
VICTOR
Cinq conseils pour renforcer la résilience face aux risques cybernétiques

L'environnement des cyber-risques est devenu infiniment plus compliqué et plus important pour les entreprises. Les menaces de cybersécurité, en constante évolution et potentiellement plus coûteuses, font que cette question reste en tête des préoccupations des entreprises. Et elle est passée d'une question du département des technologies de l'information à une question qui fait l'ordre du jour des réunions du conseil d'administration.

Cela souligne à quel point il est essentiel que les entreprises se préparent dès maintenant à assurer leur avenir. Les cyber-risques peuvent être des perturbateurs commerciaux critiques, car ils peuvent survenir n'importe où dans la chaîne d'approvisionnement, même plusieurs niveaux plus bas. Bien qu'il n'y existe pas de solution miracle pour gérer ces risques, la mise en place de contrôles de cybersécurité de base et des bonnes pratiques, ainsi que leur maintien, peuvent améliorer considérablement votre cyberrésilience.

CONSEIL #1 : SE CONCENTRER SUR LA BASE : LES CONTRÔLES DE CYBERSÉCURITÉ

La résilience face aux risques cybernétiques fait de bons progrès. Cela est en grande partie dû au fait que les entreprises se concentrent sur la base, c'est-à-dire prioriser et mettre en œuvre des contrôles de cybersécurité efficaces et robustes.

Ces contrôles peuvent inclure des mesures telles que des contrôles d'accès rigoureux, des mises à jour régulières de logiciels, le cryptage des données sensibles et l'authentification multifactorielle.

Ces améliorations progressives s'additionnent rapidement et peuvent réduire considérablement le risque de cyberattaques et d'atteintes, même de la part d'attaquants sophistiqués.

CONSEIL #2 : COMPRENDRE L'ÉVOLUTION DES OPPORTUNITÉS ET DES MENACES CYBERNÉTIQUES

Les cybermenaces évoluent à mesure que de nouvelles technologies sont déployées et que des acteurs malveillants adaptent leurs tactiques.

Actuellement, l'intelligence artificielle (IA) est une source d'optimisme et d'inquiétude. De nombreuses entreprises explorent l'utilisation d'outils d'IA pour renforcer leurs défenses cybernétiques, par exemple en filtrant le flot d'alertes qu'elles génèrent afin que les plus urgentes soient envoyées à un analyste humain. Cependant, on s'inquiète également du fait que les attaquants utilisent l'IA pour trouver des faiblesses ou même écrire du code malveillant.

Les risques liés à la chaîne d'approvisionnement et les risques de responsabilité sont un autre sujet à l'ordre du jour. Même les entreprises qui ont leurs propres systèmes sécurisés et bien gérés ne savent souvent pas à quel point leurs tierces parties sont sécurisées, et encore moins les quatrièmes parties, et d'autres encore plus loin dans la chaîne. Une tierce partie compromise peut causer des perturbations en rendant

un fournisseur indisponible et en ouvrant une voie aux attaquants pour infiltrer les entreprises connectées.

Les risques liés à la chaîne d'approvisionnement s'étendent également à des questions telles que la protection de la vie privée. Les tierces parties traitent souvent des données sensibles qui, si elles sont exposées, pourraient avoir des conséquences, notamment une atteinte à la réputation et des sanctions réglementaires, telles que celles prévues par le règlement général sur la protection des données (RGPD) en Europe.

CONSEIL #3 : RENFORCER LA CYBERRÉSILIENCE

Ces premières étapes de la gestion et de la compréhension des cybermenaces complexes et évolutives peuvent fournir une meilleure perspective de votre environnement des cyber-risques.

Pour renforcer la résilience, vous devez évaluer et mesurer la propension à accepter des cyber-risques de votre entreprise. Les principales questions à vous poser sont les suivantes :

- Quels sont les actifs et les services essentiels à la mission de l'entreprise et qui doivent absolument être protégés?
- Quel serait le coût – en argent, en temps et en atteinte à la réputation – d'une exposition ou d'une interruption?

Dans cette optique, vous pouvez décider quelles mesures sont raisonnables pour protéger l'empreinte numérique de votre entreprise.

Vous pouvez également décider de ce qu'il faudrait faire pour vous rétablir de manière efficace et rentable.

- Se concentrer sur les moyens de rétablir les opérations essentielles à la mission de l'entreprise en cas d'interruption.
- Utiliser des exercices sur table, des évaluations de fournisseurs et des études de cas pour déterminer quelles devraient être les bonnes mesures de défense et de rétablissement.
- Établir des processus et des politiques solides, afin que chacun sache ce qu'il doit faire au quotidien et quand une crise se matérialise.

Enfin, intégrez-le dans un plan de rétablissement après un incident – et testez-le régulièrement.

CONSEIL #4 : OPTIMISER LES RESSOURCES CLÉS POUR AMÉLIORER LA SITUATION

Les améliorations en matière de sécurité ne doivent pas nécessairement être coûteuses. Il existe de nombreuses ressources disponibles pour vous aider.

Les entreprises doivent faire appel à des experts internes et s'assurer qu'ils participent à la planification de nouvelles plateformes de cybersécurité et des interventions en cas de risques cybernétiques.

Des partenaires bien informés peuvent également vous aider. Par exemple, certains partenaires peuvent offrir une équipe de produits, une équipe de modélisation, une équipe de conseillers et une base de données sur les cyber-risques. Cette base de données peut être transformée en informations, en options d'atténuation des risques et de financement, ainsi qu'en solutions qui vous permettent de comprendre, de mesurer et de gérer vos risques cybernétiques.

D'autres ressources sont disponibles auprès des gouvernements et des organismes internationaux, qui publient souvent des normes et des listes de contrôle qui peuvent être appliquées de manière rentable pour sécuriser l'environnement des cyber-risques de votre entreprise.

Pour obtenir des ressources canadiennes, envisagez de consulter le Centre canadien pour la cybersécurité du gouvernement du Canada, qui offre de l'orientation, des conseils et des renseignements sur les risques cybernétiques potentiels et sur la façon dont les personnes et les entreprises peuvent préserver leur sécurité en ligne.

De plus, le Commissariat à la protection de la vie privée du Canada fournit des ressources sur la protection des données personnelles et de la vie privée.

Les entreprises peuvent également établir des liens avec des réseaux informels, comme des entreprises homologues et des organismes commerciaux. Celles-ci peuvent souvent contribuer à l'échange de bonnes pratiques et à la mise en garde contre les risques émergents.

CONSEIL #5 : MAINTENIR LES BONNES PRATIQUES TOUT AU LONG DE L'ANNÉE

Dans le paysage en constante évolution des cybermenaces, il n'y a pas de ligne d'arrivée.

Il est essentiel de ne pas négliger l'importance de maintenir vos bonnes pratiques en matière de résilience face aux risques cybernétiques et d'utiliser les renseignements sur les menaces pour garder une longueur d'avance sur les risques potentiels.

Aidez à protéger votre entreprise avec l'assurance contre les cyber-risques de Victor

Les cyberattaques constituent une menace réelle et croissante pour les entreprises de toutes tailles. C'est là que l'assurance contre les cyber-risques de Victor entre en jeu. C'est une couverture d'assurance complète avec des prix compétitifs contre des atteintes à la protection des données, des attaques par rançongiciels et des pertes d'exploitation. En plus, grâce à cette assurance, les entreprises ont accès à des services gratuits de gestion de risques – tels que des simulations d'hameçonnage et la surveillance du Web clandestin – à travers de notre application mobile, Victor Response. #LaMenaceEstRéelle

Pour plus d'informations sur l'assurance contre les cyber-risques de Victor, contactez votre courtier d'assurance et visitez : www.assurancevictor.ca/cyber.