Solving the cyber risk financial dilemma.

Why is a collaborative cybersecurity and insurance strategy critical?

Today's digital-dependent world consists of unrelenting cyberthreats. At the same time, macroeconomic conditions may place senior leaders under enormous pressure to reduce risk while managing constricted budgets. This can lead to senior leaders considering whether to invest in cybersecurity controls or purchase cyber insurance coverage.

Instead of an either-or choice, organizations should strike a balance through a two-pronged approach to financially prudent cyber resiliency. This consists of investing in cybersecurity controls while purchasing insurance that aligns with risk tolerance to cover losses following a potential cyber incident.

According to a 2023 IBM report, Canadian companies are still paying nearly 7 million dollars (CAD) in data breach costs, the third highest in the world.

Combined cybersecurity measures and insurance provide improved protection

It is critical for organizations to take actions that can help them mitigate and manage their cyber risk and improve their ability to effectively recover in case they are impacted by a cyber event.

But what steps can organizations take? The needed actions fall into three broad categories that make up the basis of risk management: **1. Avoid and mitigate; 2. Transfer;** and **3: Retain**.

1. **Avoid and mitigate**

   Cybersecurity programs help organizations by reducing their attack surface, defending against threats, securing and encrypting data, segmenting or isolating critical systems, and limiting privileged access, to name a few. Robust cybersecurity programs — and their governance — are critical, and for public companies no longer optional. However, cybersecurity budgets are often insufficient to cover the considerable non-technology costs needed to respond and recover from a cyber incident.

Additionally, putting new or enhanced cybersecurity controls into place may take years, meaning that cybersecurity investments may not yield immediate risk reduction benefits, leaving a gap that insurance could help cover.

2. **Transfer**

   Cyber insurance can provide post-incident financial protection, by transferring myriad costs associated with system failures or security breaches off an organization's own balance sheet. Crucially, these insurance programs can cover non-technology costs, including potential legal liability to third parties, regulatory costs, lost income, increased marketing costs to stem customer attrition, and costs to comply with breach notification laws. Transferring these losses helps protect the balance sheet and preserve financial health.

3. **Retain**

   Finally, organizations should evaluate, ideally quantitatively, their material cyber or technology risks. This analysis should assess how existing or expanded controls might decrease that implicit risk, what transfer programs are optimal in coverage and efficiency, and finally quantify the residual risk they can bear on their balance sheets.

   A balanced approach is particularly important amidst increased recognition that even the most advanced cybersecurity controls may not stop all threat actors or mitigate all human error. Simply put, the best controls may not be enough. Strong cybersecurity programs may reduce the likelihood or impact of a cyber event but are never event proof. When losses do occur, an adequate cyber insurance program provides yet another layer of resiliency to help organizations respond and recover.

Nearly three-quarters of data breaches include a human element. Humans are fallible and some degree of cyber risk is inevitable, underscoring the idea that risk can never be completely mitigated.

Source: 2024 Data Breach Investigations Report | Verizon

Five questions to determine the value of cyber coverage

Considering what's at stake, how can organizations make informed, financially prudent cyber risk management decisions, especially when cybersecurity experts and risk management professionals may disagree on how to allocate limited budget between cybersecurity solutions and risk transfer products? To help make objective, informed decisions, senior leaders should consider the questions below.

1. **What are my contractual requirements?**

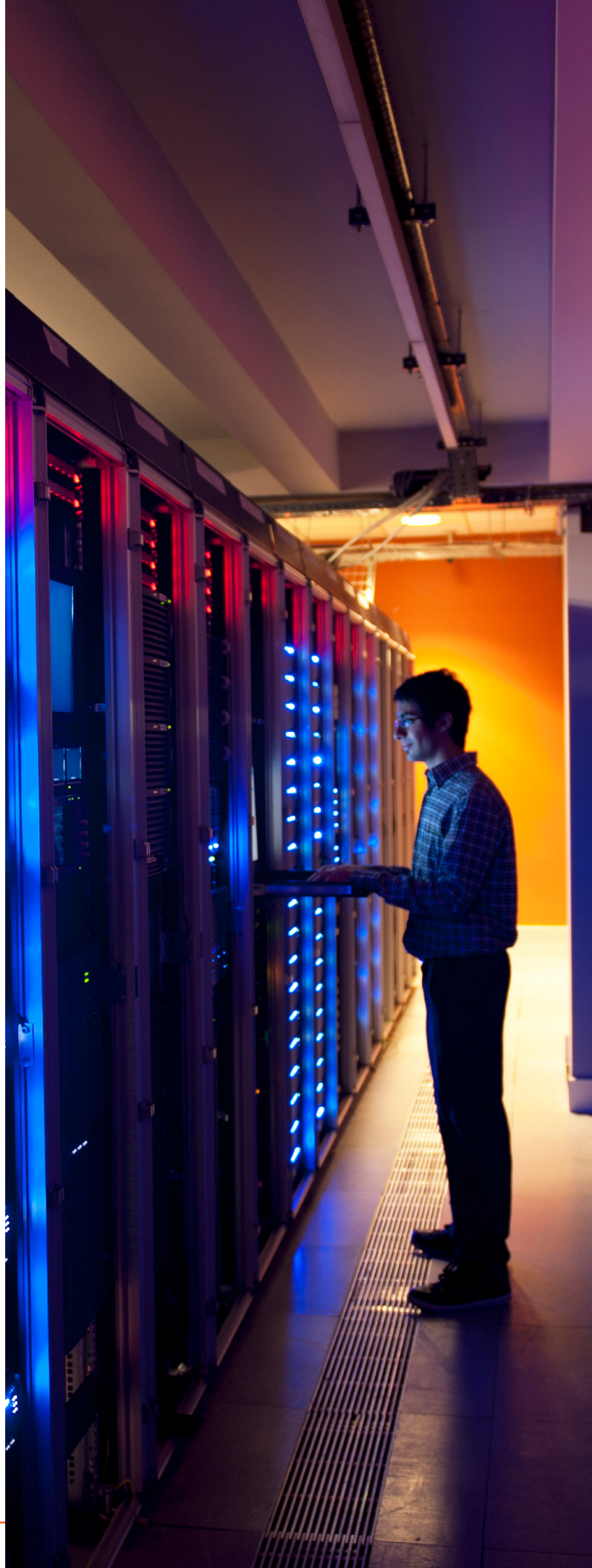
   Organizations may not have the option to forfeit cyber coverage as it is often required by lenders or clients. For instance, when considering the potential implications of a cyber incident on supply chains, many organizations are requiring that their vendors and other critical partners purchase sufficient coverage. Examine your contracts to determine the insurance limits that you are required to purchase.

2. **How much would a cyber incident cost my organization?**

   A cyber event is often an unbudgeted expense for organizations, with financial ramifications as organizations work to identify and stop the threat, and also recover from the event. Consider not only technology costs, but also other remediation expenses, including potential legal costs and third party liability. Would the organization be able to fund these costs without material impact to its financial results or without the need to secure additional funding?

3. **What does cyber insurance cover?**

   Work with your insurance broker to clarify any misconceptions about cyber insurance and gain a clear understanding of what is typically covered. Your broker should be able to clarify the services that cyber insurance typically pays for following a breach, such as costs incurred to notify clients or regulators, and which would need to be absorbed by your organization in the absence of coverage.



4. How much does cyber insurance cost?

There are often misconceptions associated with the cost of sufficient cyber insurance limits. While insurance can appear expensive, purchasing a program with adequate limits to cover expenses following a breach is often a fraction of the costs associated with recovery. Also note that the cost savings from obtaining less coverage may not be sufficient to allow an organization to make significant and speedy improvements to its cybersecurity posture.

5. Is the cyber insurance application too time-consuming?

Large corporations

While some cyber insurance applications can be time-consuming to complete for large corporations, the detailed information that is typically required is often already available. Cyber insurance applications are typically commensurate with other data requests from clients, lenders or others. Further, although it can be laborious to gather the data the first time around, this typically gets easier in subsequent renewals. Your insurance broker may be able to guide you on how to answer the questions and provide insurers with all relevant information to facilitate the application process.

Small to medium-sized businesses

Complex and lengthy cyber insurance applications can be intimidating—especially for small to medium-sized firms that don't have a lot of time and resources to dedicate in completing such forms. That's why we created a quick and easy Victor Cyber insurance application with these firms in mind!

A new, simplified application is available for small to medium-sized firms seeking Victor Cyber insurance for their business. Victor Cyber provides competitive pricing, broad coverage—and is unique in the marketplace as it helps both prevent and protect against cyberattacks.

Reach out to your insurance broker for more information or visit www.victorinsurance.ca/cyber.

Visit us at victorinsurance.ca/cyber to learn more.