Scénarios de réclamations en matière de cyberrisques

Voici des exemples de scénarios de réclamations récentes pour vous donner une idée de nos capacités :

Accès non autorisé

Secteur	Services professionnels
Entreprise	Commercial
Différence dans l'expérience de réclamation	Expert-conseil en intervention et cabinet de services d'informatique judiciaire de premier ordre
Description	Notre assuré est une organisation professionnelle qui dispose d'un portail en ligne permettant à ses membres d'accéder aux données. L'organisation a connu un incident de sécurité et ses représentants ont remarqué que dans plusieurs cas, les renseignements d'inscription des membres étaient incorrects et les données avaient été altérées. Les services d'un expert-conseil en intervention en cas d'incident et d'un cabinet de services d'informatique judiciaire de notre groupe d'experts en cyberrisques ont été retenus et il a été déterminé qu'un accès non autorisé s'était produit sur l'un de ses serveurs ayant un portail Web externe. Le cabinet de services d'informatique judiciaire n'a trouvé aucune preuve que des renseignements personnellement identifiables avaient été divulgués lors de l'attaque, et les données de la base de données de l'assuré n'étaient pas sensibles. Chubb a payé environ 100 000 $ CA en frais de risques propres à la suite de cet incident.

Attaques par rançongiciel

Secteur	Services professionnels
Entreprise	Commercial
Différence dans l'expérience de réclamation	Expert-conseil en intervention et cabinet de services d'informatique judiciaire de premier ordre
Description	Une entreprise de services professionnels a subi une attaque par rançongiciel qui a crypté plusieurs fichiers de ses serveurs. Une rançon de 10 000 $ environ a été exigée initialement. Nous avons été rapidement informés de l'incident par l'entremise de notre ligne d'assistance en cas de cyberincident, et les services d'un expert-conseil en intervention en cas de cyberincidents et ceux d'un cabinet de services d'informatique judiciaire spécialisé dans les rançongiciels ont été retenus par notre groupe d'experts en cyberrisques. Après avoir consulté ces experts, l'assuré a décidé de payer la rançon. Dès le paiement de la rançon, l'assuré a pu entamer le processus de décryptage. À la suite d'une enquête menée par le cabinet de services d'informatique judiciaire, il a été déterminé qu'aucun renseignement personnel identifiable n'avait été compromis à la suite de l'attaque. Cette attaque par rançongiciel a entraîné pour l'assuré des pertes d'environ 100 000 $, dont 15 000 $ pour l'expert-conseil en intervention en cas de cyberincident, 75 000 $ pour le cabinet de services d'informatique judiciaire et 10 000 $ pour le paiement de la rançon.

CHUBB®

Courriels d'hameçonnage

Secteur	Services financiers
Entreprise	Commercial
Différence dans l'expérience de réclamation	Enquête d'expert sur les réclamations
Description	Les employés d'une entreprise de services financiers de taille moyenne ont été victimes d'une attaque d'hameçonnage massive en cliquant sur un lien permettant à des personnes malveillantes d'obtenir des renseignements d'identification du système et d'accéder à des comptes de courriel. Environ 100 comptes de courriel ont été compromis et les personnes malveillantes ont défini une règle qui transférait les nouveaux courriels vers une adresse de courriel non autorisée. De nombreux comptes de courriel contenaient les noms et numéros d'assurance sociale de clients de l'assuré. Les services d'un expert-conseil en intervention en cas de cyberincident et d'un cabinet de services d'informatique judiciaire qui s'occupe fréquemment de ce type d'escroquerie par hameçonnage ont été retenus par notre groupe d'experts en cyberrisques. Après avoir utilisé des outils spécialisés pour déterminer quels comptes de courriels étaient touchés, le cabinet de services d'informatique judiciaire a conclu que plusieurs millions de documents devaient être examinés pour déterminer la nature et l'étendue des personnes touchées. De plus, les personnes malveillantes avaient accédé aux autres systèmes de l'assuré et effectué plusieurs virements électroniques frauduleux. Il a finalement été déterminé que 200 000 personnes devaient être informées de l'incident et qu'elles devaient bénéficier d'une surveillance du crédit pendant deux ans. Les sinistres totaux applicables aux garanties couvrant l'assuré s'élevaient à environ 3,5 millions de dollars, répartis comme suit : 2 millions de dollars pour le cabinet de services d'informatique judiciaire, 1 million de dollars pour l'expert-conseil en intervention en cas de cyberrisques et 500 000 $ de frais de surveillance du crédit et de centre d'appels.

Fournisseur et chaîne d'approvisionnement

Secteur	Soins de santé
Entreprise	Commercial
Différence dans l'expérience de réclamation	Expertise technique
Description	Un associé de l'assuré a été victime d'une attaque par rançongiciel pendant laquelle plusieurs de ses fichiers ont été cryptés. L'associé avait en sa possession les dossiers médicaux et les renseignements personnels sur la santé des clients de l'assuré et a dû retenir les services d'un expert-conseil en intervention en cas de cyberincident et d'un cabinet de services d'informatique judiciaire pour remédier à l'attaque par rançongiciel sur son système. Même si notre assuré avait déjà utilisé les services de conseils préalables aux incidents de Chubb pour mieux se préparer à une cyberattaque, il a dû néanmoins consulter son propre expert-conseil en intervention en cas de cyberincident de notre groupe d'experts en cyberrisques pour déterminer ses obligations de déclaration en vertu de la *Health Insurance Portability and Accountability Act* (HIPAA). L'expert-conseil en intervention en cas de cyberincident a finalement déterminé que personne n'avait extrait de renseignements personnels sur la santé du système de l'associé. En raison de cet incident, l'assuré a déboursé 20 000 $ en frais de risques propres.

Vous souhaitez vendre des produits Chubb?

Visitez notre site Web pour plus de renseignements sur les solutions d'assurance de Chubb.