurs, qui peuvent tirer parti de leur expertise en cybersécurité dans le secteur de l'assurance de détail.

Innovations dans le transfert de risque

Une autre innovation qui renforce le marché est l'utilisation de CAT et d'autres mécanismes de transfert de risque pour la cyberassurance. L'émission d'une obligation catastrophe par l'assureur Beazley, au début de 2023, constitue un exemple marquant, puisqu'il s'agit de la première fois que les marchés financiers prennent directement en charge le risque de catastrophe[14]. Cette obligation offre une protection sous forme d'indemnité pour les événements de cybersécurité extrêmes et systémiques (causant plus de 300 millions de dollars de pertes) et est négociable, ce qui permet d'attirer des capitaux extérieurs au cercle restreint des réassureurs traditionnels. Son succès a démontré la confiance des investisseurs dans des portefeuilles de cybersécurité bien souscrits et leur conviction que le risque catastrophique peut être quantifié et modélisé. Fort de ce précédent, six obligations catastrophes ont été émises en 2024 par quatre émetteurs, pour un total de 785 millions de dollars. Les experts anticipent d'autres transactions par CAT ou couvertures paramétriques[15] dans les années à venir, ce qui augmenterait encore la capacité du marché et sa résilience face aux catastrophes de cybersécurité. Ces évolutions témoignent d'un marché plus robuste et innovant, qui cherche activement des solutions pour gérer les risques extrêmes[16].

En 2025, le marché canadien de la cyberassurance se montre à la fois plus stable et plus mature qu'auparavant. Les assureurs ont su s'adapter aux enjeux d'un environnement à haut risque en améliorant leurs pratiques de souscription et de gestion des risques, et ils étendent désormais leur offre avec prudence. Cette stabilisation profite aux clients, qui bénéficient d'une meilleure accessibilité aux couvertures. Néanmoins, assureurs et assurés restent conscients que la situation peut évoluer rapidement. La section suivante examine comment l'évolution des cyberrisques influencera les tendances futures du marché.

14. Beazley, 9 janvier 2023. Beazley launches market's first cyber catastrophe bond.
15. Assurance qui verse des indemnités en fonction d'un paramètre ou d'un facteur prédéterminé, plutôt qu'en fonction des pertes effectivement subies.
16. Possibilité d'événements très rares, mais très graves qui se situent aux extrémités de la courbe des pertes, et qui peuvent entraîner des conséquences financières majeures.

Un paysage des cyberrisques en pleine mutation au Canada

Un paysage des cyberrisques en pleine mutation au Canada

En 2025, les cybermenaces ont encore gagné en complexité. Elles exercent une pression constante sur les assureurs comme sur les entreprises, qui doivent sans cesse tenter de garder une longueur d'avance. Deux tendances dominent en 2025 : l'essor des attaques basées sur l'IA et la persistance des rançongiciels, toujours capables de contourner les mesures de protection en place. Comprendre ces menaces en constante évolution est essentiel, tant pour les assureurs (qui doivent adapter leurs modèles et leur couverture) que pour les entreprises (qui doivent renforcer leurs défenses), car elles influent directement sur la fréquence et la gravité des sinistres.

Menaces alimentées par l'IA et nouveaux vecteurs d'attaque

L'une des évolutions les plus marquantes du paysage des cybermenaces est l'utilisation de l'IA par les acteurs malveillants. Au cours de l'année écoulée, des groupes de pirates informatiques ont de plus en plus exploité les outils d'IA générative pour mener des attaques d'ingénierie sociale plus convaincantes et à grande échelle. Les campagnes d'hameçonnage basées sur l'IA sont désormais monnaie courante : les pirates informatiques s'appuient sur de grands modèles de langage pour créer des courriels personnalisés et très convaincants, rédigés dans un style et un ton qui imitent fidèlement ceux de la personne ciblée[17]. Résultat : ces messages, souvent impeccables sur le plan grammatical et adaptés à la personne visée, sont plus difficiles à distinguer d'une communication authentique et obtiennent un meilleur taux de réussite. Concrètement, même des membres du personnel expérimentés peuvent se faire piéger, ce qui ouvre la voie à des intrusions dans les systèmes d'entreprise par vol d'identité ou via des liens malveillants.

Autre tendance inquiétante : la montée en puissance de l'hypertrucage. L'IA générative permet aujourd'hui de créer des voix et des vidéos d'un réalisme troublant. Les fraudeurs exploitent déjà ces technologies pour usurper l'identité de dirigeants et mener des arnaques de type fraude du président. Ainsi, un membre du personnel peut recevoir un extrait audio généré par l'IA imitant la voix de son PDG et l'incitant à effectuer un virement bancaire, ou encore un courriel d'hameçonnage comportant une vidéo hypertruquée destinée à rendre sa demande plus crédible. Le Centre canadien pour la cybersécurité alerte d'ailleurs sur ce phénomène : « Les outils d'IA générative permettent aux auteures et auteurs de cybermenace de créer du contenu visuel et audio réaliste en usurpant l'identité de personnes de confiance (c'est-à-dire l'hypertrucage), ce qui renforce l'apparence de légitimité aux yeux des cibles et aide à les persuader.[18] » Ce type de fraude par piratage psychologique, rendu possible par l'hypertrucage, peut contourner les mécanismes classiques de vérification et a déjà provoqué des incidents de cybersécurité à l'échelle internationale.

Au-delà de l'hameçonnage, l'IA est aussi utilisée pour perfectionner les logiciels malveillants. Les chercheurs en cybersécurité observent l'apparition de programmes capables de s'adapter de façon autonome ou d'échapper aux systèmes de protection. Bien que ce phénomène en soit encore à ses débuts, les cybercriminels déploient déjà des algorithmes d'IA capables d'adapter rapidement le comportement d'un code malveillant pour contourner les antivirus, et même de sélectionner intelligemment leurs cibles une fois infiltrés dans un réseau. L'IA peut également aider les pirates informatiques à repérer des vulnérabilités (en analysant rapidement du code à la recherche de failles), ce qui pourrait accélérer la mise au point d'exploits du jour zéro[19]. Un exemple de cette tendance est celui des « rançongiciels adaptatifs », c'est-à-dire des rançongiciels qui pourraient, à terme, utiliser l'IA pour adapter dynamiquement leurs méthodes de chiffrement ou sélectionner les données à viser selon les sauvegardes ou les dispositifs de sécurité de la victime. En somme, il est question d'optimiser l'attaque afin de causer un maximum de dommages. Les rançongiciels actuels ne reposent pas encore entièrement sur l'IA, mais leur automatisation et leur sophistication croissantes annoncent cette évolution.

Ces menaces facilitées par l'IA élargissent le champ des risques et rendent les attaques plus crédibles, plus efficaces et plus répandues. Elles abaissent les coûts et le seuil de compétence nécessaire aux pirates informatiques (même des cybercriminels peu expérimentés peuvent recourir à des outils d'IA en tant que service pour améliorer leurs escroqueries), en plus d'alourdir la charge qui pèse sur les systèmes de défense et les assureurs. Pour ces derniers, la montée des attaques renforcées par l'IA pourrait se traduire par une fréquence accrue des sinistres (puisque des hameçonnages plus convaincants entraînent davantage d'intrusions) et par des pertes plus lourdes (si, par exemple, des fraudes par hypertrucage provoquent

17. Évaluation des cybermenaces nationales 2025-2026, Centre canadien pour la cybersécurité.
18. IBID.
19. Le développement d'exploits du jour zéro désigne le processus qui consiste à découvrir et à créer des outils ou techniques permettant d'exploiter des vulnérabilités jusque-là inconnues dans un logiciel, un matériel ou un microprogramme, avant même que le fournisseur ou le public n'en ait connaissance.

des transferts frauduleux de grande valeur). Cette situation met en lumière la nécessité de revoir en permanence les questionnaires de souscription, par exemple en vérifiant les procédures de confirmation des paiements ou en formant le personnel à l'égard des courriels d'hameçonnage assistés par l'IA.

Rançongiciels et évolution des cybercriminels

Si les nouvelles attaques informatiques appuyées par l'IA attirent l'attention, les cybermenaces traditionnelles comme les rançongiciels continuent de dominer le paysage des risques et évoluent de pair avec les mécanismes de défense. Les rançongiciels demeurent la principale menace de cybercriminalité pour les entreprises canadiennes et les infrastructures essentielles. Pour les cyberassureurs, ils constituent la première source de sinistres majeurs depuis plusieurs années, et les statistiques de 2025 confirment que la menace est loin de reculer.

Le Centre canadien pour la cybersécurité met en lumière plusieurs données préoccupantes dans son rapport intitulé *Évaluation des cybermenaces nationales 2025-2026*. Selon les autorités canadiennes en cybersécurité, « la portée, la fréquence et la complexité des attaques par rançongiciel ne font qu'augmenter » depuis 2020[20]. Par ailleurs, l'année 2023 a marqué un record mondial d'activité en la matière. Le Centre cite estime notamment que les incidents liés aux rançongiciels auraient augmenté de 74 % à l'échelle mondiale en 2023 par rapport à l'année précédente, avec des paiements de rançon connus totalisant environ 1,368 milliard de dollars américains, le niveau le plus élevé jamais enregistré[21]. Au Canada, les incidents signalés au Centre c ont augmenté en moyenne de 26 % par année depuis 2021[22]. En 2023, le montant moyen versé par les victimes au Canada s'élevait à 1,13 million de dollars canadiens, soit une hausse de près de 150 % en deux ans[23]. Ces chiffres restent probablement en deçà de la réalité, puisque de nombreux cas ne sont jamais déclarés.

Les organisations criminelles spécialisées dans les attaques par rançongiciel sont désormais hautement professionnalisées et agiles. Beaucoup adoptent un modèle de type rançongiciels en tant que service, où les développeurs principaux louent leurs logiciels malveillants prêts à l'emploi à des affiliés. Cette formule élargit leur portée tout en perfectionnant sans cesse les logiciels malveillants. À mesure que les entreprises renforcent leurs sauvegardes et leurs plans d'intervention, les opérateurs de rançongiciel adaptent leurs méthodes : Pratique de la double extorsion (voler les données avant de les chiffrer afin de menacer de les divulguer), voire de la triple extorsion (s'en prendre aux clients ou partenaires de la victime initiale pour accentuer la pression). Ils visent aussi de plus en plus les données et systèmes essentiels afin de causer un maximum de perturbations dans les activités.

Le Centre canadien pour la cybersécurité souligne que les opérateurs de rançongiciel « peaufinent constamment leurs tactiques pour maximiser les profits » [24]. De fait, leurs opérations deviennent plus agiles et plus résistantes aux interventions des forces de l'ordre comme aux mesures de défense. Le ralentissement temporaire de l'activité observé en 2022 (attribué au démantèlement réussi de certaines organisations criminelles) a été suivi d'un rebond en 2023, signe que de nouveaux opérateurs (ou des anciens réorganisés) ont rapidement comblé le vide.

L'éventail des cibles s'élargit également. À l'origine, les cybercriminels visaient les grandes entreprises et institutions (sources de gains élevés), mais beaucoup se tournent désormais vers des petites ou moyennes

20. Évaluation des cybermenaces nationales 2025-2026, Centre canadien pour la cybersécurité.
21. IBID.
22. IBID.
23. IBID.
24. IBID.

entreprises, qui disposent souvent de systèmes de protection plus faibles. Parmi les victimes, on retrouve nombre d'entités disposant de ressources limitées, comme des municipalités, des hôpitaux ou des PME. Le message est clair : aucune entreprise n'est « trop petite » pour attirer des cybercriminels, surtout si elle fait partie d'une chaîne d'approvisionnement plus vaste ou si elle est assurée contre ce type de risque. Cette diversification des victimes entraîne une répartition plus large des pertes dans l'économie et pousse les assureurs à étendre leur couverture et leur soutien en gestion des risques à des secteurs qui, historiquement, accordaient moins d'importance à la cybersécurité.

Au-delà des rançongiciels, d'autres menaces persistent. Les fraudes du président continuent de causer des pertes financières importantes et s'appuient de plus en plus sur des outils d'IA comme ceux évoqués précédemment (par exemple, l'utilisation de l'hypertrucage dans des fraudes par téléphone). Les attaques de la chaîne d'approvisionnement (où des pirates informatiques compromettent un fournisseur de logiciels ou un prestataire de services de TI pour atteindre ses clients) demeurent une source de préoccupation majeure. En effet, de telles attaques peuvent toucher simultanément de nombreux assurés et générer un cumul de sinistres pour les assureurs. Les attaques visant les infrastructures essentielles (parfois menées par des acteurs étatiques ou des cybermilitants) constituent une autre menace : le piratage de réseaux pipeliniers ou de réseaux de distribution d'électricité, par exemple, peut engendrer non seulement des pertes économiques, mais aussi des risques pour la sécurité publique. Ces menaces ne sont pas nouvelles, mais les méthodes utilisées évoluent en parallèle des défenses déployées par les entreprises. Les cybercriminels cherchent désormais plus souvent à passer inaperçus en utilisant des outils administratifs légitimes à des fins malveillantes (exploitation des ressources locales), en recourant à des canaux chiffrés ou en lançant leurs attaques en dehors des heures de bureau. Le temps de présence moyen d'un intrus sur un réseau avant sa détection a heureusement diminué : Il s'établissait à une médiane mondiale de 10 jours en 2023, contre 16 jours en 2022, selon des rapports de cybersécurité. Cependant, même dix jours offrent encore largement le temps nécessaire à un cybercriminel expérimenté pour perfectionner son attaque[25].

Implications pour le secteur de l'assurance :

L'évolution constante des menaces oblige les assureurs à faire preuve d'adaptabilité. Les clauses des polices sont sans cesse mises à l'épreuve par de nouveaux scénarios de réclamation (par exemple, un virement frauduleux de fonds au moyen de l'hypertrucage pourrait relever, selon le contrat, soit d'une assurance vol et détournements, soit d'une cyberassurance). Les assureurs collaborent de plus en plus avec des firmes spécialisées en cybersécurité pour offrir des services à valeur ajoutée, tels que des filtres de courriels basés sur l'IA, des services de veille sur les menaces ou des ententes de services de réponse aux incidents. Ces services permettent aux assurés de prévenir ou de limiter les pertes liées aux menaces les plus sophistiquées. En 2025, les souscripteurs posent des questions beaucoup plus détaillées sur la façon dont les entreprises gèrent ces nouveaux risques. Par exemple : *Disposez-vous de protocoles de vérification pour lutter contre la fraude par hypertrucage? Proposez-vous à votre personnel des formations pour reconnaître les tentatives d'hameçonnage basées sur l'IA? Avez-vous segmenté vos réseaux pour limiter la propagation d'un rançongiciel?* Les réponses à ces questions peuvent influencer la décision d'accorder une couverture et le prix de celle-ci.

En 2025, les cybermenaces se caractérisent à la fois par des éléments nouveaux et des tendances persistantes. Les rançongiciels et les fraudes par piratage psychologique demeurent les principaux risques, mais l'arrivée de technologies comme l'IA leur donne une ampleur inédite. Cette évolution impose à toutes les entreprises d'élever leur niveau de cybersécurité. Même si les souscriptions se sont récemment améliorées, le marché de la cyberassurance continue de faire face à un environnement exigeant de risque. La section suivante examine comment le cadre législatif et réglementaire canadien répond ou non à ces risques, et met en évidence les implications pour les parties prenantes.

25. Google Cloud Blog. 23 avril 2024. M-Trends 2024: Our View from the Frontlines.

Les développements législatifs et le cadre réglementaire

Les développements législatifs et le cadre réglementaire

La cybersécurité ne dépend pas uniquement des forces du marché : elle nécessite également des cadres réglementaires clairs et exécutoires. Au Canada, les progrès réglementaires à cet égard ont été inégaux. En 2024, beaucoup espéraient l'adoption du projet de loi C-26 *(Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois)*, qui visait à moderniser le régime canadien de cybersécurité en introduisant des normes obligatoires et des obligations de déclaration pour les secteurs d'infrastructures essentielles tels que les télécommunications, l'énergie, les services financiers et les transports. Inspiré de régimes internationaux comme le *Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA) aux États-Unis et la directive SRI 2 (sécurisation des réseaux et des systèmes d'information) de l'Union européenne, ce projet de loi aurait exigé des opérateurs désignés qu'ils mettent en place des programmes de cybersécurité, déclarent les incidents et corrigent les vulnérabilités connues sous supervision fédérale.

Malgré quelques progrès et amendements adoptés au Sénat, le projet de loi C-26 n'a finalement pas reçu la sanction royale en raison de la prorogation du Parlement en janvier 2025. Ainsi, au début de l'année 2025, le Canada demeurait sans loi nationale sur la cybersécurité applicable aux infrastructures essentielles, laissant un vide réglementaire que le secteur de l'assurance et de la cybersécurité considère comme préoccupant.

Le 18 juin 2025, le gouvernement fédéral a relancé ces efforts en présentant le projet de loi C-8 *(Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois)*, qui reprend le projet de loi C-26. Bien que son adoption soit encore en attente au moment de la rédaction de ce rapport, le projet de loi C-8 témoigne d'un engagement fédéral renouvelé en faveur de l'instauration d'un cadre réglementaire en matière de cybersécurité. Toutefois, d'ici l'adoption de ce projet de loi, l'absence de cadre législatif continuera d'alimenter un climat de risque et d'incertitude pour les exploitants d'infrastructures essentielles et pour le secteur de l'assurance.

Implications du vide législatif actuel

Risque pour les infrastructures essentielles

En l'absence d'un cadre réglementaire clair, la cybersécurité des systèmes essentiels (réseaux électriques, pipelines, télécommunications, services financiers, etc.) repose largement sur les initiatives des entreprises et sur des règles propres à chaque secteur, très variables. Cette approche fragmentée augmente le risque de défaillances systémiques. Un incident important de cybersécurité touchant les infrastructures essentielles pourrait provoquer des effets en chaîne.

Retard du Canada sur la scène internationale

D'autres pays semblent déjà avoir mis en place des lois détaillées en matière de cybersécurité. Aux États-Unis, la déclaration obligatoire des incidents est en vigueur, tandis que la directive SIR 2 de l'Union européenne impose des obligations strictes aux secteurs essentiels. Le Canada, en revanche, n'a pas de cadre intersectoriel, ce qui peut rendre ses infrastructures plus vulnérables aux cybermenaces et donc plus intéressantes pour les pirates informatiques, et compliquer la coopération internationale. Pour les assureurs opérant à l'échelle mondiale, cette position par rapport à la réglementation peut se traduire par une prudence accrue au moment de déployer des capitaux.

Les développements législatifs et le cadre réglementaire

La stratégie gouvernementale en attendant une loi

En l'absence de loi, le gouvernement fédéral mise sur des initiatives politiques et des partenariats. La Stratégie nationale de cybersécurité renouvelée, *Sécuriser l'avenir numérique du Canada*, fixe les priorités jusqu'en 2027 : protection des infrastructures, lutte contre la cybercriminalité et coordination à l'échelle de la société.

Parmi les initiatives phares figure la mise sur pied du Collectif canadien pour la cyberdéfense (CCCD), une plateforme nationale de collaboration qui rassemble gouvernement, exploitants d'infrastructures, entreprises de cybersécurité, assureurs et universitaires. Son objectif est de favoriser la communication d'information, de coordonner les mesures d'intervention en cas d'incident et de promouvoir les pratiques exemplaires. Pour les assureurs, ce type de collaboration est crucial : il permet de mieux comprendre les risques systémiques émergents et d'envisager des solutions, comme la mise en place éventuelle d'un filet de cybersécurité soutenu par le gouvernement, à l'image des modèles d'assurance contre le terrorisme à l'étranger.

La législation sur la protection de la vie privée en suspens

Les cyberrisques sont étroitement liés à la protection des données. Parallèlement au projet de loi C-26, le gouvernement fédéral avait également présenté le projet de loi C-27 : *Loi de 2022 sur la mise en œuvre de la Charte du numérique, qui proposait de mettre en œuvre la Loi sur la protection de la vie privée des consommateurs et la Loi sur l'intelligence artificielle et les données.* S'il avait été adopté, ce projet de loi aurait renforcé les droits à la vie privée, augmenté les sanctions en cas de non-conformité et introduit de nouvelles obligations concernant l'utilisation des données et des systèmes d'IA. Cependant, le projet de loi C-27 a également été abandonné à la suite de la prorogation du Parlement et n'a pas encore été réintroduit. Résultat : la réglementation sur la protection des données au Canada demeure fragmentée, laissant entreprises et assureurs dans l'incertitude face aux cyberrisques.

La section suivante s'intéresse à l'un des groupes les plus vulnérables dans ce contexte : les PME, qui manquent souvent de ressources et de repères réglementaires clairs pour gérer efficacement les cyberrisques.

Le fossé en matière de cyberassurance pour les PME : enjeux et occasions

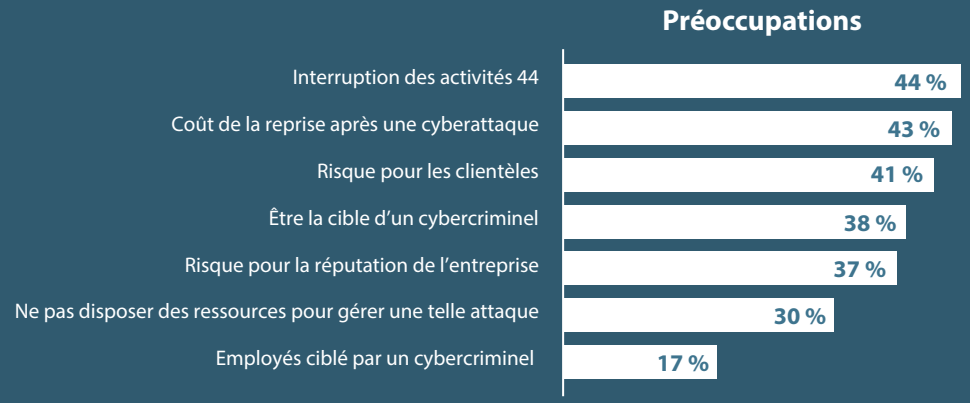
L'attitude adoptée à l'endroit des cyberrisques

Selon **61 %** des PME répondants, leur entreprise est trop petite pour être ciblée.

La cybersécurité n'est pas une priorité financière pour 64 % des PME répondantes.

Seules 12 % des PME répondantes ont souscrit une police de cyberassurance autonome.

Les trois principales préoccupations en matière de cyberrisques pour les propriétaires et les décideurs interrogés dans les petites et moyennes entreprises sont l'interruption des activités, le coût de la reprise à la suite d'une cyberattaque ou d'une violation des données, ainsi que le risque pour leurs clientèles.



Parmi les répondants, **27 %** se disent également préoccupés par le risque d'être poursuivis en justice à la suite d'une cyberattaque.

Sondage réalisé par Angus Reid pour le compte du Bureau d'assurance du Canada du 6 au 15 août 2025. Le rapport complet est disponible au www.cybersavvycanada.ca.

Le fossé en matière de cyberassurance pour les PME : enjeux et occasions

Les PME forment l'épine dorsale de l'économie canadienne et représentent la majorité des entreprises au pays. Pourtant, lorsqu'il s'agit de cyberrisque et d'assurance, elles demeurent particulièrement vulnérables et souvent sous-assurées. Beaucoup n'ont pas les ressources dont disposent les grandes entreprises pour investir dans la cybersécurité. En 2025, un défi subsiste : les PME font face à des cybermenaces croissantes, mais leur recours à la cyberassurance reste très limité. Cette section analyse la situation des PME face aux cyberrisques, les raisons de cette faible adoption et les initiatives (existantes ou nécessaires) pour combler ce manque.

Selon les estimations, seules environ 12 % des petites entreprises canadiennes bénéficient d'une couverture de cyberassurance autonome[26]. Comme la majorité d'entre elles sont des PME, ce chiffre reflète le faible taux de souscription dans ce secteur. Ce phénomène n'est pas propre au Canada : d'autres pays développés observent également une couverture limitée parmi les petites structures[27]. Même parmi les entreprises de taille moyenne, souvent conscientes des cyberrisques, beaucoup choisissent de ne pas souscrire une cyberassurance, surtout si cela n'est pas exigé par leurs partenaires commerciaux. Ce faible niveau de couverture contraste fortement avec l'exposition réelle aux risques. Des études montrent qu'une part importante des cyberattaques (rançongiciels, hameçonnage et autres) touche les petites entreprises. Les PME sont précisément la cible des cybercriminels parce qu'elles disposent de défenses plus fragiles et sont plus susceptibles de payer une rançon modeste.

Enjeux rencontrés par les PME

Conscience et perception du risque

De nombreux propriétaires de PME sous-estiment encore leur exposition aux cyberrisques. Beaucoup pensent que les cyberattaques ne concernent que les grandes entreprises ou qu'une petite entreprise « sans intérêt » ne serait pas ciblée. Les PME possèdent des données sensibles (renseignements personnels des clients, données de paiement, etc.) et peuvent constituer un point d'entrée vers des réseaux plus importants, ce qui en fait des cibles idéales. La sensibilisation aux risques progresse lentement, notamment grâce aux médias locaux qui couvrent les incidents touchant de petites entreprises, comme les violations de données ou les rançongiciels. Toutefois, une partie des PME sous-évaluent leurs cyberrisques, alors que d'autres les confondent avec l'assurance responsabilité civile générale ou supposent que leur fournisseur de services de TI gère tous les cyberrisques. Cette méconnaissance explique pourquoi, même lorsque l'assurance est disponible, elle n'est pas nécessairement souscrite. Selon les experts du secteur de l'assurance, l'éducation des propriétaires de PME est essentielle pour accroître la souscription. Il faut leur faire comprendre que les cyberrisques sont aussi importants qu'un incendie ou un vol[28].

Coût et accessibilité

Même si la prise de conscience progresse, le coût et l'accès à la cyberassurance restent des obstacles communs pour les PME. Durant la période de marché dur (2020–2022), les primes ont augmenté, ce qui a rendu certaines couvertures inabordables pour les petites entreprises. Le processus de souscription peut aussi paraître complexe, notamment pour les PME qui n'ont pas de service de soutien informatique interne, car il comporte souvent des questions détaillées sur les pratiques de cybersécurité. Dans certains cas, la couverture dépend de la mise en place de mesures minimales de sécurité, comme l'authentification multifacteur, ce qui peut nécessiter des investissements supplémentaires. En conséquence, l'accès à la cyberassurance reste un défi pour certaines PME, en raison d'obstacles à la fois financiers et opérationnels. Il est toutefois encourageant de constater qu'en 2024 et 2025, les tarifs avaient commencé à se stabiliser, offrant aux assureurs une meilleure occasion de proposer des solutions plus adaptées et accessibles pour les PME.

26. Sondage réalisé par Angus Reid pour le compte du Bureau d'assurance du Canada du 6 au 15 août 2025.
27. Exemples en Australie et au Royaume-Uni : https://insurancecouncil.com.au/wp-content/uploads/2022/03/Cyber-Insurance_March2022-final.pdf? et https://www.gov.uk/government/publications/adoption-of-cyber-insurance-by-uk-small-and-medium-sized-enterprises?.
28. Cornell University, 29 septembre 2023. Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity.

Le fossé en matière de cyberassurance pour les PME : enjeux et occasions

Absence de solutions adaptées

Les produits de cyberassurance ont longtemps été conçus pour les moyennes et grandes entreprises, avec des garanties et des plafonds souvent mal adaptés aux besoins particuliers des petites entreprises ou des organismes sans but lucratif. Par exemple, une petite boutique pourrait n'avoir besoin que de 100 000 dollars pour couvrir les frais liés à une violation de données et à une brève interruption des activités, alors que de nombreuses polices proposent des plafonds de 1 million de dollars, assortis de primes élevées. De plus, certaines clauses incluent des garanties superflues pour les petites structures (comme les frais de gestion de crise), mais laissent de côté des protections importantes (comme la perte de revenus en cas de perturbation d'un site de commerce en ligne). Cette inadéquation empêche certaines PME de souscrire une couverture réellement adaptée. Le marché évolue toutefois : les assureurs développent de plus en plus des formules ou des avenants modulables, adaptés aux petites entreprises. Ces solutions offrent des plafonds plus modestes et une souscription simplifiée, et ce qui permet de proposer une couverture sur mesure, à la fois pertinente et abordable.

Niveau de préparation en cybersécurité

Beaucoup de PME n'en sont encore qu'aux premiers stades de la mise en place de leur dispositif de cybersécurité, ce qui complique à la fois la gestion des risques et leur accès à l'assurance. Faute d'équipes dédiées à la cybersécurité, elles se tournent souvent vers des solutions de base (antivirus, pare-feu, sauvegardes, etc.) dont la mise en œuvre varie selon leurs ressources et leur niveau de sensibilisation. Pour les assureurs, cette hétérogénéité rend l'évaluation et la tarification des risques de cybersécurité plus complexes. Certains imposent donc des exigences minimales (pare-feu, antivirus, sauvegardes régulières) afin de garantir un certain niveau de protection. Les PME qui ne satisfont pas encore à ces exigences sont souvent invitées à renforcer leur système de cybersécurité et à présenter une nouvelle demande, parfois avec un accompagnement ou des conseils. À mesure que les outils deviennent plus accessibles et que la sensibilisation progresse, le niveau de préparation des PME devrait s'améliorer et renforcer à la fois leur résilience et leur assurabilité.

Conséquences de la sous-assurance

Le faible recours à la cyberassurance entraîne plusieurs conséquences. Pour une entreprise, même une attaque informatique mineure peut avoir des répercussions financières considérables. La facture peut rapidement atteindre des dizaines, voire des centaines de milliers de dollars, même pour un petit incident mineur (nécessitant, par exemple, des enquêtes techniques, la restauration des données, des avis aux clients concernés et des frais juridiques). C'est souvent une somme que peu de petites entreprises peuvent assumer. Dans les cas les plus graves, une cyberattaque peut même mener à la fermeture définitive de l'entreprise. À l'échelle macroéconomique, la sous-assurance généralisée des PME oblige l'économie canadienne à absorber ces pertes sans bénéficier du filet de sécurité qu'offre l'assurance. Le défi est donc de trouver un modèle qui reste viable pour les assureurs tout en restant abordable pour les PME.

Initiatives pour combler le fossé

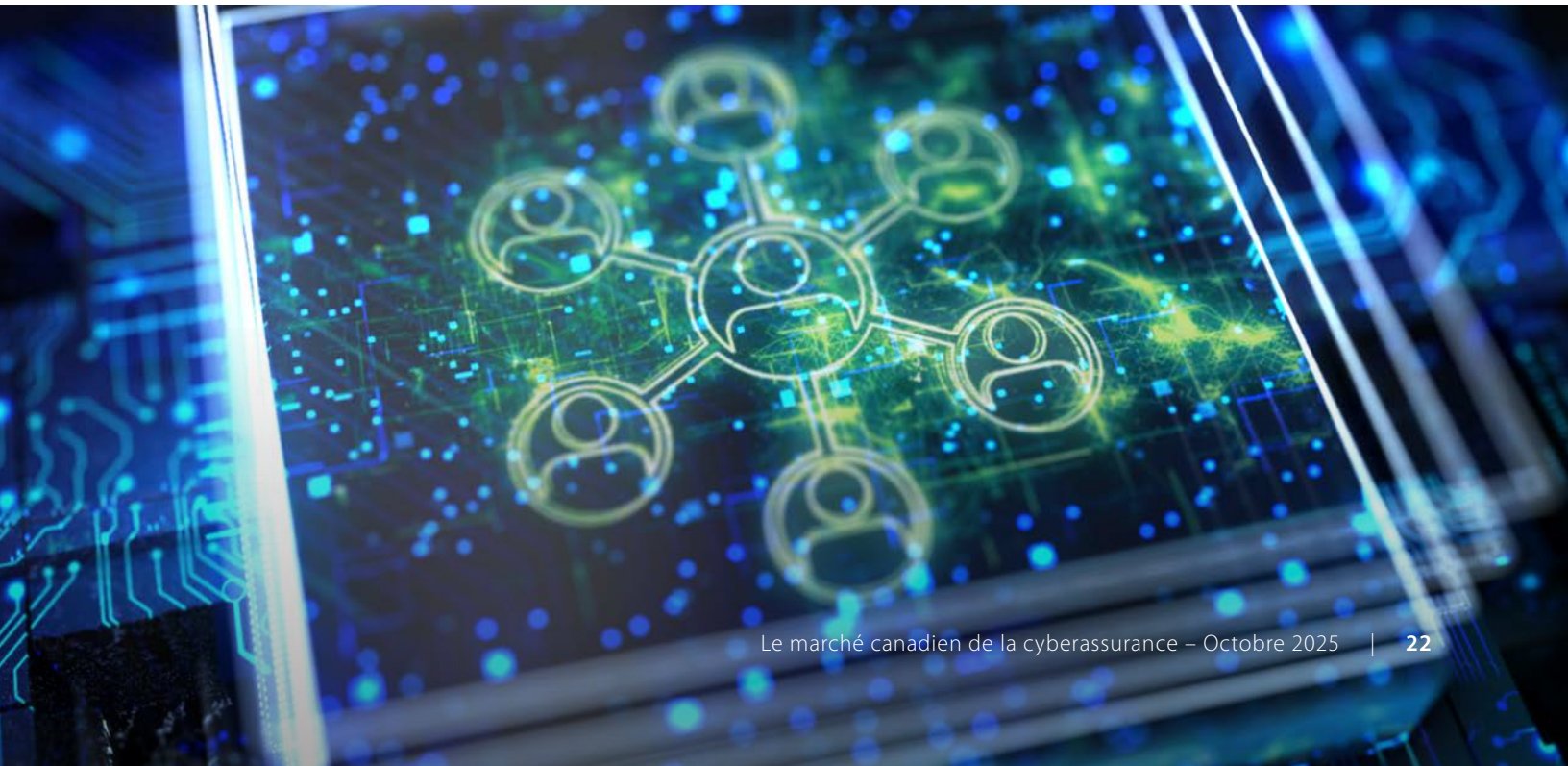
Face à ce constat, les assureurs comme les gouvernements au Canada cherchent à réduire l'écart de couverture des PME en cybersécurité. Parmi les principales initiatives, il y a les suivantes :

- **Campagnes de sensibilisation et d'éducation :** Le secteur de l'assurance et les pouvoirs publics jouent tous deux un rôle actif dans la sensibilisation des PME à la cybersécurité. Le Bureau d'assurance du Canada (BAC) mène chaque année la campagne Cyber Savvy, qui propose des ressources pédagogiques et un outil d'autoévaluation en dix questions pour aider les propriétaires de PME à définir leur profil de cyberrisque et leur niveau de préparation. L'initiative reprend le type de questions posées par les assureurs, ce qui permet de mettre en évidence les failles de sécurité et d'encourager les PME à apporter des améliorations concrètes. De leur côté, les assureurs et les courtiers participent eux aussi de plus en plus à ces efforts de sensibilisation, en proposant des webinaires, des listes de vérification et des services de conseil pour aider les PME à mieux comprendre leurs expositions aux risques et à déterminer les mesures nécessaires pour être admissibles à une couverture. Au niveau fédéral, l'initiative Pensez cybersécurité propose quant à elle des guides simples et accessibles pour promouvoir l'hygiène numérique, tant auprès des entreprises que des particuliers. Ensemble, ces initiatives contribuent à démystifier la cyberassurance, encouragent l'adoption de pratiques exemplaires en matière de sécurité et soutiennent les PME dans le renforcement de leur résilience.

Le fossé en matière de cyberassurance pour les PME : enjeux et occasions

- **Création de nouveaux produits adaptés aux PME :** Les assureurs développent de plus en plus de produits de cyberassurance spécialement conçus pour répondre aux besoins des petites entreprises. En effet, beaucoup proposent désormais des avenants intégrés à des polices existantes de responsabilité civile ou d'assurance des biens, offrant ainsi une couverture de base. Cette approche groupée favorise la souscription, puisque le produit peut être présenté au point de vente comme une composante d'un ensemble plus large de protections. En parallèle, certains assureurs simplifient le processus de demande et de souscription, et recourent par exemple à des données externes pour évaluer les risques ou à des formulaires plus courts et plus accessibles. Ces offres incluent souvent des services à valeur ajoutée, comme des lignes d'assistance en cas d'incident, particulièrement utiles pour les entreprises qui n'ont pas de service de soutien informatique interne. En clarifiant la couverture, en réduisant son coût et en l'intégrant aux polices existantes, ces innovations contribuent à éliminer les obstacles et à accroître l'intérêt des PME pour la cyberassurance.

En résumé, les PME restent le maillon faible de la résilience numérique du Canada : la majorité n'étant pas assurée, elles sont particulièrement vulnérables. Toutefois, l'année 2025 est marquée par des efforts concertés visant à mieux mobiliser ce secteur. La prise de conscience progresse : protéger les PME est une condition essentielle à la sécurité des échanges et des chaînes d'approvisionnement dans leur ensemble. Il s'agit aussi d'un potentiel de croissance pour les assureurs. Si les rapports sinistres-primes continuent de s'améliorer et que les assureurs parviennent à concevoir des produits viables pour les risques de moindre gravité, il est probable que le secteur de la cyberassurance connaisse, dans les prochaines années, une expansion importante au sein du marché des PME.



Conclusion

En 2025, le marché canadien de la cyberassurance repose sur des bases plus solides qu'auparavant. Après une période marquée par une forte volatilité, il s'est stabilisé grâce à des critères de souscription plus stricts, une sinistralité plus prévisible et une diversification accrue de l'offre de produits. La stabilisation des prix, le retour d'une offre de couverture plus large et l'essor des partenariats public-privé témoignent de la maturation progressive du marché, qui s'affirme désormais comme un secteur d'activité durable[29].

Cette évolution positive survient toutefois dans un contexte de cybermenaces en constante aggravation. La multiplication des attaques informatiques appuyées par l'IA et la sophistication croissante des rançongiciels soulèvent de nouveaux enjeux et mettent en lumière la nécessité de maintenir un haut niveau d'innovation et de vigilance[30]. Les assureurs ont déjà mis au point des modèles de scénarios catastrophes et élargi leur recours à des outils comme la réassurance et les obligations catastrophes, mais seule l'épreuve des faits permettra de tester la fiabilité de ces mécanismes[31].

Sur le plan réglementaire, l'échec du projet de loi C-26 par le gouvernement précédent a laissé un vide important dans le cadre national de cybersécurité du Canada, particulièrement pour les infrastructures essentielles. Toutefois, le dépôt du projet de loi C-8 traduit la volonté renouvelée du gouvernement fédéral d'instaurer une surveillance et des normes obligatoires. Parallèlement, des initiatives comme le Collectif canadien pour la cyberdéfense (CCCD) et la Stratégie nationale de cybersécurité contribuent à renforcer la coordination intersectorielle, à améliorer les capacités de riposte et à jeter les bases d'un écosystème numérique plus résilient.

Dans les années à venir, la priorité sera d'étendre la couverture en cybersécurité aux entreprises les plus exposées, en particulier les PME. Avec seulement 12 % d'entreprises canadiennes assurées, l'écart de protection représente à la fois une vulnérabilité majeure et un potentiel de croissance[32]. Le combler exigera une innovation continue, des efforts ciblés de sensibilisation et, possiblement, des mesures incitatives soutenues par l'État.

Ainsi, le secteur canadien de la cyberassurance entre dans une phase d'optimisme prudent. Ses fondations sont plus robustes, mais les menaces continuent d'évoluer rapidement. Seule une collaboration soutenue entre le secteur, les autorités publiques et les entreprises permettra de bâtir une économie capable de résister aux cybermenaces..

29. BAC, 2024.
30. Centre canadien pour la cybersécurité, 2024.
31. Insurance Business, Smith, J., 2023.
32. BAC, 2024.

Sources :

- **BAC (Bureau d'assurance du Canada). (2024).** *Matériel de la campagne Cyber Savvy* : renforcement de la sensibilisation des PME à la cybersécurité et à leur préparation en matière d'assurance, notamment en introduisant un outil d'autoévaluation.
- **BAC (Bureau d'assurance du Canada). (2024).** *« Le marché canadien de la cyberassurance 2024. »* : principales statistiques du marché et analyses sur les rapports sinistres-primes, la croissance du marché et les nouveaux produits.
- **Centre pour la cybersécurité (Centre canadien pour la cybersécurité). (2021)**. *« Bulletin sur les cybermenaces : La menace des rançongiciels en 2021. »* : statistiques sur les incidents liés aux rançongiciels et leurs répercussions financières sur les entreprises canadiennes.
- **Centre pour la cybersécurité (Centre canadien pour la cybersécurité)**. *« Évaluation des cybermenaces nationales 2025-2026. »*
- **Centre pour la cybersécurité (Centre canadien pour la cybersécurité).** *« Évaluation des cybermenaces nationales 2023-2024. »* : analyse des menaces actuelles, notamment les attaques facilitées par l'IA et statistiques sur les rançongiciels.
- **DiSabatino, A. (2024).** *« The rise and fall of cyber policy growth. »* Canadian Underwriter.
- **Sécurité publique Canada. (2023).** *« Stratégie nationale de cybersécurité du Canada : 2023–2027. »* : initiative fédérale qui met l'accent sur les partenariats public-privé, notamment avec le Collectif canadien pour la cyberdéfense (CCCD).
- **Araullo, K. (2024).** *« Beazley completes $140 million cyber catastrophe bond. »* Insurance Business Magazine : aperçu de la première obligation catastrophe de cyberassurance et de ses implications pour le marché.
- **Westman, R. (2025).** *« Canada's Draft Cybersecurity Legislation Must Be Resurrected. »* Centre pour l'innovation dans la gouvernance internationale : discussion sur les objectifs du projet de loi C-26 et les conséquences de son échec.

ibc.ca