Résoudre le dilemme financier des cyber-risques.

Pourquoi une stratégie collaborative de cybersécurité et d'assurance est-elle essentielle?

Le monde d'aujourd'hui, dépendant du numérique, est caractérisé par des cybermenaces incessantes. Dans le même temps, les conditions macroéconomiques peuvent exercer une pression énorme sur les directeurs principaux pour qu'ils réduisent les risques tout en gérant des budgets restreints. Cela peut amener les directeurs principaux à réfléchir à l'opportunité d'investir dans des contrôles de cybersécurité ou de souscrire une assurance contre les cyber-risques.

Selon le rapport 2023 d'IBM, les entreprises canadiennes paient encore presque 7 millions de dollars canadiens en coûts de violation des données, se classant au troisième rang le plus élevé au monde.

Au lieu de choisir entre l'un ou l'autre, les organisations devraient trouver un équilibre grâce à une approche à deux volets en matière de cyberrésilience financièrement prudente. Cela consiste à investir dans des contrôles de cybersécurité tout en souscrivant une assurance adaptée à la tolérance au risque pour couvrir les pertes à la suite d'un incident cybernétique potentiel.

Les mesures combinées de cybersécurité et d'assurance offrent une meilleure protection

Il est essentiel que les organisations prennent des mesures qui peuvent les aider à atténuer et à gérer leurs cyber-risques et à améliorer leur capacité à se rétablir efficacement au cas où elles seraient touchées par un incident cybernétique.

Mais quelles mesures les organisations peuvent-elles prendre? Les actions nécessaires se répartissent en trois grandes catégories qui constituent la base de la gestion de risques : **1. Éviter et atténuer**; **2. Transférer**; et **3. Retenir**.

1. **Éviter et atténuer**
   Les programmes de cybersécurité aident les organisations en réduisant leur surface d'attaque, en se défendant contre les menaces, en sécurisant et en chiffrant les données, en segmentant ou en isolant les systèmes critiques et en limitant les accès privilégiés, pour n'en nommer que quelques-uns. Des programmes de cybersécurité robustes – et leur gouvernance – sont essentiels et ne sont plus facultatifs pour les sociétés ouvertes. Cependant, les budgets de cybersécurité sont souvent insuffisants pour couvrir les coûts non technologiques considérables nécessaires pour réagir et se remettre d'un incident cybernétique. En outre, la mise en place de contrôles nouveaux ou améliorés en matière de cybersécurité peut prendre des années, ce qui signifie que les investissements en matière de cybersécurité risquent de ne pas produire de bénéfices immédiats en matière de réduction des risques, laissant ainsi un vide que l'assurance pourrait contribuer à combler.

2. **Transférer**
   L'assurance contre les cyber-risques peut fournir une protection financière après un incident, en transférant une myriade de coûts associés aux pannes de système ou aux failles de sécurité du propre bilan d'une organisation. Essentiellement, ces programmes d'assurance peuvent couvrir les coûts non technologiques, y compris la responsabilité juridique potentielle envers des tiers, les coûts réglementaires, la perte de revenus, l'augmentation des coûts de marketing pour réduire la perte de clientèle et les coûts de mise en conformité aux lois sur la notification des violations. Le transfert de ces pertes permet de protéger le bilan et de préserver la santé financière.

3. **Retenir**

   Enfin, les organisations devraient évaluer, idéalement de manière quantitative, leurs risques cybernétiques ou technologiques importants. Cette analyse devrait évaluer comment les contrôles existants ou élargis pourraient réduire ce risque implicite, quels programmes de transfert sont optimaux en termes de couverture et d'efficacité, et enfin quantifier le risque résiduel qu'ils peuvent supporter sur leurs bilans.

   Une approche équilibrée est particulièrement importante dans un contexte de reconnaissance accrue du fait que même les contrôles de cybersécurité les plus avancés ne peuvent pas arrêter tous les acteurs de la menace ni atténuer toutes les erreurs humaines. En d'autres termes, les meilleurs contrôles ne suffisent peut-être pas. Des programmes de cybersécurité solides peuvent réduire la probabilité ou l'impact d'un incident cybernétique, mais ne sont jamais infaillibles. Lorsque des pertes surviennent, un programme d'assurance contre les cyber-risques adéquat offre un niveau de résilience supplémentaire pour aider les organisations à réagir et à se rétablir.

Près des trois quarts des violations de données incluent un élément humain. Les humains sont faillibles et un certain degré de cyber-risque est inévitable, ce qui souligne l'idée selon laquelle le risque ne peut jamais être complètement atténué.

Source: Rapport 2024 d'enquête sur les compromissions de données | Verizon

Cinq questions pour déterminer la valeur de l'assurance contre les cyber-risques

Compte tenu des enjeux, comment les organisations peuvent-elles prendre des décisions éclairées et financièrement prudentes en matière de gestion des cyber-risques, en particulier lorsque les experts en cybersécurité et les professionnels de la gestion de risques peuvent être en désaccord sur la manière d'allouer un budget limité entre les solutions de cybersécurité et les produits de transfert de risques? Pour aider à prendre des décisions objectives et éclairées, les directeurs principaux doivent réfléchir aux questions ci-dessous.

1. **Quelles sont mes exigences contractuelles?**

   Les organisations n'ont peut-être pas la possibilité de renoncer à l'assurance contre les cyber-risques, car celle-ci est souvent exigée par les prêteurs ou les clients. Par exemple, lorsqu'elles envisagent les implications potentielles d'un incident cybernétique sur les chaînes d'approvisionnement, de nombreuses organisations exigent que leurs fournisseurs et autres partenaires critiques souscrivent une couverture suffisante. Examinez vos contrats pour déterminer les limites d'assurance que vous devez souscrire.

2. **Combien coûterait un incident cybernétique à mon organisation?**

   Un incident cybernétique représente souvent une dépense non planifiée et des conséquences financières pour les organisations, alors qu'elles s'efforcent de déterminer et de faire cesser la menace, et également de se remettre de l'incident. Il faut non seulement tenir compte des coûts technologiques, mais également des autres frais de remise en état, y compris les frais juridiques potentiels et la responsabilité envers les tiers. L'organisation serait-elle en mesure de financer ces coûts sans impact important sur ses résultats financiers ou sans besoin d'obtenir un financement supplémentaire?

3. Que couvre l'assurance contre les cyber-risques?

Parlez avec votre courtier d'assurance pour clarifier toute idée fausse sur l'assurance contre les cyber-risques et mieux comprendre ce qui est généralement couvert. Votre courtier devrait être en mesure de clarifier les services que l'assurance contre les cyber-risques paie généralement à la suite d'une violation, tels que les coûts engagés pour informer les clients ou les régulateurs, et qui devraient être absorbés par votre organisation en l'absence de couverture.

4. Combien coûte une assurance contre les cyber-risques?

Il existe souvent des idées fausses concernant le coût des limites de l'assurance contre les cyber-risques suffisantes. Bien que l'assurance puisse paraître coûteuse, l'achat d'un programme avec des limites adéquates pour couvrir les dépenses consécutives à une violation ne représente souvent qu'une fraction des coûts associés au rétablissement. Notez également que les économies réalisées grâce à une couverture moindre peuvent ne pas être suffisantes pour permettre à une organisation d'apporter des améliorations significatives et rapides à sa posture de cybersécurité.

5. La proposition d'assurance contre les cyber-risques est-elle trop chronophage?

Grandes entreprises
Même si certaines propositions d'assurance contre les cyber-risques peuvent prendre beaucoup de temps à remplir pour les grandes entreprises, les informations détaillées généralement requises sont souvent déjà disponibles. Les propositions d'assurance contre les cyber-risques sont généralement adaptées aux autres demandes de données des clients, des prêteurs ou autres. De plus, même s'il peut s'avérer laborieux de rassembler les données la première fois, cela devient généralement plus facile lors des renouvellements ultérieurs. Votre courtier d'assurance pourra peut-être vous aider à répondre aux questions et à fournir aux assureurs tous les renseignements pertinents pour faciliter le processus de la demande d'assurance.

Petites et moyennes entreprises
Des propositions d'assurance contre les cyber-risques longues et complexes peuvent être intimidantes - en particulier pour les petites et moyennes entreprises qui n'ont pas beaucoup de temps et de ressources à consacrer pour remplir ces formulaires. C'est pourquoi nous avons créé une proposition rapide et facile pour l'assurance contre les cyber-risques de Victor, en pensant à ces entreprises!

Une nouvelle proposition simplifiée est disponible pour les petites et moyennes entreprises qui souhaitent souscrire une assurance contre les cyber-risques de Victor. Cette assurance offre des prix compétitifs, une couverture étendue et est unique sur le marché car elle aide à prévenir les cyberattaques et à s'en protéger.

Contactez votre courtier d'assurance pour plus d'informations ou visitez www.assurancevictor.ca/cyber.

Visitez assurancevictor.ca/cyber pour en apprendre davantage.

Le présent document a été publié uniquement à des fins illustratives et ne constitue pas un contrat d'assurance. Il a été conçu pour fournir un aperçu global du programme. Seule la police d'assurance peut fournir les modalités, la garantie, les montants, les conditions et les exclusions réels. La disponibilité du programme de même que les garanties sont assujetties à des critères de souscription individuels.

© 2025 Gestionnaires d'assurance Victor inc. | 24-327750-CA