Les cyberrisques dans le secteur de la construction

L'incidence des avancées technologiques sur l'évolution du risque

Les avancées technologiques modifient la façon dont les activités sont menées dans le secteur de la construction. L'utilisation de la technologie des réseaux électriques intelligents, l'ajout de la « technologie prêt-à-porter » dans les casques de protection, les gilets de sécurité et les outils, ainsi que dans la modélisation collaborative des données du bâtiment en 3D ne sont que quelques exemples de la manière dont la technologie transforme la façon dont les projets sont réalisés. Cependant, 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 d'une organisation, ce qui crée de nouveaux risques technologiques et cyberrisques ou accroît les risques existants.

Par conséquent, nous avons assisté à une réglementation plus contraignante de la part des gouvernements relativement à la conformité en matière de cybersécurité dans de nombreux secteurs et à un recours plus fréquent à des protections contractuelles contre les cyberrisques, notamment à des exigences contractuelles imposant la souscription de produits d'assurance contre les risques technologiques et les cyberrisques aux entrepreneurs et autres fournisseurs de services. De plus, nombre d'entreprises du secteur de la construction prennent des mesures proactives pour étudier les options disponibles afin de réduire et de transférer les risques technologiques et les cyberrisques au moyen de solutions d'assurance.

Les risques technologiques et les 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. Beaucoup d'entreprises de construction stockent de grandes quantités de renseignements sur la paie et la santé des employés, ce que certains experts estiment être en fait 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 dont on pourrait tirer un avantage concurrentiel.

Les pirates peuvent également chercher à exploiter les 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. S'ils peuvent accéder aux données utilisées dans 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 potentiellement vulnérables à d'autres manœuvres perturbatrices des pirates, les 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 ce qu'ils soient payés. Ils ont également ciblé des employés, ce qui a amenés ceux-ci 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.

Les polices d'assurance standards ne sont pas suffisantes

Bien que certaines polices d'assurance puissent offrir une protection limitée contre les risques technologiques et les cyberrisques, la plupart n'ont pas été rédigées dans le but de couvrir les types de pertes qui pourraient découler d'une cyberattaque ou d'une atteinte à la vie privée :

- Responsabilité civile générale : couvre les dommages corporels et matériels, et non les pertes économiques, et peuvent contenir des exclusions relatives aux données et aux atteintes à la vie privée.
- Responsabilité civile professionnelle : couvre les dommages économiques découlant de la prestation défaillante de services définis seulement (pas assez étendue pour inclure les autres services technologiques fournis), et peuvent contenir des exclusions relatives aux données et aux atteintes à la vie privée. La nature et l'étendue de l'assurance ne couvrent pas les frais de gestion de crise engagés par l'assuré durant une atteinte à la cybersécurité.
- Assurance des biens : couvre les biens matériels, ce qui exclut les données. Les pertes doivent avoir été causées par un risque matériel, tandis que les risques pour les données sont les virus et les pirates.
- Vols et détournements : couvre les employés et en général seulement l'argent, les titres et les biens matériels. Aucune couverture des biens de tiers tels que les données des clients.

- De plus, il peut y avoir des situations où les polices d'assurance standards sont insuffisantes pour des motifs de nature contractuelle :
  - Une entreprise de construction engagée par un tiers pourrait avoir l'obligation contractuelle de souscrire une assurance responsabilité civile professionnelle contre les risques technologiques et/ou les cyberrisques dans certains cas.
  - L'assurance pourrait être nécessaire pour bien couvrir le cyberrisque lié à un tiers qui serait chargé de stocker ses données électroniques et qui refuserait d'admettre sa responsabilité en cas d'atteinte à la cybersécurité de ces données.

Assurance responsabilité civile professionnelle contre les risques technologiques et les cyberrisques (erreurs et omissions)

Une solution d'assurance responsabilité civile professionnelle contre les risques technologiques et les cyberrisques 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 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, de renseignements protégés sur la santé 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, que ces menaces aient lieu ou non dans le cadre de la prestation de services professionnels par l'assuré
- Frais de défense, sommes payées dans le cadre d'un jugement et/ou d'un règlement amiable pour toute action alléguant une erreur, une omission ou une négligence dans la réalisation d'analyses de données ou dans la fourniture de produits ou de services technologiques
- 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 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

Couverture des dommages subis par l'assuré

Coûts d'une interruption des activités réseau attribuable à un incident de sécurité sur le réseau, y compris la perte de revenus et les dépenses supplémentaires pour remettre le système en état de fonctionner

- Coûts liés à des dommages causés à des biens intangibles ou à une altération de ceux-ci, y compris les frais engendrés pour restaurer ou reconstituer les données ou les logiciels qui ont été altérés ou détruits en raison d'un incident de sécurité sur le réseau
- Coûts de l'intervention liée à une atteinte à la cybersécurité, y compris :
  - Dépenses de déclaration en cas d'atteinte à la sécurité, entre autres le coût d'embauche de conseillers juridiques et de consultants en relations publiques
  - Services de protection et de surveillance du crédit
  - Notification et établissement d'un centre d'appels
  - Coûts de l'expertise judiciaire en informatique
  - Ressources en matière de vol d'identité
- Coûts induits par une cyberextorsion, y compris le montant de toute rançon versée et les frais engagés pour embaucher des experts afin d'aider à la résolution de la situation d'extorsion

Un transfert efficace des risques technologiques et des cyberrisques

Le marché de l'assurance évolue rapidement dans le domaine des cyberrisques et nombre d'assureurs offrent maintenant aux assurés l'accès à des coachs en protection des données, à des ressources pour le contrôle des pertes, à des ressources spécialisées dans les réclamations et à des listes de fournisseurs préapprouvés de services d'intervention en cas d'atteinte lorsqu'ils souscrivent une cyberassurance. Toutefois, la qualité des produits d'assurance varie beaucoup dans le domaine de la cyberresponsabilité, il importe donc de travailler avec un courtier d'assurance qui connaît bien les subtilités d'une telle couverture ainsi que les autres ressources que les assureurs peuvent offrir en cas d'atteinte.

Nous sommes là pour produire des résultats

Katharine A Hall
780.423.9820
katharine.hall@aon.ca

Stella Lee
416.868.5855
stella.lee@aon.com

Katie Andruchow
416.868.5526
katie.andruchow@aon.ca

aon.ca