ASSURANCE DES CYBERRISQUES

CONÇUE POUR VOTRE ENTREPRISE

Les cybermenaces sont en hausse, et plus de 20 % des entreprises canadiennes ont subi un incident lié à la cybersécurité[1].

Bien que ce soient les cyberattaques contre de grandes sociétés qui tendent à faire la manchette, les cybercriminels ciblent en fait des entreprises de toutes les tailles et de tous les secteurs.

Si votre entreprise est atteinte, la récupération peut être coûteuse, en temps comme en argent.

C'est pourquoi nous offrons une assurance complète contre les cyberrisques conçue pour vous protéger contre les menaces évolutives d'aujourd'hui.

EN VOICI QUELQUES EXEMPLES :

- Vous téléchargez un virus informatique qui vous empêche d'avoir accès à des données cruciales.
- Un employé perd un appareil qui contient des renseignements confidentiels.
- Une base de données essentielle est corrompue par un maliciel.
- Vous êtes victime d'une attaque par rançongiciel.

Notre police offre une protection pour les pertes

subies par l'assuré et la responsabilité civile, et elle couvre les données stockées sur votre système informatique ou celui d'un fournisseur de service – partout dans le monde.

De plus, nos services Assistance Cyberrisques peuvent vous aider à prendre des mesures préventives pour protéger vos données, et ils comprennent des services réactifs en cas d'atteinte.

Cette nouvelle solution fait partie de notre engagement à vous protéger dans notre monde de plus en plus numérique.

PLUS QU'UNE SIMPLE POLICE D'ASSURANCE

Nous avons établi un partenariat avec la société CyberScout, un chef de file de la gestion des risques liés aux données, pour offrir les services Assistance Cyberrisques à nos clients.

Inclus sans frais additionnels dans nos polices d'assurance des cyberrisques :

- Services proactifs et réactifs de renseignements sur les atteintes à la protection des données
- Ressources pour la gestion des risques
- Planification d'intervention en cas d'incident
- Soutien en matière de gestion des crises
- Assistance pour la notification
- Services de consultation sur les relations avec les médias

POURQUOI ENVISAGER D'OBTENIR L'ASSURANCE DES CYBERRISQUES?

- Les petites et moyennes entreprises comptent pour 61 % de toutes les victimes de cyberattaques[1].
- Les cyberévénements touchent des entreprises de tous les secteurs.
- Le coût moyen d'une intervention en cas de cyberatteinte est de 6,11 millions de dollars[2].
- Le temps moyen d'interruption des activités en raison d'une cyberatteinte est de 23 heures[3].
- Le non-respect des lois canadiennes concernant l'obligation de déclarer les atteintes à la vie privée et de les consigner dans un registre peut entraîner une amende pouvant s'élever à 100 000 $.

[1] Verizon, « Data Breach Investigations Report », 2017.

[2] Ponemon Institute d'IBM, « Cost of Data Breach Study », 2017.

[3] Statistique Canada, « L'incidence du cybercrime sur les entreprises canadiennes, 2017 ». Publication : 2018-10-15.

OPTIONS DE COUVERTURE

Solution standard

Notre solution standard est offerte à toute entreprise dont le revenu ne dépasse pas 15 millions de dollars, et le montant de garantie maximal est de 1 million de dollars.

Solutions sur mesure

Nous offrons des solutions sur mesure d'assurance des cyberrisques pour les entreprises dont le revenu dépasse 15 millions de dollars ou qui nécessitent des montants de garantie plus élevés.

Garantie / caractéristique	Description	Solution standard	Solution sur mesure
GARANTIES VISANT LES PERTES SUBIES PAR L'ASSURÉ			
Frais pour répondre à un incident	Frais pour gérer un incident lié à la protection des renseignements personnels et en aviser les personnes touchées, y compris les frais liés aux services de relations publiques visant à réduire l'atteinte à la réputation.	✓	✓
Frais liés aux actifs numériques	Frais pour restaurer ou récupérer des données endommagées ou corrompues par une atteinte.	✓	✓
Interruption des activités	Garantie des pertes de revenu résultant d'une interruption des services causée notamment par un maliciel ou une attaque entraînant un refus de service.	✓	✓
Frais d'extorsion liés au commerce électronique	Frais pour empêcher une menace d'extorsion de nuire aux activités de l'entreprise.	✓	✓
GARANTIES VISANT LA RESPONSABILITÉ CIVILE			
Responsabilité civile liée à la sécurité du réseau et à la protection des renseignements personnels	Garantie des incidents résultant d'un accès non autorisé ou de l'activité de fouinards. Garantie des incidents relatifs à la transmission d'un maliciel ou à la participation à une attaque entraînant un refus de service.	✓	✓
Responsabilité civile liée aux médias sur Internet	Garantie du préjudice personnel et de la violation de la propriété intellectuelle causés par la publication de contenu en ligne.	✓	✓
Frais liés aux procédures réglementaires	Frais engagés par l'entreprise et pénalités lui étant imposées dans le cadre d'une procédure réglementaire découlant d'une atteinte liée à la protection des renseignements personnels ou à la sécurité du réseau.	✓	✓
Capacité	Montant de garantie global maximal disponible.	1 000 000 $	10 000 000 $
Prime minimale		175 $	Variable
Assistance Cyberrisques	Services-conseils en matière de mesures préventives pour protéger l'entreprise ainsi que des services réactifs en cas d'atteinte à la protection des renseignements personnels.	Incluse sans frais additionnels	Incluse sans frais additionnels

EXEMPLES DE SINISTRES EN CYBERRISQUES

Employé déloyal | Plusieurs millions
Un employé a enfreint les politiques de l'entreprise : il a consulté et vendu les renseignements de milliers de clients à une entreprise de marketing tierce. Quand il a pris connaissance de la situation, l'employeur a lancé une enquête interne. Pendant ce temps, d'autres dossiers ont été consultés et vendus.

L'entreprise a engagé une agence de relations publiques pour l'appuyer dans ses communications avec les clients et le public relativement à l'incident. L'employé déloyal a été congédié, et des accusations criminelles ont été portées contre lui pour lesquelles des amendes lui ont été imposées. Un recours collectif qui pourrait atteindre des millions de dollars a été intenté contre l'entreprise par les clients touchés.

Interruption des activités | 200 000 $
Une moyenne entreprise de fabrication de pièces de métal a été victime d'une atteinte à la sécurité de son réseau. Ses systèmes informatiques et d'automatisation ont été infectés par un maliciel. Il a fallu deux jours à l'entrepreneur informatique de l'entreprise pour récupérer les données électroniques des supports de stockage corrompus, et les données n'étaient pas toutes récupérables. Même si les dernières sauvegardes de sécurité remontaient à un mois seulement, l'intégrité des données n'avait pas été vérifiée, et certaines étaient inutilisables. Quarante-huit heures supplémentaires ont été nécessaires pour réinstaller, réparer et reconfigurer les systèmes informatiques de l'entreprise avant que celle-ci puisse reprendre ses activités.

Au cours des quatre jours où ses activités ont été interrompues, l'entreprise a subi des pertes de revenu et accumulé du retard dans ses contrats. Par conséquent, ses clients ont également subi des pertes de revenu et ont pris du retard à leur tour.

Le fabricant (l'assuré) a subi une perte de 209 000 $ (4 000 $ en frais d'expertise judiciaire en informatique et en assistance connexe, 5 000 $ en frais juridiques et 200 000 $ en perte de revenu).

Attaque entraînant un refus de service | 34 000 $
Une petite entreprise de services professionnels a été victime d'une attaque entraînant un refus de service; ses systèmes informatiques ont été touchés à un point tel qu'elle a dû les mettre hors service pendant quelques jours afin d'effectuer les correctifs requis.

Une part importante des travaux consistait en des réparations logicielles, qui étaient couvertes par la police Assurance des cyberrisques. Les dommages matériels subis par le réseau, quant à eux, étaient couverts par la police d'assurance des biens.

Maliciel | 4 000 $
Pendant la fin de semaine, un maliciel a infecté le réseau informatique d'une clinique vétérinaire. Le lundi, les membres du personnel de la clinique ne pouvaient pas accéder à leur logiciel de gestion des vaccinations et des relations avec la clientèle. Ils ne pouvaient pas non plus appeler les clients pour déplacer les rendez-vous ni servir les clients.

Après une dizaine d'heures, une équipe externe a réussi à décrypter le système informatique et à déterminer qu'aucun renseignement confidentiel de la clinique n'avait été atteint ni volé.

NORTHBRIDGE ASSURANCE

Northbridge Assurance est l'une des plus importantes sociétés d'assurance des entreprises au Canada. En collaboration étroite avec nos courtiers partenaires, et en nous appuyant sur notre expertise sectorielle approfondie, nous aidons les entreprises à exercer leurs activités de façon plus sécuritaire afin qu'elles puissent se concentrer sur les occasions à saisir plutôt que sur les risques. Visitez le www.nbins.com pour en savoir plus.

3818-004-ed02F | 08.2020