
VICTOR
Always on:
Preparing for the
future of cyber risk

Why a holistic cyber risk strategy is essential to protect your organization.

Cybersecurity is essential, but it's only part of the equation. Here's why a holistic cyber risk strategy is essential to protect your organization.

Securing our world requires more than just technical measures. The risks organizations face today are continuous, evolving and far-reaching, demanding constant vigilance.

While technical defenses — like firewalls, anti-malware systems and encryption protocols — are essential, cyber risk goes beyond cybersecurity. It encompasses everything from security controls to internal vulnerabilities, organizational readiness and resilience. Yet too few organizations give cyber risk the priority it requires.

Now is the perfect time to build on its foundations by creating a comprehensive plan that addresses cybersecurity as part of the broader topic of cyber risk — a vital business risk that must be managed with a multi-pronged insurance, mitigation and resilience approach.

Taking a holistic view

Too often, organizations rely entirely on technical defenses to keep their data safe. For example, a company might have state-of-the-art cybersecurity tools to protect against breaches or system failures but lack a clear incident response plan that assigns roles and responsibilities for when one happens, leading to avoidable business disruptions. It's like preparing for a natural disaster — recovery is just as important as prevention.

Effective cyber risk management takes a holistic view, addressing everything from security controls to human behavior, which may be the weakest link. Human error remains a significant cause of cyber incidents, but it can be reduced with regular internal training and by fostering a culture of cyber awareness. Organizations that broaden their focus are better positioned to mitigate the fallout from a cyber event.

Resilience and response

Managing cyber risk effectively requires a proactive, multi-layered approach. Promoting good cyber hygiene across the organization is one of the simplest yet most effective measures. This includes basics like multi-factor authentication, secure data storage, and regular updates to software and hardware systems. Training staff to recognize phishing attempts and suspicious activity also plays a key role in preventing breaches.

When adopting new technologies, such as artificial intelligence, organizations must take a long-term view. Too often, vulnerabilities are embedded in systems because security was an afterthought. Involving cybersecurity professionals from the start of a new technology project may help ensure that these tools are integrated into the overall security framework.

Preparedness also means having a robust incident response plan that not only contains damage during a breach or system failure but ensures the business can recover quickly too. Without proper response strategies, even minor incidents can cause major disruptions.

Seeking expert advice

Given the complexity of cyber risk, many organizations partner with trusted cyber risk advisors for strategic and practical support. Advisors can help identify vulnerabilities, design risk management plans and prepare incident response strategies.

For less mature organizations, advisors can help establish basic cybersecurity measures and foster a culture of risk awareness. For more advanced companies, a cyber risk advisor can help refine existing strategies. A trusted partner doesn't just bring expertise but may act as an external checkpoint to ensure a company's strategies are robust.

Advisor-client relationships vary. Some organizations retain advisors for ongoing support, while others engage them for specific projects.

Smart risk management

Cyber insurance is a vital layer of protection. It allows organizations to better manage their risk balance sheet, helps with compliance targets, and may provide financial support for breach and other incident remediation.

A good cyber insurance policy can cover everything from business interruption and extortion to risks stemming from key suppliers. The financial impact of a data breach or system failure can be crippling, so insurance helps organizations recover by providing resources that may help rebuild. It gives businesses an extra level of confidence that they are managing potential risks.

It's also important to tailor insurance policies to an organization's specific needs. Policies can be customized to include first party coverage for immediate response costs and third party coverage for liability to customers or partners.

Cyberthreats don't follow a calendar, so organizations must adopt an always-on mindset. By continuously refining their risk management strategies, businesses can be better prepared for current and emerging threats.

Cyber risk is not just a technical problem; it's a business problem. By promoting good cyber hygiene, planning for new technologies responsibly, partnering with trusted advisors and securing the right insurance, organizations can build a strategy that instills confidence. While the risks are real, potential solutions are within reach. With the right approach, businesses can better secure their world every day of the year.

Help protect your organization with Victor Cyber

Cyberattacks are a real and growing threat for organizations of all sizes. That's where Victor Cyber comes in. It's a full insurance package with competitively priced coverage against data breaches, ransomware attacks and business interruption. In addition, with Victor Cyber, organizations have access to free risk management services—such as phishing simulations and dark web monitoring—through our Victor Response mobile app #TheThreatIsReal

For more information about Victor Cyber, contact your insurance broker and visit: www.victorinsurance.ca/cyber.