Janvier 2019

Alerte : Comment le cyberterrorisme pourrait avoir une incidence sur votre couverture d'assurance

NotPetya, WannaCry et d'innombrables piratages informatiques touchant tant les organisations publiques que les organisations privées et gouvernementales ont conduit certains des pays les plus puissants à se blâmer mutuellement. Les cyberattaques et les atteintes à la sécurité des réseaux ne datent pas d'hier. Cependant, l'ampleur et la gravité de certaines cyberattaques ont donné lieu à des accusations de cyberterrorisme contre certains gouvernements et pays. Mais en ce qui vous concerne, vous, l'assuré, pourquoi est-il important que la cyberattaque qui a fait des ravages dans votre entreprise soit qualifiée de « cyberterrorisme »? C'est important parce que le fait qu'un incident de cybersécurité soit considéré comme un acte de cyberterrorisme peut avoir une incidence sur la couverture offerte par votre police d'assurance.

Litige en matière d'assurance contre le cyberterrorisme

En juin 2017, Mondelez, le géant de la confiserie, a été victime de l'attaque mondiale par le logiciel malveillant NotPetya. Le virus a été désactivé et aurait causé des dommages permanents à 1 700 serveurs et 24 000 ordinateurs portables de l'entreprise. Mondelez s'est également dit victime d'un vol d'identifiants d'utilisateurs, de commandes de clients non exécutées et d'autres pertes; au total, les dommages ont été estimés à plus de 100 millions de dollars. Elle a en demandé le règlement en vertu de sa police d'assurance des biens, qui couvrait 1) « la perte ou les dommages touchant des données, des programmes ou des logiciels, y compris la perte ou les dommages causés par l'introduction malveillante d'un code ou d'instructions machine », et 2) « l'interruption résultant directement de la défaillance de matériel informatique de traitement de données ou de supports découlant des cyberdommages causés par malveillance ». En juin 2018, Zurich, l'assureur, a refusé de l'indemniser sur la base d'une exclusion contenue dans la police, qui ne prévoyait pas de couverture pour les pertes résultant « d'un acte d'hostilité ou de guerre en temps de paix ou de guerre... par tout gouvernement ou pouvoir souverain, ou toute force militaire, navale ou aérienne, ou encore tout agent ou autorité de toute partie susmentionnée. » Depuis, les deux parties se livrent une bataille juridique quant à la couverture. Notamment, en février 2018, le gouvernement britannique a publiquement attribué l'attaque NotPetya à la Russie. Des déclarations officielles similaires d'autres pays ont suivi, y compris des États-Unis. Comme le fardeau de la preuve incombait à Zurich qui devait justifier que l'exclusion s'appliquait pour empêcher la couverture, l'assureur a présenté ces déclarations à l'appui de sa position selon laquelle l'exclusion relative au « terrorisme » s'applique.

Les cyberattaques sont notoirement difficiles à attribuer à une partie précise, et les motifs qui les sous-tendent sont tout aussi difficiles à prouver. Cela peut conduire à une incertitude quant à la couverture, comme en témoigne le litige Mondelez-Zurich. Ce litige soulève sans aucun doute de nombreuses questions, tant sur l'aspect juridique qu'en matière d'assurance, et il donnera certainement lieu à une décision ayant valeur de précédent et aura des répercussions sur les assurés partout en Amérique du Nord. Toutefois, une question très importante subsiste : Mondelez cherchait à obtenir une cybercouverture pour certaines pertes en vertu de sa police d'assurance des biens qui offre une cybercouverture plus limitée par rapport à une police d'assurance cyberresponsabilité spécialisée.

Assurance cyberresponsabilité

La grande majorité des polices d'assurance de responsabilité civile générale des biens et des entreprises prévoient une exclusion relative à la « guerre » ou au « terrorisme », comme celle qui figure dans la police d'assurance des biens de Mondelez, et d'ailleurs, ces polices n'ont pas été conçues pour offrir une cybercouverture robuste. Bien que la plupart des polices de cyberassurance contiennent également une forme de cette exclusion, c'est la norme dans l'industrie d'adapter l'exclusion relative à la guerre ou au terrorisme afin de permettre la couverture des risques liés au cyberterrorisme, y compris les cyberattaques commanditées par un état. Dans le même ordre d'idées, une police d'assurance cyberresponsabilité peut vous protéger si vous êtes victime d'un piratage ou d'un virus malveillant potentiellement déclenché par un acteur commandité par un état. De plus, une police d'assurance cyberresponsabilité peut offrir la solide couverture suivante :

AON

Couverture	Assurance cyberresponsabilité
Coûts de l'intervention liée à une atteinte à la vie privée ou à la cybersécurité (réelle ou présumée), notamment : • Équipe d'intervention spécialisée composée d'experts, dont un conseiller juridique, qui fournit du soutien sur appel 24 heures sur 24, 7 jours sur 7 • Dépenses de notification en cas d'atteinte à la sécurité, entre autres le coût d'embauche de conseillers juridiques et de consultants en relations publiques • Coûts des services de surveillance du crédit et de protection • Notification et établissement d'un centre d'appels • Coûts de l'expertise judiciaire en informatique • Ressources en matière de vol d'identité • Initiatives de gestion de crise proactives dans le cas d'une atteinte à la cybersécurité suspectée	✓
Coûts d'interruption des activités découlant d'un incident de sécurité sur le réseau (c'est-à-dire la perte de revenus, les dépenses pour remettre le système en état de fonctionner, etc.)	✓
Coûts de restauration des données dans le cas de dommages causés à des biens intangibles ou d'une altération de ceux-ci (c'est-à-dire les frais engendrés pour restaurer/recréer les données ou les logiciels qui ont été altérés/détruits lors d'un incident de sécurité sur le réseau)	✓
Coûts d'une cyberextorsion (c'est-à-dire le montant de la rançon payée, les frais engendrés pour embaucher des experts pour aider à la résolution de la situation)	✓
Frais de défense, sommes payées dans le cadre d'un jugement et/ou d'un règlement amiable pour toute action en dommages et intérêts résultant de l'omission de protéger les renseignements permettant d'identifier une personne ou les renseignements d'entreprise confidentiels confiés au cabinet, ou placés à ses soins ou sous sa surveillance, par l'intermédiaire d'un réseau informatique ou hors ligne (p. ex., par l'intermédiaire d'un ordinateur portable, de papiers, de dossiers, de disques)	✓
Frais de défense, sommes payées dans le cadre d'un jugement et/ou d'un règlement amiable pour toute action en dommages et intérêts résultant d'un code malveillant (virus, ver, cheval de Troie, etc.) qui est transmis au système d'un tiers et qui l'envahit	✓
Frais de défense, sommes payées dans le cadre d'un jugement et/ou d'un règlement amiable dans le cadre des risques de responsabilité de contenu, comme des actions en diffamation ou en violation de droits de la propriété intellectuelle découlant d'activités de marketing, de publicité ou sur un site Web	✓
Frais de défense liés aux procédures réglementaires découlant de l'atteinte à la vie privée ou à la cybersécurité et couverture des amendes et sanctions administratives, dans la mesure où elles sont assurables	✓

L'approche intégrée d'Aon

Le marché de l'assurance cyberresponsabilité est l'un des plus spécialisés dans le monde de la responsabilité civile des entreprises. La combinaison de cette couverture avec un programme complet d'assurance responsabilité civile générale et des biens de façon adéquate constitue une tâche complexe qui requiert une profonde compréhension de chaque forme de police. Nous recommandons donc de travailler avec un courtier doté d'une grande expérience et d'une bonne compréhension des solutions de transfert de risques qui sont offertes. En plus de proposer les principaux types d'assurances, Aon dispose d'une pratique intégrée spécialisée dans la cyberresponsabilité et la responsabilité en matière de confidentialité au plan national, composée de courtiers, de chargés de compte, d'avocats et de professionnels des technologies de l'information spécialisés. Nos courtiers comprennent que nombre de risques liés à la sécurité et à la confidentialité sont uniques, et que les organisations ont des besoins spécifiques en fonction de leur taille, de leur situation, de leur utilisation de la technologie et du type de travail effectué.

Préparé par

Jessica Foster J.D.
+1.416.868.5651
jessica.foster@aon.ca

À propos d'Aon

Aon plc (NYSE : Aon) est un des principaux cabinets mondiaux de services professionnels, fournissant un vaste éventail de solutions de risques, de retraite et de santé. Nos 50 000 employés dans 120 pays donnent à nos clients les moyens de prospérer en utilisant des données exclusives et analytiques pour communiquer des informations qui réduisent la volatilité et améliorent le rendement.