



**Toujours en alerte :
Se préparer à l'avenir
des cyber-risques**



Pourquoi une stratégie globale de gestion des risques cybernétiques est essentielle pour protéger votre entreprise.

La cybersécurité est essentielle, mais elle ne représente qu'une partie de l'équation. Voici pourquoi une stratégie globale de gestion des risques cybernétiques est essentielle pour protéger votre entreprise.

Pour sécuriser notre monde, il ne suffit pas de prendre des mesures techniques. Les risques auxquels les entreprises font face aujourd'hui sont continus, évolutifs et de grande envergure, ce qui exige une vigilance constante.

Si les défenses techniques, comme les pare-feux, les systèmes anti-maliciels et les protocoles de cryptage, sont essentielles, les cyber-risques vont au-delà de la cybersécurité. Ils englobent tout, des contrôles de sécurité aux vulnérabilités internes, en passant par la préparation organisationnelle et la résilience. Pourtant, trop peu d'entreprises accordent aux risques cybernétiques la priorité qu'ils méritent.

Le moment est venu de consolider ses fondations en élaborant un plan complet qui aborde la cybersécurité dans le cadre plus large des cyber-risques – un risque commercial essentiel qui doit être géré selon une approche multidimensionnelle en matière d'assurance, d'atténuation et de résilience.

Adoption d'une vision globale

Trop souvent, les entreprises comptent entièrement sur des défenses techniques pour assurer la sécurité de leurs données. Par exemple, une entreprise pourrait disposer d'outils de cybersécurité de pointe pour se protéger contre les violations ou les pannes de système, mais ne pas avoir de plan clair d'intervention en cas d'incident qui attribue des rôles et des responsabilités en cas d'incident, ce qui entraîne des interruptions évitables des affaires. C'est comme se préparer à une catastrophe naturelle : la récupération est tout aussi importante que la prévention.

Une gestion efficace des risques cybernétiques nécessite une approche globale, qui prend en compte tous les aspects, des contrôles de sécurité au comportement humain, lequel peut être le maillon le plus faible. L'erreur humaine reste une cause importante des incidents cybernétiques, mais elle peut être réduite grâce à des formations internes régulières et à la promotion d'une culture de sensibilisation à la cybersécurité. Les entreprises qui élargissent leur champ d'intérêt sont mieux placées pour atténuer les conséquences d'une atteinte cybernétique.

Résilience et plan d'intervention

La gestion efficace des risques cybernétiques nécessite une approche proactive à plusieurs niveaux. La promotion d'une bonne hygiène cybernétique à l'échelle de l'entreprise est l'une des mesures les plus simples et les plus efficaces. Cela comprend des éléments de base comme l'authentification multifactorielle, le stockage sécurisé des données et les mises à jour régulières des systèmes logiciels et matériels. La formation du personnel à la reconnaissance des tentatives d'hameçonnage et des activités suspectes joue également un rôle clé dans la prévention des violations.

Lorsqu'elles adoptent de nouvelles technologies, comme l'intelligence artificielle, les entreprises doivent se projeter sur le long terme. Trop souvent, les vulnérabilités sont intégrées aux systèmes parce que la sécurité a été pensée après coup. Faire appel à des professionnels

de la cybersécurité dès le début d'un nouveau projet technologique peut contribuer à garantir que ces outils sont intégrés au cadre de sécurité global.

La préparation implique également de disposer d'un plan robuste d'intervention en cas d'incident qui non seulement limite les dommages en cas de violation ou de panne du système, mais permet aussi à l'entreprise de se rétablir rapidement. Sans stratégies d'intervention appropriées, même des incidents mineurs peuvent causer des perturbations majeures.

À la recherche de conseils d'experts

Compte tenu de la complexité des cyber-risques, de nombreuses entreprises s'associent à des conseillers en risques cybernétiques de confiance pour bénéficier d'un soutien stratégique et pratique. Les conseillers peuvent aider à repérer les vulnérabilités, à concevoir des plans de gestion des risques et à préparer des stratégies d'intervention en cas d'incident.

Pour les entreprises moins matures, les conseillers peuvent aider à mettre en place des mesures de cybersécurité de base et à favoriser une culture de sensibilisation aux risques. Pour les entreprises plus avancées, un conseiller en risques cybernétiques peut aider à affiner les stratégies existantes. Un partenaire de confiance n'apporte pas seulement son expertise, mais peut également servir de

point de contrôle externe pour s'assurer que les stratégies d'une entreprise sont solides.

Les relations entre le conseiller et le client varient. Certaines entreprises font appel à des conseillers pour un soutien continu, tandis que d'autres les engagent pour des projets précis.

Une gestion intelligente des risques

L'assurance contre les cyber-risques est une couche de protection essentielle. Elle permet aux entreprises de mieux gérer leur bilan de risques, les aide à atteindre leurs objectifs de conformité et peut fournir un soutien financier pour remédier aux violations et autres incidents.

Une bonne police d'assurance contre les cyber-risques peut tout couvrir, des pertes d'exploitation et de l'extorsion aux risques liés aux principaux fournisseurs. Les conséquences financières d'une atteinte à la protection des données ou d'une panne du système peuvent être dévastatrices; l'assurance aide donc les entreprises à se rétablir en leur fournissant des ressources qui peuvent contribuer à la reconstruction. Elle donne aux entreprises un niveau de confiance supplémentaire dans leur gestion des risques potentiels.

Il est également important d'adapter les polices d'assurance aux besoins particuliers d'une entreprise. Les polices peuvent être personnalisées pour inclure une couverture des

risques propres pour les coûts d'intervention immédiate et une couverture envers les tiers pour la responsabilité envers les clients ou les partenaires.

Les cybermenaces ne suivent pas de calendrier; les entreprises doivent donc adopter un état d'esprit consistant à être « toujours en alerte ». En perfectionnant continuellement leurs stratégies de gestion des risques, les entreprises peuvent être mieux préparées aux menaces actuelles et émergentes.

Les risques cybernétiques ne relèvent pas seulement de la technique; ils sont un enjeu commercial. En promouvant une bonne hygiène cybernétique, en planifiant de façon responsable l'adoption de nouvelles technologies, en collaborant avec des conseillers de confiance et en souscrivant la bonne assurance, les entreprises peuvent élaborer une stratégie qui inspire confiance. Alors que les risques sont bien réels, les solutions potentielles sont à portée de main. Avec la bonne approche, les entreprises peuvent mieux sécuriser leur monde tous les jours de l'année.



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.



La présente publication est destinée à un usage informatif seulement. Elle ne doit pas être utilisée comme s'il s'agissait d'un conseil ou d'une opinion juridique sur des circonstances ou des faits en particulier. La disponibilité du programme de même que les garanties sont assujetties à des critères de souscription individuels.

© 2025 Gestionnaires d'assurance Victor inc. | 25-689300-CA