

Exemple de tableau de bord d'exposition aux cyberrisques

Présenté par le siège social de
Cowan Insurance Group Ltd

QUESTION	RÉPONSE	POINTAGE
Votre entreprise utilise-t-elle un réseau sans fil ou des employés ou des clients ont-ils accès à vos systèmes internes à partir de sites distants?		
Quelqu'un dans votre entreprise apporte-t-il des appareils mobiles appartenant à l'entreprise (ordinateurs portables, téléphones intelligents, clés USB, etc.) avec lui à la maison ou pendant ses déplacements?		
Votre organisation utilise-t-elle un logiciel ou un stockage d'informatique en nuage?		
Votre organisation utilise-t-elle une politique « Apportez votre propre appareil » (AVPA) autorisant les employés à utiliser des appareils personnels à des fins professionnelles ou sur un réseau d'entreprise?		
Des employés sont-ils autorisés à accéder aux privilèges administratifs sur votre réseau ou vos ordinateurs?		
Votre entreprise dispose-t-elle de systèmes opérationnels essentiels connectés à un réseau public?		
Quelqu'un dans votre organisation utilise-t-il des ordinateurs pour accéder à des comptes bancaires ou effectuer des transferts d'argent?		
Votre organisation stocke-t-elle des renseignements sensibles (c.-à-d. rapports financiers, secrets commerciaux, propriété intellectuelle et conceptions de produits) susceptibles de compromettre votre organisation en cas de vol?		
Votre organisation stocke-t-elle sous forme numérique les renseignements personnels des employés ou des clients? Ces renseignements peuvent comprendre des numéros d'identification délivrés par le gouvernement et des renseignements financiers.		
Votre organisation fait-elle partie d'une chaîne d'approvisionnement ou avez-vous des partenaires dans la chaîne d'approvisionnement?		
Votre organisation exerce-t-elle des activités dans des pays étrangers, physiquement ou en ligne?		
Votre entreprise a-t-elle déjà omis d'appliquer les règles relatives à l'utilisation acceptable des ordinateurs, des courriels, de l'Internet, etc.?		
Le grand public peut-il accéder aux installations de votre organisation sans utiliser de carte d'identité?		
La formation en matière de sécurité du réseau des employés est-elle facultative dans votre organisation?		
Les employés peuvent-ils utiliser leurs ordinateurs ou les périphériques de l'entreprise indéfiniment sans mettre à jour leurs mots de passe?		
Votre service informatique a-t-il déjà omis d'installer un logiciel antivirus ou d'effectuer des contrôles de vulnérabilité réguliers?		
Les employés peuvent-ils éliminer de l'information sensible dans des bacs non sécurisés?		
Votre entreprise perdrait-elle des renseignements essentiels en cas de défaillance du système ou d'un autre sinistre réseau?		
Les employés peuvent-ils facilement voir ce que leurs collègues font sur leur ordinateur?		
Votre organisation a-t-elle négligé de passer en revue ses politiques et procédures de sécurité des données au cours de la dernière année?		

© 2016 Zywave, Inc. Tous droits réservés.

Instructions

Au cours des dernières années, les cyberattaques sont devenues l'une des menaces les plus importantes pour les organisations de toutes tailles. L'Internet et d'autres opérations réseau ont créé des risques que l'on ne voyait pas il y a moins de dix ans. Lorsque des cyberattaques (telles que des fuites de données et des piratages) se produisent, elles peuvent entraîner des dommages dévastateurs, tels que des interruptions d'activité, des pertes de revenus, des frais juridiques, des analyses judiciaires et des notifications de clients ou d'employés.

Il est important de se rappeler qu'aucune organisation n'est à l'abri de l'incidence de la cybercriminalité. En conséquence, l'assurance contre les cyberrisques est devenue un élément essentiel de tout programme de gestion des risques.

Commencez par répondre aux questions de gauche. Une valeur numérique sera attribuée à chaque réponse selon une échelle préétablie. À la fin, nous calculerons votre pointage pour déterminer le niveau de cyberrisque de votre organisation.

OUI = 5 points
INCERTAIN = 5 points
NON = 0 point

Après avoir répondu à toutes les questions, calculez votre pointage pour déterminer le niveau de cyberrisque de votre organisation à l'aide de l'échelle ci-dessous :

ÉCHELLE DE RISQUE : 55-100
RISQUE ÉLEVÉ : 30-50
RISQUE MODÉRÉ : 15-25
RISQUE FAIBLE : 0-10



POINTAGE :

NIVEAU DE RISQUE :