CYBERRESPONSABILITÉ

Nous sommes dans une nouvelle ère. Les technologies ainsi qu'Internet ont des répercussions sur les opérations du monde des affaires d'aujourd'hui. Avec ces changements, la cyberexposition a augmenté de façon exponentielle. Afin de protéger les systèmes informatiques de votre institution et les données personnelles de vos clients, ARM a préparé cette fiche d'information sur certains des cyberrisques auxquels vous pouvez devoir faire face, ainsi que les solutions que nous pouvons vous offrir pour minimiser ces risques.

Cyberrisques

L'exposition aux cyberrisques et les conséquences qui en découlent sont très réelles et très nombreuses. Elles peuvent inclure des attaques par déni de service et générer des coûts d'interruption d'activités. En conséquence, une organisation peut ne plus être en mesure d'accéder à son propre système informatique et perdre un temps important de traitement de données. L'accès par les décideurs à des données importantes qui peuvent être essentielles à la mission peut devenir impossible.

QUELS SONT QUELQUES-UNS DES CYBERRISQUES AUXQUELS VOUS POUVEZ ÊTRE EXPOSÉ ?

- Atteinte de la vie privée (divulgation de renseignements personnels identifiables : par exemple le numéro de Sécurité sociale, le nom, l'adresse, etc.) ;
- Cyberextorsion (données prises en otage à moins de payer le maître chanteur) ;
- Cybercriminalité (vandalisme, sabotage des systèmes informatiques, etc.)
- Le risque de terrorisme (utilisation de systèmes informatiques pour saboter des infrastructures telles que l'énergie, les communications, ou l'approvisionnement en eau, etc.) ;
- La responsabilité pouvant découler de failles de sécurité réseau (poursuites judiciaires et exigences de conformité, etc.) ;
- L'utilisation de médias électroniques (comme des photos en ligne, de la musique, des vidéos et des messages texte) ;
- L'utilisation de propriété intellectuelle appartenant à autrui (par exemple les droits d'auteur, marques, brevets) ;
- Erreurs et omissions technologiques (mauvaise conception ou entretien ou dans l'installation des systèmes)
- Collèges devant faire face à la manipulation des dossiers scolaires ou des notes des étudiants en cas d'atteinte à la protection des données causée par des pirates informatiques.
- Les centres médicaux sont toujours confrontés au risque lié à l'intégrité des données des dossiers des patients.
- L'accès illégal ou non autorisé aux systèmes informatiques peut permettre un transfert frauduleux d'argent par utilisation d'instructions de paiement en ligne.
- Une attaque de virus informatique, par exemple, peut endommager les systèmes informatiques, y compris les logiciels, et corrompre les données du système.

Adventist Risk Management,® Inc. ©2015

Solution

IDENTIFICATION ET ANALYSE DE VOS CYBERRISQUES

Les coûts de récupération ou de restauration des données qui ont été modifiées, détruites ou supprimées ne sont pas facilement quantifiables. Cependant, une procédure de gestion des risques peut conduire à l'identification de cyberrisques spécifiques auxquels votre institution est exposée. Elle peut également aider à analyser le niveau des risques et leur impact sur le ministère de votre organisation.

ASSURANCE RISQUE DE CYBERRESPONSABILITÉ

L'assurance risques de cyberresponsabilité est un outil utile pour minimiser les conséquences financières d'une atteinte potentielle à la protection des données des systèmes informatiques. Une police d'assurance cyberresponsabilité pour les églises peut couvrir l'église pour ses risques propres. Cela signifie protéger la propre infrastructure informatique de l'église en cas de sinistre. La police dispose également d'une couverture tierce qui met l'accent sur la responsabilité juridique envers les autres, tels que la perte ou l'exposition d'informations privées de vos clients. Le résumé ci-dessous présente les deux niveaux de couverture de la police de cyberresponsabilité :

TIERCE (AUTRES PERSONNES):
COUVERTURE CYBERRESPONSABILITÉ

- Sécurité réseau ;
- Atteinte à la vie privée ;
- Média Internet.

RISQUES PROPRES (ASSURÉ/VOUS) :
FRAIS CYBERCRIMINALITÉ

- Procédures réglementaires ;
- Surveillance du crédit ;
- Pertes de données propres ;
- Interruption de l'exploitation du réseau ;
- Extorsion réseau.

Lorsque vous réfléchirez sur les cyberrisques, votre organisation devra se poser les questions suivantes:

- Qu'est-ce que notre organisation doit faire pour mener notre ministère à l'ère de la technologie?
- De quels outils ou ressources, tels que les systèmes informatiques, notre organisation dépend-elle?
- Quel coût financier ou quel préjudice à notre réputation notre organisation devrait-elle affronter à la lumière d'une atteinte à la protection des données ou d'une indisponibilité des systèmes informatiques?

Nous vous invitons à inclure les cyberrisques dans votre planification de continuité et d'ajouter une police de cyberresponsabilité à votre couverture d'assurance. Pour plus de détails et un formulaire de demande, veuillez vous adresser à votre chargé de compte.

Le cycle de réponse à une atteinte à la protection des données

GLOSSAIRE

CYBER: signification « ordinateur », « réseau informatique », ou « réalité virtuelle », préfixe utilisé dans la formation de mots composés (cyberdiscussion ; cyberart ; cyberespace).
ATTEINTE À LA PROTECTION DES DONNÉES: une atteinte à la protection des données consiste en la libération intentionnelle ou non intentionnelle d'informations sécurisées dans un environnement non sécurisé.
DÉNI DE SERVICE: c'est un type d'attaque de réseau conçu pour entraver ou nuire au réseau en l'inondant de trafic inutile.
RISQUES PROPRES: couverture de l'organisation ou de la personne assurée.
SYSTÈME INFORMATIQUE: également appelé système de technologies de l'information (TI).
RESPONSABILITÉ: une obligation juridiquement exécutoire.
MINIMISATION: pour rendre moins grave, pour prévenir d'autres dommages.
NOTIFICATION: la notification des atteintes à la sécurité est requise par la loi dans la plupart des États.
TIERS: une organisation ou une personne autre que les parties du contrat, par exemple, un client dont les données ont été extorquées.
VIRUS: Un segment de code autorépliquant planté illégalement dans un programme informatique, souvent dans le but d'endommager ou de bloquer un système ou un réseau.

DÉCLAREZ IMMÉDIATEMENT VOTRE SINISTRE

24/7 HOTLINE 1.888.951.4276 PRESS 2 • CLAIMS@ADVENTISTRISK.ORG

TENEZ-VOUS INFORMÉ

ADVENTISTRISK.ORG/SOLUTIONS

Adventist Risk Management, Inc. © 2015