RÉCLAMATIONS EN MATIÈRE DE CYBERRISQUES

L'assurance contre les cyberrisques fournit une couverture pour les pertes subies par un assuré (première partie) et pour les pertes de tiers (responsabilité civile) associées à la violation de réseaux de sécurité ou à la perte, au vol ou à la divulgation non autorisée de données personnelles identifiables ou à la perte relative aux renseignements confidentiels d'une entreprise. Cette couverture peut comprendre des dépenses associées à la notification en cas de violation de la sécurité, associées à des menaces d'extorsion, aux relations publiques, à la surveillance du crédit, aux enquêtes médico-légales, aux frais de défense ainsi qu'aux frais reliés à des décisions ou à des règlements judiciaires.

Toute entreprise, quelle que soit sa taille ou son secteur d'activité, est confrontée à des risques et doit être protégée en conséquence. Ces risques peuvent se présenter sous diverses formes, dont les suivantes : renseignements personnels sur les employés ou les clients, accès Internet, communications électroniques et activités de réseau, de même que l'utilisation de la technologie dans son ensemble.

L'affaire de l'ordinateur portable manquant

Une employée travaillant pour un petit cabinet comptable a emprunté l'ordinateur portable du bureau pour travailler chez elle au cours d'un week-end. Cependant, un arrêt à un centre commercial a provoqué un incident malencontreux. Sa vitre d'automobile a été fracassée et une personne s'est emparée de l'ordinateur qui contenait les dossiers personnels de plus de 120 000 personnes. Son cabinet avait conseillé plusieurs grands hôpitaux relativement à leurs audits comptables et les renseignements personnels sur la santé (RPS, ce qui comprenait des ordonnances médicales, des procédures et des codes diagnostiques) de leurs patients étaient maintenant à la merci des voleurs. Il suffisait d'un simple mot de passe pour y accéder. Notre équipe d'intervention a été en mesure de conseiller le cabinet sur la façon de notifier chaque hôpital et ensuite chaque patient. Le cabinet a pu subséquemment continuer à exercer ses activités.

Renseignements personnels sur des employés affichés sur le site Web d'une entreprise

Une société ouverte s'est ouverte un peu plus que souhaité quand elle a involontairement affiché en ligne des renseignements personnels concernant plusieurs cadres supérieurs de l'entreprise. Les numéros d'assurance sociale des principaux dirigeants de l'entreprise étaient accessibles à quiconque visitait son site Web pour une période de quatre à six semaines. Le service juridique interne de l'entreprise communiqua avec le panel d'experts de Trisura au sujet de cette violation. Ces experts ont formulé deux principales recommandations : faire enquête sur les blogues des visiteurs qui étaient en ligne durant cette période et tenter de déterminer si les moteurs de recherche avaient répertorié ces renseignements. Il a été conclu que le niveau de violation était minimal. Les moteurs de recherche n'avaient pas répertorié ces informations qui étaient, du reste, hébergées dans une section du site qui faisait l'objet de très peu de visites. Cependant, en raison du niveau hiérarchique élevé des dirigeants, plusieurs mesures ont été conseillées et prises : l'entreprise a ainsi mis en place un système d'alerte à la fraude sur tous les comptes bancaires; elle a également mené une revue des activités en ce qui a trait au dossier de crédit; et elle a enfin placé toutes les personnes concernées au plus haut niveau de surveillance du crédit et des fraudes.

Une bévue des TI mène à une violation

Quand un service de police a mis à jour ses bases de données, des renseignements essentiels ont été enregistrés sur un serveur standard et non-sécurisé. Les renseignements personnels sur plus de 200 000 officiers, prisonniers et informateurs ont donc été accessibles durant une période de huit mois en raison de cette erreur commise par les TI, et ce, jusqu'à ce qu'une personne ait exprimée sa préoccupation de voir des données personnelles apparaître sur les moteurs de recherche. Le service de police prit contact avec le panel d'experts de Trisura pour déterminer s'il devait envisager de procéder à une évaluation des risques de fraude. L'équipe d'experts a alors pris en considération plusieurs facteurs, notamment le grand nombre de personnes exposées à cette fraude potentielle et la possibilité de poursuites contre le service de police. Ce dernier décida de donner suite à des préoccupations spécifiques en matière de sécurité plutôt que de lancer une campagne axée sur la protection du consommateur. D'ailleurs, une surveillance étroite et une résolution de la fraude potentielle furent considérées comme des options impossibles à appliquer.

Le mauvais bordereau de carte de crédit

Un petit commerçant en ligne s'apprêtait à transférer ses données et son site Web remanié sur un nouvel hébergeur quand l'ancien site Web a été piraté. Les voleurs potentiels ont réussi à avoir accès à près de 30 000 numéros de cartes de crédit remontant à près de cinq ans. Même s'il est illégal de conserver de telles données si longtemps après une transaction, le commerçant devait néanmoins informer ses clients de cette violation de données. L'équipe d'intervention en cette matière a suggéré au commerçant de filtrer tous les numéros de cartes de crédit encore actifs, ce qui a réduit le nombre de victimes de cette violation de données à 12 000.

Par la suite, l'équipe d'intervention a travaillé avec le conseiller juridique du commerçant pour déterminer s'il était à-propos d'informer le groupe touché de cette situation (c'était le cas). L'équipe a également fourni une lettre de notification et un gabarit de foire aux questions, de même que l'accès à notre équipe d'intervention composée d'experts en matière de cyberrisques afin de donner aux clients les conseils dont ils avaient besoin pour mieux se protéger. De plus, l'équipe d'intervention a aidé le commerçant à se préparer adéquatement pour le litige qu'il allait entreprendre contre l'hébergeur qui avait causé cette violation initialement.

Vol des données personnelles de titulaires de polices

Un agent d'assurance a quitté une compagnie d'assurance pour se joindre à une autre. En partant, il a utilisé les justificatifs d'accès d'un ancien collègue pour voler les données personnelles de milliers de clients. Par la suite, il a appelé ces clients et leur a proposé des soumissions à de meilleurs tarifs pour leur assurance habitation, santé et automobile. L'équipe d'intervention en matière de cyberrisques de Trisura est intervenue pour gérer la situation après que la compagnie d'assurance où travaillait cette personne ait intenté des procédures criminelles et civiles à l'encontre de cet ancien employé. Quel était le risque évalué pour ces titulaires de polices dont les renseignements personnels avaient été volés ? Pas très élevé et assurément pas aussi élevé pour justifier l'intervention des tribunaux et des organismes de réglementation. L'équipe d'intervention a alors conseillé la compagnie sur la façon de contrôler cette violation, car la menace était faible, et de recouvrer les coûts à titre de dommages-intérêts dans le cadre de la poursuite au civil intentée contre l'ancien agent d'assurance.

Des demandes de prêt hypothécaire disparaissent

Une coopérative d'épargne et de crédit a demandé conseil après qu'un fournisseur tiers ait égaré un certain nombre de demandes de prêt hypothécaire fermées. La coopérative était légalement tenue de conserver les demandes de prêt hypothécaire fermées. Elle a alors retenu les services d'un fournisseur de solutions de stockage qui a signalé qu'une boîte contenant 14 demandes de prêt hypothécaire fermées était manquante. Le fournisseur a passé son installation au peigne fin, mais n'a rien trouvé. L'équipe d'intervention en matière de cyberrisques de Trisura a alors collaboré avec l'avocat général de la coopérative afin de rédiger une lettre informant les consommateurs touchés sans créer de panique. L'équipe a ensuite aidé les personnes touchées par cette situation à s'inscrire à des services qui avaient pour but d'assurer que leurs renseignements personnels ne seraient pas utilisés à mauvais escient. Le fournisseur de solutions de stockage s'est également impliqué en payant toutes les dépenses associées à l'avis de notification et au processus de surveillance que cette situation a engendrée.

Un photocopieur précédemment loué mène à une violation

Une organisation médiatique a acheté un photocopieur qui avait précédemment été loué à une compagnie d'assurance. Le reporter d'enquête du groupe médiatique a découvert que le disque dur interne du photocopieur contenait toujours tous les renseignements qui avaient été copiés par la compagnie d'assurance. Le journaliste a donc communiqué avec l'assureur parce qu'il préparait un reportage sur les risques posés par les photocopieurs relativement à la protection de renseignements personnels sensibles. L'équipe d'intervention en matière de cyberrisques de Trisura a collaboré avec la compagnie d'assurance cliente afin de déterminer la nature des renseignements qui avaient fait l'objet de cette fuite et de préparer un gabarit de lettre de notification. Notre équipe a référé le client à un cabinet de relations publiques spécialisé dans la tenue d'entrevues télévisées pour des fins de reportages. Le reportage qui s'ensuivit était empreint de respect, n'a pas cherché à cibler ou à attaquer le client, et les organismes de réglementation concernés ont décidé de n'entreprendre aucun recours judiciaire sur la base des faits présentés dans ce reportage.

À propos de Trisura

La **Compagnie d'assurance Trisura Garantie** est une compagnie canadienne d'assurance spécialisée et de cautionnement. Par l'intermédiaire d'un réseau choisi de cabinets de courtage régionaux et nationaux, Trisura Garantie procure une expertise et des solutions innovantes en matière de cautionnement de contrat, de cautionnement commercial, de cautionnement pour promoteurs immobiliers, de responsabilité des administrateurs et dirigeants, d'assurance contre les détournements, de responsabilité professionnelle – y compris la responsabilité des médias et la responsabilité liée aux technologies et aux cyberrisques – d'assurance des biens et de la responsabilité civile générale, ainsi que de produits de garanties. Trisura est cotée A- (Excellent) par l'agence A.M. Best.

Trisura Garantie est une filiale de Trisura Group Ltd., un fournisseur d'assurance spécialisée de premier plan à l'échelle internationale qui exerce ses activités dans les segments de marché suivants : cautionnement, solutions de risques, assurance pour les membres de la direction et réassurance. Trisura Group regroupe principalement trois filiales règlementées : Compagnie d'Assurance Trisura Garantie, Trisura International Insurance Ltd. et Trisura Specialty Insurance Company. Trisura Group est cotée à la Bourse de Toronto sous le symbole « TSU ».

Pour plus d'information et pour télécharger nos formulaires de proposition, visitez notre site Web à l'adresse www.trisura.com