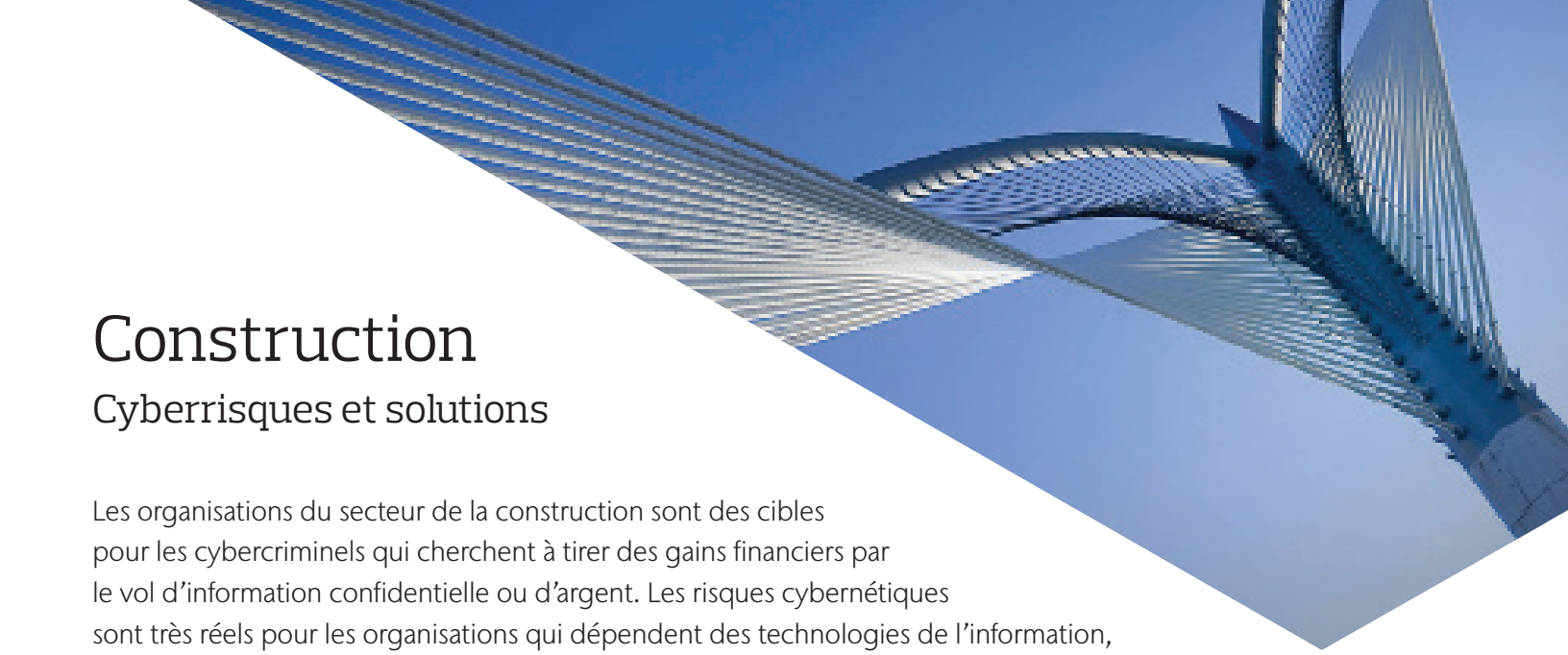

Construction

Cyberrisques et solutions

Les organisations du secteur de la construction sont des cibles pour les cybercriminels qui cherchent à tirer des gains financiers par le vol d'information confidentielle ou d'argent. Les risques cybernétiques sont très réels pour les organisations qui dépendent des technologies de l'information, de la connectivité et de processus automatisés. Dans un environnement juridique et réglementaire de plus en plus punitif, où les exigences contractuelles concernant l'assurance cyberresponsabilité sont plus fréquentes, les entreprises prévoyantes prennent des mesures proactives pour étudier et transférer le cyberrisque.

De nombreux facteurs contribuent au profil de cyberrisque d'une organisation, y compris les actions des employés, les erreurs des systèmes et des programmes, les mesures de sécurité, le secteur, la nature et la quantité des données recueillies, l'importance politique ou stratégique et la dépendance à l'égard des technologies.

Facteurs de cyberrisque pour les organisations du secteur de la construction

- Collecte, conservation, diffusion ou stockage de renseignements privés
- Grande dépendance à l'égard des processus électroniques ou des réseaux informatiques
- Dommages corporels et matériels consécutifs à des cyberincidents
- Attention accrue des pirates liée à des immeubles ou projets très visibles, y compris des immeubles gouvernementaux, des infrastructures (eau et électricité) et des projets militaires
- L'utilisation de l'infonuagique expose les entrepreneurs à une responsabilité à l'égard, notamment, de la sécurité des données, des pannes réseau et de questions de conformité réglementaire
- Dépendance à l'égard d'infrastructures essentielles ou exploitation de celles-ci
- Assujettissement aux lois de réglementation

  Risque associé à la construction d'installations médicales en vertu du *Health Insurance Portability and Accountability Act*
- Dépendance à l'égard de fournisseurs, d'entrepreneurs indépendants ou d'autres fournisseurs de services
- Renseignements détenus par les fournisseurs :
  - Programmes de modélisation des données du bâtiment (MDB)
  - Utilisation d'ordinateurs et autres appareils portables (téléphones cellulaires, tablettes, etc.) pour accéder aux systèmes dans les locaux de tiers, par exemple des chantiers ou des hôtels

Cyberincidents potentiels pour les organisations du secteur de la construction

- Accès aux données de construction par des pirates, ce qui peut perturber l'exploitation par la destruction physique des données, des serveurs et de l'infrastructure ou des menaces à la sécurité des personnes sur place
- Interruption de réseau entraînant une perte de revenus d'entreprise
- Actes intentionnels commis par des employés malhonnêtes
- Attaques de rançongiciels

Nous sommes là pour produire des résultats

cyber.deal.desk@aon.ca

aon.com/canada/fr

AON
Empower Results®

Étendue de la cybercouverture traditionnelle offerte dans le marché de l'assurance

Éléments de la couverture des dommages subis par des tiers

- ***Sécurité et protection des renseignements personnels :*** Frais de défense et dommages subis par des tiers découlant d'une défaillance de la sécurité informatique, y compris la responsabilité liée au vol ou à la communication non autorisée d'information confidentielle, à l'accès non autorisé, à une attaque par déni de service ou à la transmission d'un virus informatique.
- ***Défense liée à des procédures réglementaires et amendes :*** Frais de défense liés à des procédures intentées par un organisme gouvernemental relativement à une incapacité de protéger des renseignements privés ou à une défaillance de la sécurité du réseau.
- ***Responsabilité relative aux médias :*** Frais de défense et dommages subis par des tiers liés à des préjudices attribuables au contenu, comme la diffamation écrite ou orale, la calomnie, les atteintes au droit d'auteur, les infractions aux marques déposées ou les violations du droit à la vie privée.
- ***Amendes et évaluations relatives à l'industrie des cartes de paiement :*** Frais de défense liés à des enquêtes menées par l'industrie des cartes de paiement relativement à une incapacité de protéger des renseignements privés ou à une défaillance de la sécurité du réseau.

Éléments de la couverture des dommages subis par l'assuré

- ***Coûts de l'intervention liée à une atteinte à la sécurité :*** Frais liés à la notification de l'atteinte, y compris le recrutement de cabinets d'avocats externes et de consultants en relations publiques, à l'expertise judiciaire, à la surveillance ou à la protection du crédit, à une ligne téléphonique ou à un centre d'appels pour la notification et aux ressources en matière de vol d'identité.
- ***Interruption des activités réseau :*** Perte de revenu et dépenses supplémentaires attribuables à une défaillance de la sécurité du réseau.
- ***Pertes d'exploitation d'entreprises dépendantes :*** Remboursement à l'assuré de la perte de revenu net réelle et des dépenses supplémentaires engagées lorsque le système informatique du fournisseur de service de l'assuré a été interrompu ou suspendu en raison d'une défaillance de la sécurité du réseau.
- ***Pertes d'exploitation dues à une défaillance de système :*** Couverture des pertes d'exploitation dues à une défaillance de système non intentionnelle ou imprévue qui n'a pas été causée par une défaillance de la sécurité du réseau.
- ***Restauration des données :*** Coûts liés à la restauration ou à la recréation des données ou des logiciels consécutive à une défaillance de la sécurité du réseau.
- ***Cyberextorsion :*** Remboursement à l'assuré des dépenses engagées pour enquêter sur une menace et des paiements effectués par suite d'une extorsion pour prévenir ou résoudre la menace.

Aon a réussi à négocier les importantes améliorations de la couverture suivantes (sous réserve de l'acceptation du risque individuel par le marché)

- Montants de garantie complets pour l'intervention liée à l'incident et les coûts liés à la notification de l'atteinte
- Définition élargie de système informatique
- Couverture du cyberterrorisme
- Suppression de l'exclusion des appareils non chiffrés
- Aucune exclusion pour défaut d'appliquer les correctifs
- Couverture des pertes d'exploitation liées à la chaîne d'approvisionnement
- Coûts liés à la détérioration – remplacement des documents transférés
- Couverture de la perte d'utilisation – coûts de remplacement des appareils IdO
- Couverture des retards de livraison ou d'exécution
- Couverture de la responsabilité environnementale

Empower Results®

Notre approche

Adoption d'une stratégie de cyberassurance fondée sur le risque

Les capacités d'Aon en matière de cybersécurité peuvent aider les organisations à adopter une approche fondée sur le risque par les moyens suivants :

- ***Évaluation des risques cybernétiques :*** Une approche à l'échelle de l'entreprise des risques cybernétiques qui procure une vue détaillée du profil technologique unique d'une organisation et des menaces auxquelles elle peut être exposée, dans le but de faciliter la quantification des risques et l'assurabilité.
- ***Analyse des répercussions cybernétiques :*** Un cadre d'analyse fondé sur des données qui aide les organisations à optimiser leur stratégie de résilience en atténuant et en transférant les risques. Les stratégies de financement des risques actuelles peuvent aussi être améliorées par la modélisation des scénarios de sinistres informatiques et la soumission des plafonds actuels à des simulations de crise.

Innovation en cybersécurité

- Nos polices élargissent l'étendue de la cybercouverture au cas par cas pour inclure les dommages matériels résultant d'une défaillance de la sécurité du réseau, la couverture des pertes d'exploitation et des dépenses supplémentaires consécutives à des défaillances des systèmes, la carence des fournisseurs de réseau (fournisseurs de TI et chaîne d'approvisionnement) et la couverture du cyberterrorisme.

Notre cadre de cyberrésilience

Aon et Stroz Friedberg offrent une gamme complète de services pour vous aider à traiter le cyberrisque comme un risque d'entreprise et à atteindre la cyberrésilience.

Rechercher

N'attendez pas que ça arrive, recherchez-le.

Certaines organisations estiment qu'elles n'ont pas à se préparer en cas de cyberincident, tandis que d'autres se croient en sécurité. Notre équipe vous aide à comprendre et à quantifier ce qui est à risque.

- Évaluation du dispositif de sécurité de votre organisation
- Respect de cadres de sécurité éprouvés
- Essais et recherche proactifs des activités malveillantes
- Quantification des dommages financiers potentiels d'un cyberincident
- Listes de mesures prioritaires pour améliorer votre cyberrésilience

Protéger

Connaître les risques liés à une cyberattaque ne vous aidera pas à protéger votre organisation.

La protection des actifs essentiels est l'une des décisions les plus importantes que vous devez prendre. Laissez notre équipe vous faciliter cette tâche.

- Protection de votre entreprise contre les pertes financières dues à un cyberincident
- Compréhension des risques liés à vos placements
- Élaboration de politiques et de normes de sécurité sur mesure
- Correction des vulnérabilités
- Conseils stratégiques en cybersécurité et élaboration d'un programme

Résoudre

Au bout du compte, vous avez besoin de spécialistes pour vous aider à vous rétablir.

Notre équipe de professionnels chevronnés est extrêmement efficace pour vous aider à vous rétablir après une attaque. Qu'il s'agisse de sécuriser vos systèmes ou de simplifier les réclamations, nous veillons à ce que tout se déroule sans heurt.

- Intervention défensive en cas d'attaque
- Minimisation des pertes d'exploitation
- Recours à des techniques criminalistiques de pointe
- Déploiement de spécialistes de haut niveau des domaines techniques, juridiques et policiers qui comprennent les conséquences juridiques, réglementaires et financières
- Aide à la maximisation de la couverture et au recouvrement des coûts

Empower Results®

L'expérience d'un client

Stroz Friedberg a travaillé avec une firme mondiale de conseil en ingénierie et en conception œuvrant dans 23 emplacements, qui s'interrogeait à propos des répercussions qu'un cyberincident pourrait avoir sur ses technologies et activités essentielles.

Afin de comprendre le profil de risque de l'organisation, nous avons produit une évaluation détaillée de la cybersécurité et de la vulnérabilité de l'architecture de système du client. Pour ce faire, nous avons examiné des scénarios d'incidents graves et plausibles auxquels la firme conseil en ingénierie pourrait faire face, puis quantifié les pertes financières potentielles.

Après l'évaluation et la quantification des cyberrisques, l'équipe a aussi été en mesure de recommander et de mettre en œuvre de nombreuses mesures d'optimisation de la cybersécurité par les moyens suivants :

- Essais de pénétration et mise à l'essai des plans
- Évaluation et planification de l'amélioration de l'architecture de système
- Ateliers et planification à l'intention du conseil d'administration
- Examen de la police de cyberassurance actuelle comparativement au coût total du risque

En traitant le cyberrisque comme un risque d'entreprise, la firme conseil a pu comprendre parfaitement les répercussions d'un cyberincident et corriger les vulnérabilités de ses technologies et activités essentielles.