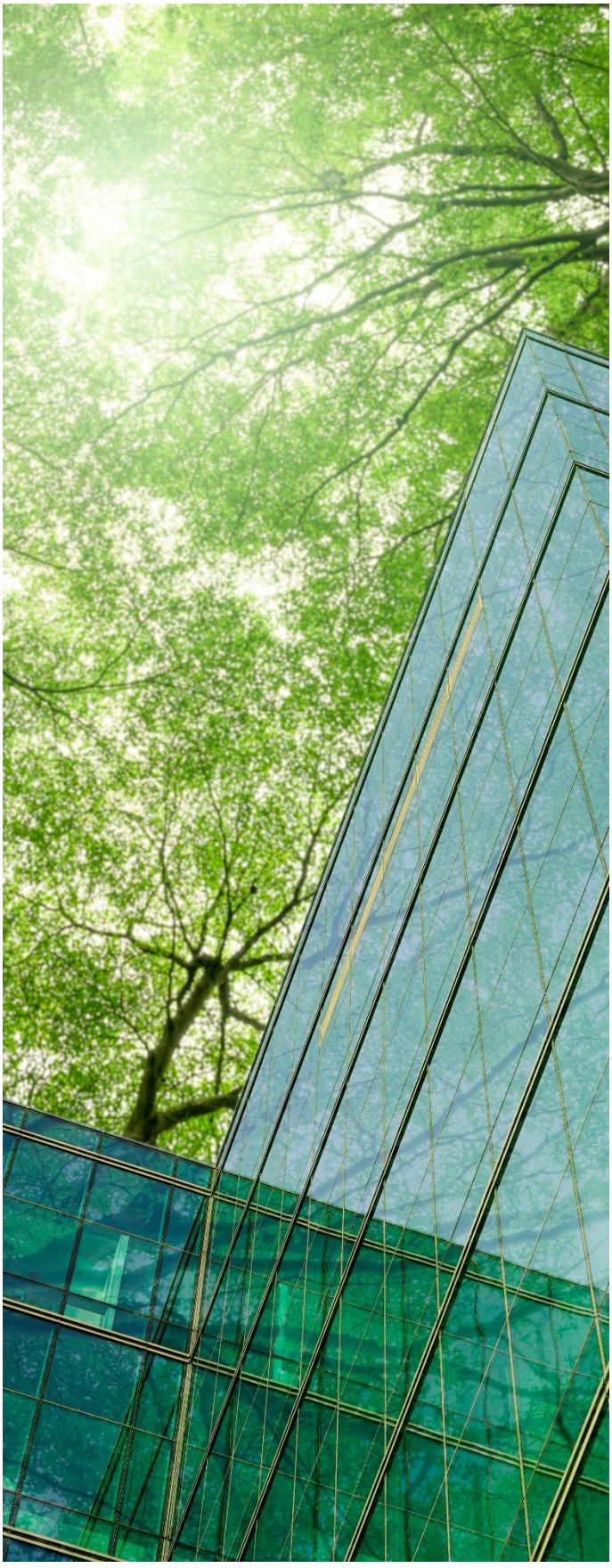


MIEUX COMPRENDRE LA CYBERASSURANCE : UN ÉLÉMENT ESSENTIEL DE LA STRATÉGIE DE CYBERSÉCURITÉ



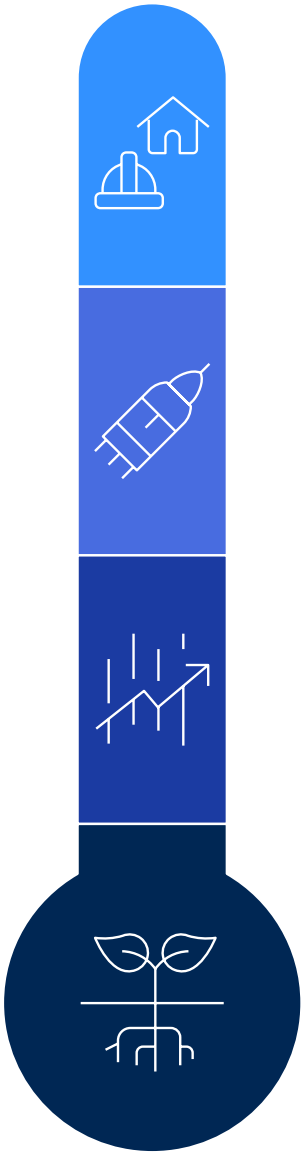
PRÉFACE

Alors que nous évoluons dans un monde de plus en plus numérique, l'importance de la cybersécurité n'a jamais été aussi grande. Compte tenu du fait que les entreprises s'appuient fortement sur la technologie, l'étendue des menaces s'est élargie, ce qui rend cruciale la protection des entreprises contre les cyberattaques. Dans le domaine de la gestion de risques, les organisations peuvent choisir d'atténuer, d'éviter, d'accepter ou de transférer un risque. La cyberassurance fait partie de l'option de transfert, servant de filet de sécurité pour les organisations faisant face aux répercussions financières des cybermenaces.

La multiplication des cyberincidents ces dernières années a mis en évidence la nécessité d'une cyberassurance. Pour 2025, Munich Re prévoit que le marché mondial de la cyberassurance atteindra 16,3 milliards de dollars, avec un paysage de cyberrisques divisé en quatre menaces majeures : les rançongiciels (record de paiement de 75 millions de dollars), les escroqueries (55 milliards de dollars de pertes en dix ans), l'attaque des chaînes d'approvisionnement (coût prévu de 60 milliards de dollars pour 2025) et les violations de données (4,88 millions de dollars de pertes en moyenne et 5,5 milliards de comptes compromis). Ces attaques ont montré l'impact financier et opérationnel dévastateur des cybermenaces dans le monde entier. En outre, l'évolution des exigences réglementaires, avec le Règlement général sur la protection des données (RGPD) et Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), la Loi 25 et la CCPA, a rendu impératif pour les organisations de disposer d'une couverture adéquate afin d'éviter de lourdes amendes et des répercussions juridiques.

QU'EST-CE QUE LA CYBERASSURANCE?

Alors que les cybermenaces continuent de croître en fréquence et en sophistication, il est devenu essentiel pour les professionnels de l'assurance de comprendre les nuances de la couverture cyber. Dans les pages qui suivent, nous explorerons l'évolution de la cyberassurance, les principales protections, les processus de souscription et la dynamique du marché propre au contexte canadien.



Présent

La cyberassurance est désormais un produit courant pour les organisations de toutes tailles. Les gouvernements et les organismes de réglementation soulignent son rôle dans la gestion de risques face à la montée des menaces. Le marché canadien continue de mûrir, avec davantage d'assureurs et de capacité, mais aussi avec une souscription plus prudente.

Essor de 2015–2023 (Canada)

L'intensification des cybermenaces a entraîné une croissance exponentielle. Les primes de cyberassurance au Canada ont bondi de 18 millions de dollars en 2015 à 550 millions de dollars en 2023. Cependant, les pertes ont dépassé les primes : les assureurs canadiens ont enregistré un ratio combiné moyen de 153 % entre 2019 et 2023, ce qui a conduit à un resserrement de la souscription et à une hausse des taux.

Croissance dans les années 2000

À mesure que les entreprises se transformaient au numérique, les assureurs ont élargi leurs couvertures pour tenir compte des violations de données et des incidents liés à la sécurité des réseaux. Au début des années 2010, la demande a rapidement augmenté à la suite de violations très médiatisées. Le marché mondial de la cyberassurance a atteint environ 1 milliard de dollars de primes en 2013.

Origines (années 1990)

La cyberassurance est apparue à la fin des années 1990. En 1997, AIG a lancé la première police d'assurance responsabilité civile sécurité internet, marquant ainsi le lancement d'une couverture spécifique aux cyberrisques. Les premières polices étaient limitées et souvent associées à une couverture responsabilité civile professionnelle pour les technologies ou à une couverture responsabilité civile pour les médias.

Évolution de la cyberassurance : d'un produit de niche à un produit courant

QU'EST-CE QUE LA POLICE DE CYBERASSURANCE?

La cyberassurance est une police d'assurance spécialisée conçue pour aider les organisations à atténuer les risques financiers associés aux cybers incidents. Les polices de cyberassurance modernes sont généralement divisées en plusieurs contrats d'assurance correspondant à différents domaines de couverture. Les polices regroupent souvent ces derniers en deux sections : couverture de l'assuré et couverture des tiers. La première partie couvre les pertes subies par l'assuré, tandis que la deuxième couvre les responsabilités envers les tiers. Les domaines de couverture les plus courants comprennent les violations de données, les attaques par des rançongiciels, les pertes d'exploitation, la cyber extorsion et les frais juridiques liés au respect des réglementations (Loi 25 au Québec, LPRPDE, etc.).

1. Définitions

Il s'agit généralement de la première section de la police. Elle définit les conditions qui déterminent les événements déclencheurs et l'étendue de la couverture. Les définitions clés sont les suivantes : assuré, événement cyber, violation des données ou de la confidentialité, défaillance ou panne du système, tiers, pertes d'exploitation et extorsion.

2. Nature et étendue de l'assurance

Cette section décrit ce que couvre la police d'assurance. Les principales couvertures que l'on trouve dans une police de cyberassurance sont détaillées à la page suivante.

3. Exclusions

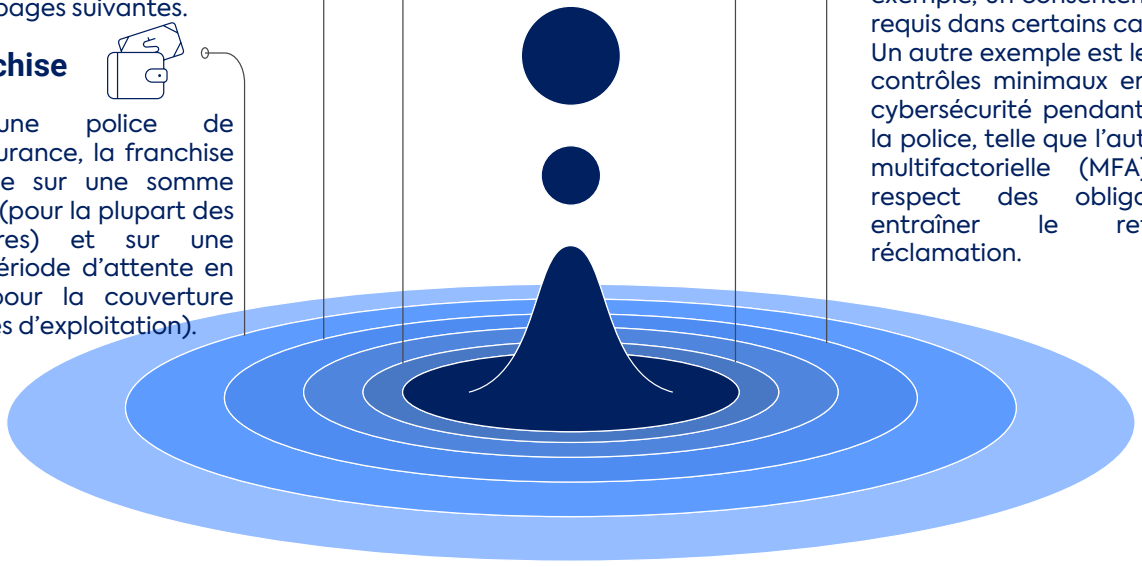
Cette section énumère ce qui n'est pas couvert par la police d'assurance. Les principales exclusions que l'on peut trouver dans une police de cyberassurance sont détaillées dans les pages suivantes.

4. Modalités

Cette section précise les exigences, les obligations préventives et les devoirs du titulaire de la police. Par exemple, un consentement écrit est requis dans certains cas spécifiques. Un autre exemple est le maintien de contrôles minimaux en matière de cybersécurité pendant la durée de la police, telle que l'authentification multifactorielle (MFA). Le non-respect des obligations peut entraîner le refus d'une réclamation.

5. Franchise

Dans une police de cyberassurance, la franchise est basée sur une somme d'argent (pour la plupart des couvertures) et sur une durée (période d'attente en heures pour la couverture des pertes d'exploitation).



Anatomie d'une police de cyberassurance

COUVERTURES CYBER PRINCIPALES

Couverture de l'assuré

Protège les intérêts et les actifs du titulaire de la police

Frais liés à une violation
Couvre les frais engagés par l'assuré pour répondre à une violation des données, y compris l'enquête judiciaire, la notification des clients, la surveillance du crédit, les relations publiques et les conseils juridiques/réglementaires. La plupart des fournisseurs proposant ces services peuvent être sélectionnés parmi un panel défini par l'assureur.

Pertes d'exploitation
Couvre la perte de revenus de l'assuré due à une panne de réseau ou de système causée par un cyberévénement. Les polices couvrent les attaques directes et les pertes d'exploitation contingentes (pannes chez des fournisseurs informatiques tiers).

Rançongiciels
Couvre les incidents liés aux rançongiciels et à l'extorsion, ainsi que le paiement des demandes de rançon et les frais de négociation et d'assistance d'experts associés.

Restauration des actifs numériques et des systèmes
Couvre les coûts de restauration ou de remplacement des données, des logiciels et des systèmes endommagés par une cyberattaque. Cela comprend le coût de la récupération des données à partir de sauvegardes et de la réparation des logiciels. Certaines polices couvrent le « bricking », c'est-à-dire le fait que le matériel informatique soit rendu inutilisable par un logiciel malveillant.

** Crime électronique*
Certaines polices couvrent l'ingénierie sociale et la fraude par transfert de fonds.

Couverture des tiers

Protège contre les réclamations faites par des tiers en raison des actions de du titulaire de la police.

Responsabilité civile liée à la sécurité des réseaux
Garantie responsabilité civile pour les réclamations découlant d'une défaillance de la sécurité des réseaux de l'assuré. Cela comprend les poursuites intentées par des clients ou des partenaires qui allèguent que la cybersécurité inadéquate de l'assuré leur a causé un préjudice.

Procédures réglementaires
Couvre les amendes et pénalités réglementaires (PCI, LPRPDE, Loi 25, RGPD, etc.) lorsqu'elles sont assurables en vertu de la loi.

Responsabilité civile pour les médias
Couverture pour les risques liés aux médias en ligne et au contenu. Protège contre la diffamation, la violation du droit d'auteur ou de la marque déposée, ou les dommages corporels résultant de publications numériques.

Responsabilité civile professionnelle pour les technologies
Pour les entreprises de technologie ou celles qui fournissent des services technologiques, les polices de cyberassurance incluent souvent une garantie responsabilité civile professionnelle pour les technologies. Elle couvre la responsabilité civile pour les défaillances de produits ou services technologiques qui causent des pertes aux clients.

EXCLUSIONS CYBER PRINCIPALES



Guerre et cyberguerre
Presque toutes les polices de cyberassurance excluent les actes de guerre. Les formulations modernes excluent spécifiquement la cyberguerre (cyberattaques parrainées par un État). Cette exclusion a fait l'objet d'un examen minutieux après que des incidents tels que NotPetya ont été considérés comme des actes « hostiles/belliqueux ».



Terrorisme
De nombreuses polices de cyberassurance excluent le terrorisme, ou plus précisément le cyberterrorisme. Certaines polices limitent la couverture du cyberterrorisme, mais en général, les pertes dues au cyberterrorisme ne sont pas couvertes par la couverture standard.



Actes antérieurs/violations antérieures
Les polices de cyberassurance excluent généralement les incidents ou violations connus qui se sont produits avant la période de couverture. Cela permet d'éviter la sélection adverse (souscription d'une assurance pour une violation en cours).



Dommages corporels et dommages matériels
La cyberassurance exclut généralement les réclamations pour dommages corporels ou matériels. Ces risques sont censés être couverts par une assurance de biens ou une assurance responsabilité civile générale.



Actes commis par des initiés et fraude commise par l'assuré
Les actes délibérés et illicites commis par l'assuré (ou ses dirigeants) sont exclus. Par exemple, si un dirigeant commet intentionnellement une violation ou collabore avec des attaquants, la police ne paiera pas.



Vol de propriété intellectuelle
La couverture pour la perte de brevets/secrets commerciaux est souvent exclue ou très limitée. Il s'agit d'une lacune importante pour les entreprises qui possèdent des actifs de propriété intellectuelle de grande valeur.



Responsabilité contractuelle
Les amendes ou paiements convenus par contrat par l'assuré sont généralement exclus, sauf s'ils résultent d'une violation couverte. Cela limite la couverture des pénalités contractuelles.



Défaillance des infrastructures
Les pannes du réseau électrique ou les défaillances de l'infrastructure internet qui ne sont pas causées par un cyberévénement sont généralement exclues, car elles ne constituent pas une violation du système de l'assuré.

CONSIDÉRATIONS ADDITIONNELLES RELATIVES À LA POLICE

Les polices de cyberassurance offrent bien plus que les couvertures clés présentées ci-dessus et varient d'un assureur à l'autre. Comme pour toute autre forme de contrat, plusieurs éléments doivent être examinés et pris en considération avant de choisir la police de cyberassurance appropriée.

Couvertures/clauses spéciales

Couverture des coûts d'amélioration — certaines polices de cyberassurance offrent cette couverture pour les coûts liés à l'amélioration ou à la mise à jour de votre système informatique après un cyberincident. Elle est généralement exclue ou plafonnée à 250/500 000 $.

Couverture en cas d'arrêt volontaire — la plupart des polices (mais pas toutes) offrent cette couverture. Cette couverture de perte d'exploitation de l'assuré s'applique lorsque ce dernier arrête intentionnellement ses propres systèmes en réponse à une cybermenace potentielle ou réelle, avant que des dommages ne surviennent, afin de minimiser ou de prévenir les pertes.

Clause d'acquisition — l'acquisition d'une nouvelle filiale sera automatiquement couverte si elle représente moins d'un certain pourcentage du chiffre d'affaires annuel consolidé de l'entreprise assurée. Si la nouvelle filiale représente plus que ce seuil du chiffre d'affaires annuel consolidé, le titulaire de la police doit en informer l'assureur dans un délai de 30 à 90 jours à compter de la nouvelle acquisition.

Clause de limitation — les clauses de limitation les plus courantes dans les polices de cyberassurance sont celles qui excluent les pratiques anticoncurrentielles/commerciales de l'accord de réponse aux violations et certaines violations des données/de la sécurité (en supposant qu'il n'y ait pas de collusion de la part du groupe de contrôle).

Consentement écrit

La plupart des polices de cyberassurance exigent le consentement écrit avant que l'assuré ne prenne certaines mesures susceptibles d'entraîner le paiement d'une indemnité. Il est essentiel que les assurés identifient ces mesures. En règle générale, le consentement écrit de la compagnie d'assurance est requis pour le paiement d'une rançon ou pour la sélection d'un « breach coach » (consultant en intrusion informatique) en dehors du panel existant des assureurs.

Période de restauration (période d'indemnisation)

La couverture des pertes d'exploitation liées à la cybercriminalité n'est pas illimitée. Les assureurs limitent la durée pendant laquelle ils couvrent les pertes de revenus et les frais supplémentaires. La couverture des pertes d'exploitation prend fin lorsque les systèmes sont restaurés, et non lorsque les revenus reviennent à la normale. La période de restauration désigne la durée maximale pendant laquelle les pertes d'exploitation sont couvertes à la suite d'un cyberincident. Elle varie de 60 à 365 jours.

Frais de défense au Québec

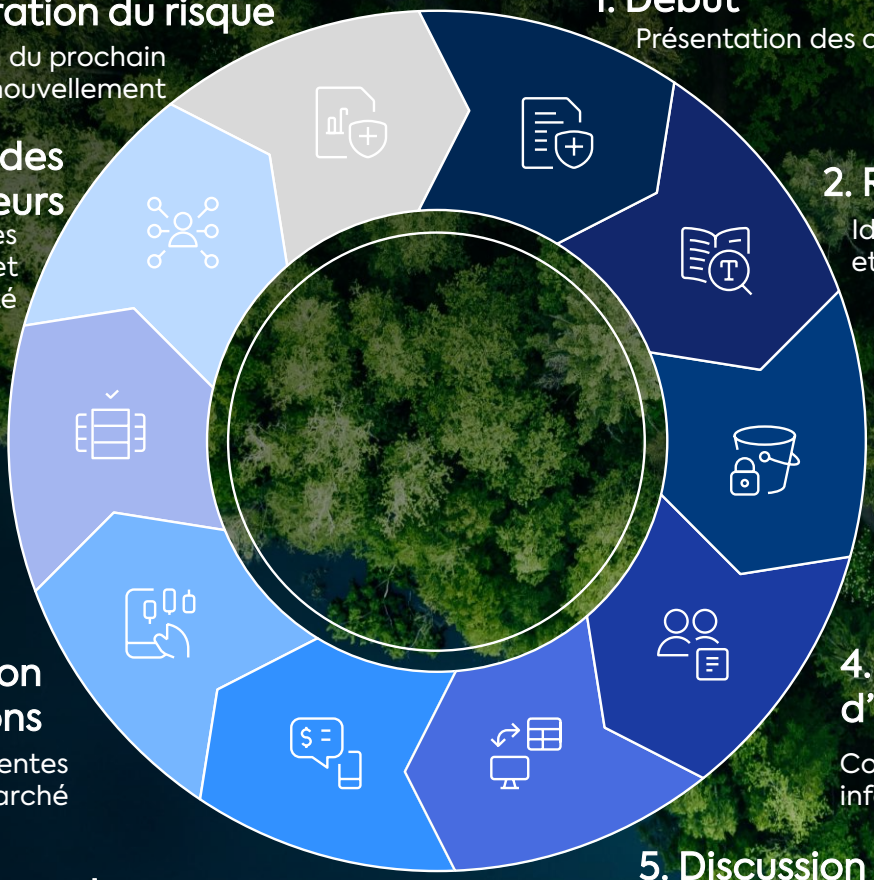
Dans une police de cyberassurance, les frais de défense sont couverts par la section responsabilité civile. Au Québec, historiquement, les frais de défense en matière d'assurance responsabilité civile sont déduits de la limite de la police et sont payés en sus, en vertu du Code civil. Il est important de vérifier si votre police de cyberassurance vous permet d'inclure les frais de défense dans la limite ou non.

Services supplémentaires liés à la cybersécurité

La plupart des polices de cyberassurance donnent accès à des services et produits de cybersécurité gratuitement ou à un taux préférentiel (analyse des surfaces d'attaque externes, simulations d'hameçonnage, rapports sur les vulnérabilités, sensibilisation des employés, simulation sur table, remises sur les EDR*, etc.). Certains assureurs offrent même un remboursement en espèces pour tout investissement visant à améliorer la posture de sécurité des assurés. *(*Endpoint Detection & Response ou Détection et la réponse des points d'accès)*

CHOISIR LA BONNE POLICE DE CYBERASSURANCE AUPRÈS DU BON ASSUREUR

Le choix d'une police d'assurance cybernétique appropriée nécessite un examen minutieux. Par conséquent, chez BFL CANADA, nos courtiers suivent un processus de souscription spécifique pour les nouveaux placements ou les renouvellements.



1. Début
Présentation des couvertures et des étapes

2. Révision technique
Identification des lacunes et faiblesses

3. Analyse du domaine public
Identification des vulnérabilités publiques

4. Demande d'assurance
Collecte des informations techniques

5. Discussion sur le placement de la cyberassurance
Discussion sur la stratégie par rapport à l'état technique

6. Négociation avec les assureurs
Négociation des modalités et conditions

7. Présentation des options
Présentation des différentes options du marché

8. Finalisation du placement
Signature des documents et facturation

9. Sélection des fournisseurs
Entretiens avec les cabinets d'avocats et entreprises de sécurité

10. Amélioration du risque
Préparation du prochain renouvellement

IMPACT DES MESURES DE CYBERSÉCURITÉ SUR LA CYBERASSURANCE

L'un des aspects les plus importants de la souscription d'une cyberassurance est de faire preuve d'une position solide en matière de cybersécurité. Les assureurs évaluent souvent les mesures de cybersécurité d'une organisation avant de lui accorder une couverture. **Les organisations qui ont donc de solides pratiques de gestion de risques, des plans d'intervention en cas d'incident et des programmes de formation des employés peuvent avoir plus de facilité à obtenir une couverture à des taux favorables.** Cela souligne l'importance d'investir dans des mesures de cybersécurité proactives non seulement pour protéger les données sensibles, mais aussi pour réduire les primes d'assurance.

IDÉES FAUSSES COURANTES SUR LA CYBERASSURANCE

Plusieurs idées fausses persistent sur la cyberassurance, malgré son importance croissante.

One common myth is that cyber insurance covers all losses associated with a cyber incident. Policies often have limitations and exclusions, which stresses the need for organizations to have comprehensive cyber security strategies alongside insurance. Another misconception is that only large companies require cyber insurance. In fact, small- and medium-sized enterprises are increasingly targeted by cybercriminals, making them equally in need of protection.

While everybody buys property insurance for tangible assets like buildings and equipment, they do not typically purchase it for non-tangible assets, such as digital data and intellectual property, which are just as vulnerable to cyber threats. This common but irrational behaviour applies to organizations as well.

En fait, selon BFL CANADA, la plus grande société canadienne privée de courtage d'assurance, seulement 25 % des entreprises canadiennes ont souscrit à une cyberassurance et moins de 1 % des particuliers souscrivent actuellement une police d'assurance personnelle contre les cyberrisques.





LE PARADOXE DU BESOIN CROISSANT DE CYBERASSURANCE

Même si nous dépendons de plus en plus de la technologie en tant qu'individus, notre sensibilisation aux risques et notre protection contre ces derniers ne sont pas au même niveau. À la maison, nous utilisons la technologie pour nos activités quotidiennes sans nécessairement être conscients de l'exposition aux cyberrisques, alors que le Canada est l'un des pays les plus connectés à l'internet dans le monde.

Par exemple, l'internet des objets (IoT), comme les téléviseurs intelligents connectés, les systèmes de caméras et la domotique (éclairage, contrôle de température, contrôle audio/vidéo, sécurité des portes, etc.), représente une porte d'entrée potentielle pour les pirates informatiques, en plus des risques découlant de l'utilisation d'ordinateurs portables, de tablettes et de téléphones cellulaires personnels.

En outre, la plupart des gens pensent qu'il n'y a pas de raison de s'inquiéter des cyberrisques en quittant le bureau parce qu'il s'agit principalement d'un risque d'entreprise.

Cependant, même si nous nous sentons plus en sécurité à la maison, le cyberrisque y est plus élevé, car en tant qu'individus, notre niveau de cybersécurité personnelle est évidemment inférieur à celui d'une organisation. Les pirates informatiques sont bien conscients de cette situation et s'attaquent de plus en plus aux particuliers. Le gain est certes moins élevé qu'avec une organisation, mais il est plus facile à réaliser. La dernière tendance en matière de piratage consiste à cibler des personnes fortunées plutôt que des personnes ordinaires ou des personnes choisies au hasard.

En outre, si les pirates informatiques parviennent à accéder aux appareils individuels connectés, ils peuvent également prendre le contrôle des appareils de l'entreprise, en établissant un pont entre les informations personnelles et celles de la compagnie, en prenant par exemple le contrôle du deuxième facteur de l'authentification multifactorielle (MFA) ou en obtenant les informations d'identification de l'utilisateur.

Par ailleurs, malgré le recours accru à l'IA, la plupart des entreprises et des employés ne comprennent pas toujours le processus qui la sous-tend. Cela peut conduire à des fuites de données et à la création de nouvelles voies potentielles pour les cyberattaques.

IMPACT DE LA CYBERASSURANCE SUR LA STRATÉGIE DE SÉCURITÉ

La cyberassurance joue un rôle essentiel dans une stratégie de cybersécurité, car elle sert à la fois de mécanisme de transfert des risques financiers et de partenaire stratégique pour renforcer la cyberrésilience d'une organisation. Il ne s'agit plus seulement de couvrir les pertes, mais aussi de permettre la prévention, la réponse et le redressement. La cyberassurance n'est pas une dépense, mais un outil budgétaire pour la maturité de la cybersécurité.

Transfert de risques pour les événements catastrophiques

Atténue de manière proactive les risques financiers liés aux cyberincidents. Sans assurance, ces coûts pourraient entraîner la faillite d'une entreprise ou perturber gravement ses activités.

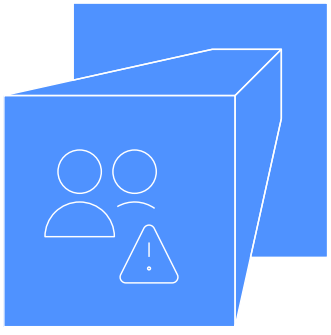


Application des pratiques exemplaires en cybersécurité

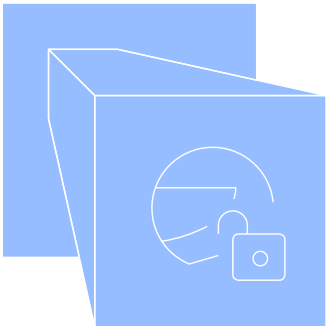


Applique des contrôles de sécurité pour prévenir de futurs incidents. La plupart des assureurs cyber exigent désormais ou encouragent l'utilisation de l'authentification multifactorielle (MFA), de la EDR, des sauvegardes de données, de la segmentation et de la PAM. Cela oblige les assurés à faire évoluer leurs contrôles, souvent en s'alignant sur les normes NIST ou ISO 27001.

Les polices comprennent généralement une assistance téléphonique disponible 24 h/24 et 7 j/7 en cas de violation, l'accès à des cabinets d'experts judiciaires de premier plan et les services d'un « breach coach » (consultant en intrusion informatique) à des taux négociés à l'avance. Cela accélère la maîtrise et le redressement, ce qui est essentiel lors d'attaques sous haute pression.

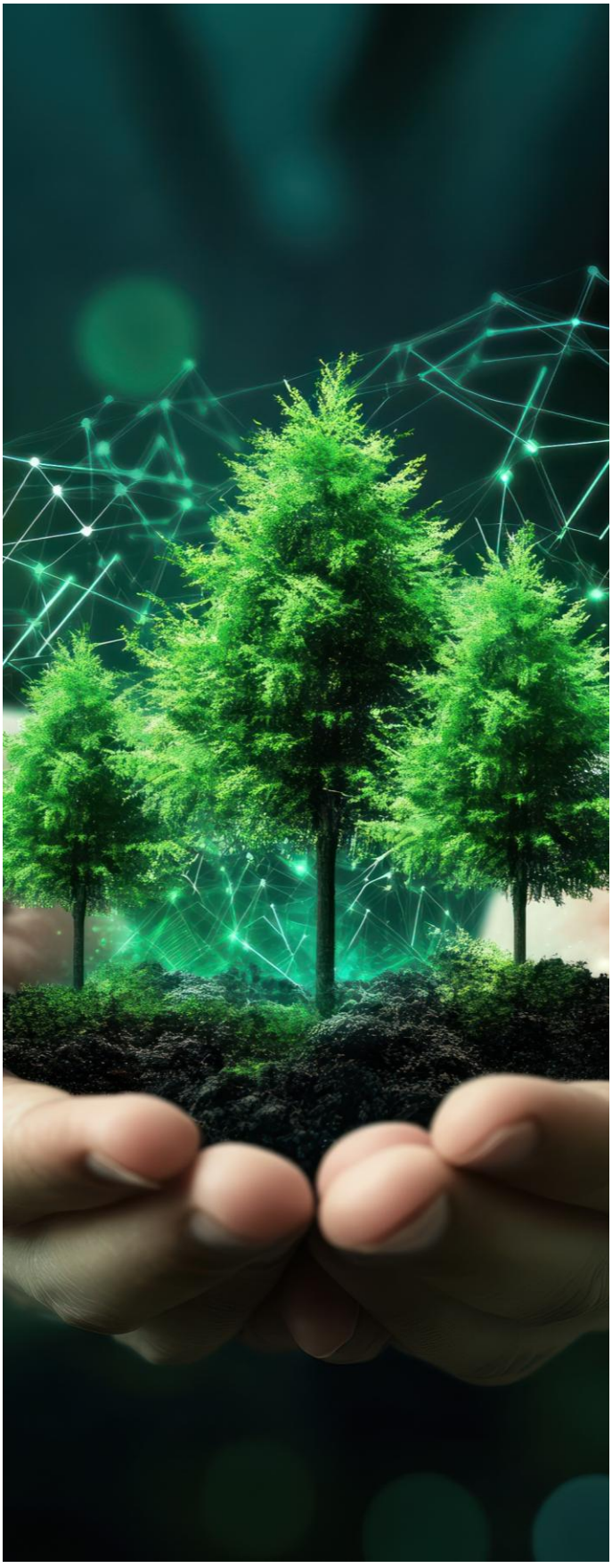


Accès à des experts en réponse aux incidents



Démontre la gouvernance des cyberrisques aux conseils d'administration et aux organismes de réglementation (p. ex., BSIF, AMF, SEC et RGPD). Requis ou recommandé dans les contrats avec les fournisseurs, les fusions et acquisitions et la diligence raisonnable relative à la chaîne d'approvisionnement.

Alignement du conseil d'administration et des réglementations



CONCLUSION

Dans un monde où les cybermenaces sont partout présentes, la cyberassurance joue un rôle crucial dans la stratégie de cybersécurité d'une organisation. Ainsi, en comprenant les complexités de la cyberassurance et l'importance de pratiques de cybersécurité solides, les organisations peuvent mieux se protéger contre l'impact financier et opérationnel des cyberincidents. Il est donc essentiel, en 2025, que les entreprises évaluent leurs cyberrisques et envisagent une couverture appropriée pour protéger leurs actifs et leur réputation.

Dans ce contexte, BFL CANADA considère l'assurance comme un service, et non simplement comme une stratégie et une dépense. Nous allons au-delà du transfert de risque, car le cyberrisque est en effet un risque d'entreprise, pas un risque informatique. Le fait de pouvoir intégrer tous les éléments de la cybersécurité dans notre offre permet à nos clients d'optimiser leurs contrats, d'éliminer le dédoublement des dépenses, d'améliorer leur posture de maturité, de quantifier leur exposition, ainsi que de rationaliser le programme d'assurance et le processus d'intervention en cas d'incident.

Restez à l'écoute : BFL CANADA publiera prochainement des articles sur d'autres sujets connexes (Impact de l'IA sur la cybersécurité, les rançongiciels, la Couverture cyber silencieuse et les tendances du marché de la cybersécurité).

RESSOURCES SUPPLÉMENTAIRES

Pour plus d'informations, vous pouvez consulter les ressources suivantes :

– National Institute of Standards and Technology (NIST) Cybersecurity Framework;

– Munich Re;

– BFL CANADA — Cyberrisques.

Si vous êtes à la recherche de conseils de professionnels en cyber sur les options de cyberassurance, vous pouvez vous adresser à un courtier agréé spécialisé dans ce domaine.

Vous pouvez contacter cyberpractice@bflcanada.ca pour plus d'informations.

Tableau 1 — Les événements liés aux cyberrisques et à la cybersécurité pouvant être couverts par une cyberassurance

Scénario d'une cyberattaque	Description de l'attaque	Couverture potentielle
Violation de données	Un pirate informatique accède sans autorisation à la base de données d'une entreprise et extrait des données sensibles sur les clients, notamment des noms, des adresses et des informations sur les cartes de crédit. L'entreprise doit informer les personnes concernées et les autorités de réglementation.	Coûts liés à la notification des personnes concernées, aux services de surveillance du crédit, aux frais juridiques et aux dépenses de relations publiques pour gérer les retombées, ainsi que les coûts liés à l'atténuation de l'attaque et la restauration des services. Frais juridiques pour se défendre contre les poursuites judiciaires.
Attaque par déni de service (DoS)	Le site Web d'une entreprise est inondé de trafic, ce qui provoque une panne et le rend indisponible pour les clients. Il en résulte une perte de revenus et une réputation ternie.	Couverture des pertes de revenus causées par les pertes d'exploitation pendant le temps d'arrêt, ainsi que les coûts liés à l'atténuation de l'attaque et la restauration des services.
Menace interne	Un employé mécontent divulgue intentionnellement des informations sensibles de l'entreprise à des concurrents ou au public, ce qui entraîne une atteinte à la réputation et une action judiciaire.	Frais juridiques pour se défendre contre les poursuites judiciaires et coûts associés aux enquêtes et aux efforts de relations publiques pour atténuer les dommages.

Tableau 1 — Les événements liés aux cyberrisques et à la cybersécurité pouvant être couverts par une cyberassurance (suite)

Scénario d'une cyberattaque	Description de l'attaque	Couverture potentielle
Infection par logiciel malveillant	Un employé télécharge à son insu un logiciel malveillant qui compromet le réseau de l'entreprise en volant des données et en se propageant éventuellement à d'autres systèmes.	Coûts liés à l'identification et à la suppression du logiciel malveillant, à la réparation du système et aux éventuels frais juridiques résultant de la perte de données. Perte d'exploitation possible.
Défaillance du réseau	Une cyberattaque exploite les vulnérabilités de l'infrastructure du réseau de l'entreprise, provoquant des pannes généralisées et entraînant une interruption de la connectivité pour les employés et les clients. L'attaque peut impliquer la manipulation de protocoles de routage ou des modifications non autorisées de la configuration du réseau.	Couverture des pertes de revenus causées par les pertes d'exploitation pendant le temps d'arrêt du réseau, coûts associés au rétablissement de la fonctionnalité du réseau et frais juridiques potentiels en cas de dégradation du service à la clientèle.
Attaque par hameçonnage	Les employés reçoivent des courriels qui semblent légitimes et qui les incitent à saisir des informations sensibles sur un site Web pastiche. Cette action compromet les informations d'identification des employés et les données des clients.	Couverture des pertes dues aux escroqueries par ingénierie sociale, les coûts associés à l'enquête et à la remédiation, et les réclamations potentielles en responsabilité civile de la part des clients concernés.
Attaque par rançongiciels (Cyberextortion)	Les fichiers d'une entreprise sont cryptés par un rançongiciel, ce qui rend des données essentielles inaccessibles. Les attaquants exigent une rançon en cryptomonnaie pour rétablir l'accès à ces fichiers. L'entreprise doit donc décider si elle veut payer la rançon ou assumer les coûts de récupération.	Couverture des pertes de revenus causées par les pertes d'exploitation, paiement de la rançon (s'il est jugé nécessaire), frais juridiques liés à la négociation avec le pirate et coûts des améliorations de la sécurité après l'incident.

Tableau 1 — Les événements liés aux cyberrisques et à la cybersécurité pouvant être couverts par une cyberassurance (suite)

Scénario d'une cyberattaque	Description de l'attaque	Couverture potentielle
Non-conformité à la réglementation	Un pirate obtient un accès non autorisé au système d'une organisation, compromettant les données sensibles des clients ou les informations personnelles soumises à des normes réglementaires spécifiques (par exemple, le RGDP, la CCPA, la Loi 25). La violation entraîne le non-respect par l'organisation des exigences de conformité en matière de confidentialité et de sécurité des données, ce qui déclenche des enquêtes réglementaires, des amendes et des pénalités.	La couverture de la conformité à la réglementation comprend les frais juridiques liés à la défense contre les enquêtes et les actions réglementaires, ainsi que la couverture des amendes et des pénalités imposées par des autorités telles que le RGDP, la CCPA ou la Loi 25. La police peut également couvrir les coûts liés à la notification des personnes concernées et à la fourniture des services nécessaires de surveillance du crédit ou de protection de l'identité. Les services de tiers, tels que les services de relations publiques et les consultants en réponse aux violations, peuvent également être couverts afin de gérer les atteintes à la réputation et de faciliter les efforts de rétablissement de la conformité.
Panne du système	Une vulnérabilité logicielle est exploitée, entraînant une panne du système qui provoque une interruption des opérations pendant plusieurs jours. L'interruption affecte le chiffre d'affaires et la confiance des clients.	Couverture des pertes de revenus causées par les pertes d'exploitation pendant le temps d'arrêt, les coûts de rétablissement du système et les éventuels frais judiciaires si les clients sont touchés.
Violation de données par un tiers	Un fournisseur de services de stockage en nuage subit une violation qui compromet les données de plusieurs clients. L'entreprise touchée doit ainsi faire face à des actions judiciaires de la part de clients dont les données ont été exposées.	Couverture de la responsabilité civile pour les actions judiciaires et les frais de notification aux clients, ainsi que les frais de remédiation et de gestion de la réputation.
Défiguration d'un site Web	A hacker gains access to a company's website and changes the content to display offensive messages. This damages the company's reputation and misleads clients.	Coûts de restauration du site Web, coûts des efforts de relations publiques pour faire face à l'incident et coûts juridiques potentiels.

CE DOCUMENT EST PRÉSENTÉ PAR :

BFL CANADA – Services-conseils en risques et de la pratique cyberrisques
2001, avenue McGill College, bureau 2200
Montréal (Québec) H1A 1G1

cyberpractice@bflcanada.ca

T. 514 843-3632
F. 514 843-3842

Sans frais : 1 800 465-2842