Police de cyberassurance de Zurich

Sécurité, solutions, simplicité.

Une cyberattaque perturbera votre entreprise : il ne s'agit pas de savoir si cela va se produire, mais quand.

En 2017, les organisations du monde entier ont été frappées par les attaques des rançongiciels WannaCry et NotPetya. Ces deux programmes malveillants, qui ont rapidement fait le tour du globe, se sont infiltrés dans les réseaux pour détourner et verrouiller des données critiques, perturbant ainsi les processus et les chaînes logistiques, et causant des dégâts numériques totalisant des centaines de millions de dollars. Ces événements isolés se répéteront-ils? Étant donné l'environnement de cyberrisque actuel, qui est en constante mutation et qui se montre de plus en plus menaçant, cela est fort probable. Pour la plupart des organisations, il n'est pas question de savoir « si » une cyberattaque grave et potentiellement dommageable se produira, mais bien « quand » elle se produira.

Sécurité contre la menace croissante de cyberattaques coûteuses
Solutions programmées pour intervenir dans un environnement de risque en constante évolution
Simplicité de protection contre les risques grâce à un programme pratique

Selon l'étude de 2018 sur le coût des brèches de données *(2018 Cost of Data Breach Study: Global Overview)* commanditée par Sécurité IBM et menée par le Ponemon Institute, le coût total moyen d'une atteinte à la protection des données s'élève maintenant à 3,86 millions de dollars de dollars américains, une augmentation de 6,4 % par rapport à l'étude de 2017[1]. Selon cette même étude, on estime désormais que le coût moyen par dossier perdu ou volé revient à 148 $. Multipliez ce coût par le nombre de dossiers que votre organisation pourrait perdre si elle était frappée par une grave attaque entraînant une brèche et un vol de données. Même les attaques moins importantes que celles des fameux rançongiciels de 2017 peuvent endommager votre réseau, vos activités et votre réputation. Comment quantifier l'impact à long terme sur la confiance des clients?

Une solution unique et pratique pour vous aider à vous protéger contre les cyberrisques

La police de cyberassurance de Zurich peut vous aider à vous protéger contre les risques d'une grave atteinte à la protection des données. Le programme regroupe des caractéristiques souvent associées à d'autres polices d'assurance des entreprises sous forme d'avenants individuels dans une solution unique et pratique, qui peut être adaptée aux besoins particuliers de votre organisation.

Garanties et avantages clés

Garanties de responsabilité civile

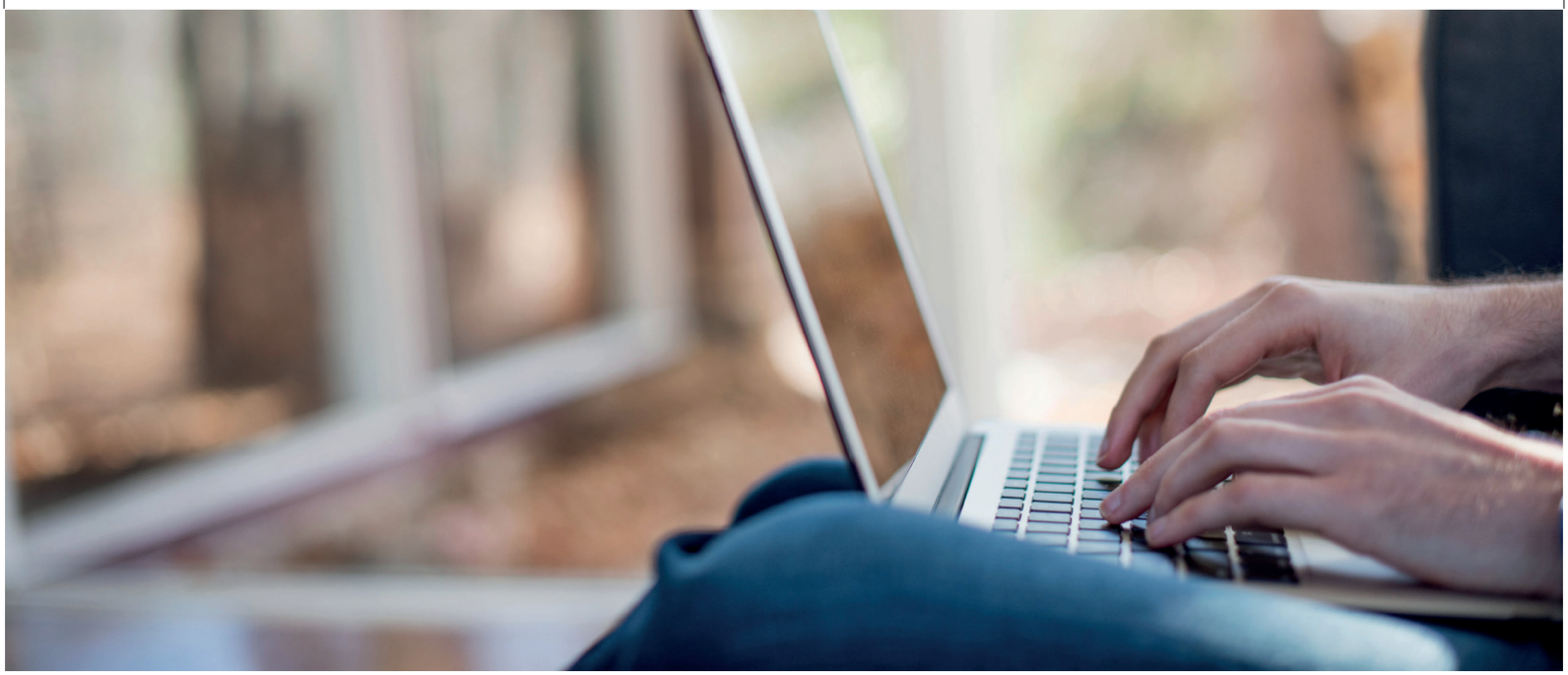
- Responsabilité civile liée à la sécurité et à l'atteinte à la vie privée
- Frais de défense pour les procédures réglementaires
- Amendes et pénalités civiles associées à l'industrie des cartes de paiement et au Règlement général sur la protection des données (RGPD)
- Garantie de responsabilité civile liée aux médias

Garanties autres que la responsabilité civile

- Frais liés aux atteintes à la vie privée, y compris:
  - Frais d'enquête judiciaire
  - Frais de justice et de relations publiques
  - Frais de surveillance du crédit et de l'identité
  - Frais d'assurance contre le vol d'identité et de restauration de l'identité
  - Frais de centre d'appels
- Perte de revenu d'entreprise, perte de revenu d'entreprise découlant de la défaillance de tiers indispensables (perte de revenu à cause d'un événement menaçant la sécurité du réseau d'un fournisseur) et dépenses supplémentaires
- Frais liés au remplacement de biens numériques
- Paiements des récompenses et menaces de cyberextorsion
- Défaillance de système et défaillance de système d'un tiers indispensable
- Atteintes à la réputation
- Transfert de fonds en cas de piratage psychologique
- Protection de prévention des demandes de règlement

Autres faits saillants de la police

- Limites de garantie pouvant aller jusqu'à 25 millions de dollars américains
- Garantie d'interruption des affaires déclenchée en cas d'atteinte à la protection des données nécessitant un arrêt volontaire des activités
- Garantie possiblement également déclenchée en cas de défaillance de système et d'erreurs administratives
- Protection pour la collecte de données non autorisée
- Possibilité de protection relativement au Règlement général sur la protection des données (RGPD) de l'Europe
- Définition de « personne assurée » étendue pour inclure les employés temporaires, les bénévoles et les stagiaires
- Définition de « dépenses supplémentaires » modifiée pour inclure les frais d'enquête judiciaire
- Définition large de « système informatique », comprenant les systèmes de commande industriels et les programmes « apportez votre équipement personnel de communication »
- Pas de restrictions relativement aux fournisseurs – vous pouvez demander l'assistance des fournisseurs de votre choix à la suite d'une brèche
- Demande simplifiée et claire fondée sur le cadre du National Institute of Standards and Technology (NIST), un organisme non réglementaire du département du Commerce américain



Services spécialisés en cyberrisque

En souscrivant une police de cyberassurance de Zurich, votre organisation bénéficiera d'une consultation initiale gratuite avec un professionnel chevronné spécialisé en cyberrisque de Zurich. L'objectif est de vous aider à cerner les risques potentiels et de vous aider à établir un plan de restauration efficace.

Moyennant certains frais, les professionnels spécialisés en cyberrisque de Zurich peuvent aussi vous aider à élaborer et à entretenir de façon continue un rigoureux système de gestion de la sécurité de l'information basé sur trois piliers essentiels : les employés, les processus et la technologie.

Employés

- Éducation du conseil d'administration et des cadres supérieurs
- Formation visant à accroître la sensibilisation des utilisateurs, notamment sur l'hameçonnage, le piratage psychologique, les normes et la gestion des mots de passe et les courriels d'affaires compromis
- Formation de l'équipe de sécurité
- Directives sur la sécurité des pratiques d'embauche
- Gestion de l'accès (utilisateurs, fournisseurs, utilisateurs privilégiés et utilisateurs à distance)

Processus

- Stratégie de cybersécurité
- Feuille de route des capacités
- Élaboration de politiques et de procédures, y compris, mais sans s'y limiter, sur l'utilisation acceptable, la gestion d'actifs, la gestion de la vulnérabilité et des correctifs, l'évaluation des risques, la gestion des fournisseurs, la réponse aux incidents et la reprise après sinistre
- Mesures de gestion pour la cybersécurité

Technologie

- Recommandations pour une gamme de solutions technologiques spécialisées auprès de fournisseurs et de consultants en sécurité externes chefs de file dans leur domaine

Contrôle du réseau 24 heures sur 24, 7 jours sur 7

Service optionnel offert aux organisations qui souscrivent la police de cyberassurance de Zurich

En association avec un fournisseur de services de sécurité (MSSP) de premier plan, Zurich peut offrir les services ci-dessous aux clients qui le demandent en les incluant dans la prime d'assurance.

- Une évaluation technique gratuite de l'ensemble de votre réseau et des périphériques qui y sont connectés
- Une surveillance en temps réel, 24 heures sur 24 et 7 jours sur 7, des périphériques connectés sur votre réseau (jusqu'à concurrence de 50), comme les serveurs, les stations de travail, les pare-feu et les autres dispositifs de consignation
- Sur une base hebdomadaire, une analyse complète de la vulnérabilité de tous les périphériques précisés dans votre convention d'assurance, y compris des rapports d'état complet et des recommandations de correctifs pour atténuer les vulnérabilités révélées
- La possibilité d'effectuer la surveillance de plus de 50 périphériques, moyennant certains frais

Services spécialisés en cyberrisque

Si un cyberincident se produit, vous aurez droit à l'assistance d'une équipe de spécialistes en cyberrisque chevronnés qui comprennent les enjeux et qui savent comment vous aider à atténuer les impacts d'un tel incident aussi rapidement et efficacement que possible. Les spécialistes en cyberrisque de Zurich sont des avocats qualifiés et expérimentés qui comprennent les dimensions uniques des cyberincidents, de même que les services et les stratégies permettant de les gérer.

Renseignements supplémentaires

Pour obtenir de plus amples renseignements sur la police de cyberassurance de Zurich, communiquez avec votre courtier ou :
Service des risques
416 586-2740
riskservices@zurich.com

1. Ponemon Institute. Étude de 2018 sur le coût des brèches de données (2018 Cost of Data Breach Study: Global Overview.) Commanditée par Sécurité IBM. 11 juillet 2018. https://www.ibm.com/Security/Data-Breach

Zurich Canada
First Canadian Place
100, rue King Ouest
Bureau 5500, C.P. 290
Toronto (Ontario) M5X 1C9

www.zurichcanada.com
1 800 387-5454

A1-112011497-A (10/18) 112011497

ZURICH®