LES FAITS SUR
LE CYBERCRIME

Le cybercrime implique habituellement une attaque à l'infrastructure électronique d'une organisation ou l'accès non autorisé à des données dans l'intention de les voler. **Ces attaques ne sont pas seulement contraignantes et coûteuses, elles peuvent également représenter une menace existentielle pour une entreprise ou une organisation.**

Des pirates informatiques travaillent jour et nuit pour trouver de nouveaux moyens de compromettre les systèmes de sécurité des organisations, peu importe la taille de l'organisation. Des particuliers, des réseaux complexes de cybercriminels et même des gouvernements étrangers participent aux cybercrimes. **Personne n'est à l'abri de ces crimes.**

Des questions au sujet de l'assurance? Appelez-nous.

Le Bureau d'assurance du Canada
Sans frais : 1 844-227-5422

ibc.ca

@InsuranceBureau
facebook.com/insurancebureau
youtube.com/insurancebureau

Le Bureau d'assurance du Canada est l'association sectorielle nationale qui représente les sociétés privées d'assurance habitation, automobile et entreprise du Canada.

IBC BAC

10/18

ASSURANCE ENTREPRISE → PARCOUREZ IBC.CA

Quelle est la taille du problème?

Le cybercrime occasionne des problèmes considérables et coûteux.

- La cybercriminalité coûte près de **600 milliards de dollars à l'économie mondiale chaque année.**[1]
- Les cyberattaques peuvent être catastrophiques pour les entreprises. Près de **60 % des petites entreprises cessent leurs activités dans les six mois d'une cyberattaque.**[2]
- Au Canada, **le coût moyen d'une atteinte à la protection des données est de 4,7 millions de dollars.**[3]
- Chaque année, le Canada perd 0,17 % de son produit intérieur brut en raison du cybercrime, **l'équivalent de 3,12 milliards de dollars par année.**
- En 2015, **la fraude représentait 47,1 % des cybercrimes** déclarés par les services de police canadiens.[4]
- Le vol d'identité et la fraude d'identité représentaient **1,1 %** et **3,5 %** respectivement des cybercrimes en 2016.[5]
- Le **coût moyen et l'escalade des coûts des atteintes à la protection des données** au Canada, qui comprennent les activités d'enquête et d'analyse judiciaire, les services d'évaluation et d'audit, l'équipe de gestion de crise et des communications, et la surveillance du crédit, est de **1,78 million de dollars** par année.[6]

IBC BAC

[1] McAfee 2018, The Economic Impact of Cybercrime: No Slowing Down
[2] Fédération canadienne de l'entreprise indépendante
[3] Étude de l'institut Ponemon, juillet 2018, sur les pertes reliées au cybercrime
[4,5] Statistique Canada
[6] Étude de l'institut Ponemon, juillet 2018, sur le coût des atteintes à la protection des données

Comment votre entreprise ou organisation peut-elle être attaquée?

Les portes de sécurité et les chambres fortes du passé ont été remplacées par des ordinateurs protégés par des mots de passe et le cryptage. Les criminels ont évolué et trouvé de nouvelles façons de miner les organisations et d'accéder à leurs renseignements. Alors que les pirates informatiques créent sans cesse de nouvelles techniques, voici quelques moyens les plus utilisés pour attaquer les organisations.

- **Attaque par déni de service :** Surcharger un site Web en augmentant le trafic au-dessus de la capacité de traitement du serveur du site afin d'empêcher les visiteurs légitimes d'accéder au site.
- **Hameçonnage :** Un attaquant prétend représenter une organisation de confiance pour duper un utilisateur à agir, à ouvrir une pièce jointe malicieuse ou à cliquer sur un lien trompeur, par exemple, contrairement à ce qu'il ferait habituellement.
- **Logiciel malveillant :** Ce logiciel dommageable prend le contrôle d'une machine, surveille les actions et la frappe de l'utilisateur et envoie des données confidentielles d'un ordinateur ou d'un réseau infecté à la base de l'attaquant.
- **Logiciel rançonneur :** Ce logiciel chiffre les fichiers pour empêcher les utilisateurs d'y accéder et exige ensuite un paiement pour leur récupération. Ces attaques peuvent survenir après avoir cliqué sur un lien d'hameçonnage ou visité un site Web compromis. Les paiements de rançon sont habituellement dans une monnaie non retraçable, ou cryptomonnaie, comme bitcoin.
- **Arnaques :** Une fois que les cybercriminels ont accédé à un réseau, ils se font passer pour un autre utilisateur ou appareil afin d'attaquer les hôtes du réseau, de voler des renseignements, de propager des logiciels malveillants ou de contourner les contrôles d'accès.
- **Force brute :** Ce type d'attaque utilise le tâtonnement pour décoder les données chiffrées en essayant le plus grand nombre de combinaisons possibles, le plus rapidement possible. En raison des améliorations récentes dans la puissance informatique, cette tactique peut être hautement efficace.

Combien une cyberattaque peut-elle coûter à votre organisation?

Plusieurs frais peuvent être associés à une cyberattaque.

- **Frais de défense juridique :** Les dépenses engagées et les amendes civiles encourues pour les démarches réglementaires résultant d'une atteinte à la protection des renseignements personnels ou à la sécurité d'un réseau.
- **Dommages-intérêts statutaires et civils :** Comprennent les frais de représentation juridique et les dommages possibles reliés à l'atteinte à la sécurité du réseau ou à la protection des renseignements personnels.
- **Mesure corrective pour les infractions à la sécurité et frais de notification :** Les frais de notification et de gestion d'un incident relié à la protection des renseignements personnels.
- **Frais de gestion de crise :** Frais de relations publiques pour gérer les dommages à la réputation de votre société à la suite d'une atteinte à la protection des données ou d'une cyberattaque.
- **Frais d'enquête :** Pour les services d'une société d'intervention en cas d'atteinte à la protection des données.
- **Frais de restauration de programmes informatiques et de données électroniques :** Les frais de restauration ou de récupération des données endommagées ou corrompues par une atteinte, une attaque par déni de service ou un logiciel rançonneur.
- **Couverture pour extorsion liée à une menace visant le commerce électronique et les paiements :** Les montants versés à la personne ou à l'organisation qui vous ont extorqué de l'argent, à vous ou à votre société.
- **Pertes d'exploitation et frais supplémentaires :** Le revenu que votre entreprise perd et les frais qu'elle engage en raison d'une interruption de services.

Pour en savoir plus sur l'assurance contre le cyberrisque

L'assurance contre le cyberrisque est une option prudente à considérer lorsque d'autres préparations contre des cyberattaques potentielles ont échoué. **Elle peut couvrir vos pertes et votre responsabilité pour les pertes à autrui qui surviennent en raison des activités électroniques de votre entreprise.** Les contrats peuvent couvrir la responsabilité associée à la possession de renseignements personnels en format papier ou électronique.

L'assurance contre le cyberrisque peut ne pas être incluse à un contrat d'assurance entreprise ou commerciale traditionnelle et peut devoir être ajoutée comme couverture distincte. Pour comprendre les risques auxquels s'expose votre entreprise et connaître la couverture qui convient le mieux à votre entreprise, contactez votre représentant d'assurance.