Les Expositions aux Cyberrisques et les Solutions de Transfert de Risques Dans le Secteur de la Construction

Les avancées technologiques modifient la façon dont les activités sont menées dans le secteur de la construction. L'utilisation de logiciel de modélisation hydraulique, l'ajout de la « technologie prêt-à-porter » dans les casques de protection, les gilets de sécurité et les outils, ainsi que les techniques de conception 3D collaborative ne sont que quelques exemples de la manière dont la technologie transforme la façon dont les projets sont réalisés. Alors que les entreprises utilisent ces avancées technologiques pour améliorer leur efficience, faciliter la communication et réduire le temps nécessaire à la réalisation d'un projet, l'utilisation de ces outils modifie également les profils de risque des organisations, ce qui favorise des expositions aux cyberrisques nouveaux et accrus.

Les expositions aux cyberrisques dans le secteur de la construction

Pendant de nombreuses années, les entreprises de construction ont affecté des ressources importantes pour assurer la sécurité physique de leurs projets, mais n'ont pas consacré la même attention et les mêmes ressources à la sécurité des systèmes d'information et électroniques. Bien que de nombreuses entreprises du secteur ne croient peut-être pas qu'elles font réellement face à des cyberrisques, en réalité, la plupart possèdent des renseignements confidentiels qui pourraient faire d'elles des cibles attrayantes pour des pirates informatiques. En 2016, Construction Dive, une entreprise américaine qui fournit des nouvelles et des analyses, a signalé une augmentation de 400 % des attaques de rançongiciels dans le secteur de la construction au cours de l'année précédente. Par ailleurs, un récent sondage américain réalisé par Forrester Research, Inc. a révélé que plus de 75 % des répondants dans les secteurs de la construction, de l'ingénierie et des infrastructures avaient connu un cyberincident au cours des 12 derniers mois. Bien que ces statistiques concernent les États-Unis, les tendances observées au sud de la frontière sont souvent des signes précurseurs de ce qui attend le Canada.

De nombreuses entreprises de construction stockent de grandes quantités de renseignements sur la paie et la santé des employés, ce que certains experts estiment être plus précieux pour les pirates que les données de cartes de paiement de tiers. De plus, les renseignements relatifs aux projets de haute visibilité et de grande envergure pourraient être ciblés pour des raisons politiques ou, dans certains cas, utilisés pour accéder à des données d'entreprise précieuses pouvant être exploitées pour obtenir un avantage concurrentiel. Les pirates peuvent également chercher à tirer parti des vulnérabilités des modèles procéduraux ou structurels partagés, des logiciels de conception et de construction (tels que BIM, Procor et Revit), des systèmes de surveillance d'immeubles intelligents ou d'autres systèmes dotés de capacités d'accès à Internet ou accessibles à distance. Si les cybercriminels peuvent accéder aux données de ces systèmes, ils peuvent créer des problèmes opérationnels, modifier ou détruire des données et éventuellement retarder l'achèvement d'un projet.

Les organisations fortement dépendantes des processus électroniques ou des réseaux informatiques sont aussi potentiellement vulnérables aux attaques de cyberextorsion. Des pirates cherchant à obtenir une rançon ont utilisé des attaques par déni de service distribuées (attaques DDoS) pour saturer un système au moyen du trafic provenant de réseaux de zombies et empêcher l'accès aux serveurs de l'entreprise, aux sites Web et aux portails Web des clients jusqu'à la réception de la rançon. Des extorqueurs ont également ciblé des employés, ce qui les a amenés à télécharger sans le savoir des logiciels malveillants envoyés par l'entremise d'un courriel apparemment inoffensif qui crypte des fichiers et exige une rançon pour les débloquer.

Des menaces réelles pour les entreprises de construction

Bien trop souvent, les entreprises négligent de s'attaquer aux cyberrisques, estimant qu'elles ne seront jamais une cible en raison de leur taille, de leur situation géographique ou d'autres facteurs. Cependant, la réalité d'aujourd'hui est telle que les petites et moyennes entreprises sont en fait plus ciblées plus fréquemment que les grandes, car les criminels s'attaquent aux propriétaires de petites entreprises qui sont sans méfiance et sans protection. Étant donné la gravité évidente des cyberincidents sur les plans financier, juridique et de la réputation, il est prudent pour toutes les entreprises de construction de mettre en œuvre un programme de gestion des cyberrisques pour atténuer les effets de cyberincidents tels que ceux-ci :

- Le chef de la direction d'une entreprise de béton a ouvert un courriel d'hameçonnage qui s'est infiltré dans le réseau informatique de l'entreprise, sans être détecté par un logiciel antivirus. Le code malveillant a dévoilé les noms, les adresses, les numéros d'assurance sociale et les dossiers médicaux de 50 employés. L'entreprise a été condamnée à une amende de 218 797 $ par un comité d'enquête réglementaire pour « ne pas avoir protégé des renseignements identificatoires ».

- Turner Construction a été victime d'un hameçonnage ciblé en 2016 lorsqu'un employé a envoyé des renseignements fiscaux sur des employés actuels et anciens à un compte de messagerie frauduleux. Les renseignements comprenaient les noms complets, les numéros d'assurance sociale, les provinces d'emploi et de résidence ainsi que les données relatives aux retenues d'impôt pour 2015.

- En 2016, Whiting-Turner Contracting a été informée par un fournisseur externe qui préparait des formulaires fiscaux W-2 et 1095 pour les employés de l'entreprise d'activités suspectes sur ses systèmes. À peu près au même moment, les employés de Whiting-Turner ont signalé des déclarations de revenus frauduleuses faites en leur nom. Outre les renseignements sur les employés, il est également possible que des données personnelles sur les enfants et les bénéficiaires d'employés bénéficiant d'une couverture d'assurance maladie par l'entremise de Whiting-Turner ont été compromises.

Assurance cyberresponsabilité

Une solution d'assurance cyberresponsabilité peut couvrir les dommages subis par l'assuré ou par des tiers résultant d'une atteinte à la cybersécurité ou à la vie privée. Voici un résumé de la couverture offerte par cette assurance :

Couverture des dommages subis par l'assuré

- 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)

Couverture des dommages subis par des tiers

- 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'une communication non autorisée de renseignements permettant d'identifier une personne ou de 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'une incapacité de l'assuré à protéger son réseau informatique contre des menaces telles que les pirates, les virus, les vers, les chevaux de Troie et les attaques par déni de service
- 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. Intégrer cette couverture dans un programme d’assurance complet de façon adéquate constitue une tâche complexe qui requiert une profonde compréhension de nombreux formulaires 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 pouvoir compter sur son Groupe de services de construction, Aon est la seule entreprise canadienne du secteur du courtage qui 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 entreprises de construction ont des besoins spécifiques en fonction de leur taille, de leur situation, de leur utilisation de la technologie et du type des projets réalisés.

Nous prenons le temps d’analyser les expositions uniques de chaque entreprise de construction, et travaillons avec nos clients pour leur offrir un programme d’assurance personnalisé exhaustif et efficace.

Personnes-ressources

Sean Hoare
+1.416.868.5593
sean.hoare@aon.ca

Katie Andruchow
+1.416.868.5526
katie.andruchow@aon.ca

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

À propos d'Aon au Canada

Aon Reed Stenhouse

Depuis plus de 160 ans, Aon Reed Stenhouse est, d'une manière ou d'une autre, un chef de file du secteur canadien des assurances.

Aon Reed Stenhouse, faisant affaire sous le nom commercial d'Aon Risk Solutions/Conseillers en gestion des risques, est le premier courtier d'assurance et cabinet de services de gestion des risques au Canada. Nous servons une vaste clientèle, traitant plus de 2 milliards de dollars de primes annuelles au nom de nos clients.

- Courtage d'assurance
- Gestion des risques
- Avantages sociaux et santé des employés

Nos 1 600 professionnels de l'assurance servent notre clientèle depuis 23 succursales situées dans l'ensemble du Canada. Nous offrons à nos clients une large gamme de solutions innovantes. Chaque jour, les professionnels d'Aon œuvrent à offrir les meilleures solutions à nos clients.

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.

aon.ca