
VICTOR
Five tips on building cyber risk resilience

The cyber risk environment has become immeasurably more complicated and significant for organizations. Ever-changing and more potentially costly cybersecurity threats are keeping the issue high on the list of organizations' concerns And it's moved from an information technology (IT) department issue to one that makes, and even drives, the agenda at board meetings.

This underscores how vital it is that organizations prepare now to secure their futures. Cyber risks can be critical business disruptors, as they can crop up anywhere in the supply chain – even several layers down. While there isn't a silver bullet to managing these risks, putting in place even basic cybersecurity controls and the right best practices, and ensuring they are maintained, can markedly improve your cyber resilience.

TIP #1: FOCUS ON THE BASICS—CYBERSECURITY CONTROLS

Cyber risk resilience is making good progress. That's largely due to organizations focusing on the basics—prioritizing and implementing effective and robust cybersecurity controls.

These controls can include measures such as strong access controls, regular software updates, encryption of sensitive data and multi-factor authentication.

Such incremental improvements quickly add up and can significantly reduce the risk of cyberattacks and breaches—even from sophisticated attackers.

TIP #2: UNDERSTAND EVOLVING CYBER OPPORTUNITIES AND THREATS

Cyberthreats evolve as new technology is deployed and malicious actors adapt their tactics.

Currently, artificial intelligence (AI) is a source of both optimism and concern. Many organizations are exploring the use of AI tools to bolster their cyber defenses, for example by filtering the flood of alerts they generate so the most urgent are sent to a human analyst. However, there is also concern about attackers using AI to find weaknesses or even write malicious code.

Supply chain and third party risks are another topic climbing the agenda. Even organizations with their own secure and well-managed systems often don't know how secure their third parties are, let alone fourth parties, and others even further down the chain. A compromised third party can cause disruption by making a supplier unavailable and by opening a route for attackers to infiltrate connected organizations.

Supply chain risk also extends to matters such as privacy. Third parties often handle sensitive data that, if exposed, could have consequences including reputational damage and regulatory sanctions, such as those under the General Data Protection Regulation (GDPR) in Europe.

TIP #3: BUILD TOWARD GREATER CYBER RESILIENCE

These initial steps toward managing and understanding evolving and complex cyberthreats can provide a better perspective into your cyber risk environment.

To further build up resilience, you need to assess and measure your organization's cyber risk appetite. Key questions to ask yourself include:

- Which assets and services are mission critical and must absolutely be protected?
- What would it cost—in money, time and reputational damage—if exposed or disrupted?

With this in mind, you can decide what steps are reasonable to protect your organization's digital footprint.

You also can decide what it would take to recover efficiently and effectively.

- Focus on ways to recover mission critical operations in the event of a disruption.
- Use tabletop exercises, vendor assessments and case studies to help determine what the right defense and recovery measures should be.
- Establish robust processes and policies, so that everyone knows what they should be doing day-to-day and when a crisis materializes.

Finally, build this into a plan for recovering from an incident—and test it regularly.

TIP #4: LEVERAGE KEY RESOURCES FOR IMPROVEMENTS

Security improvements need not be expensive. There are plenty of resources available to help.

Organizations should make use of internal experts and ensure they are involved in the planning of new cybersecurity platforms and cyber risk responses.

Knowledgeable partners can help too. For instance, some partners can offer a product team, modeling team, advisory team and cyber risk database. This database can be turned into insights, risk mitigation and finance options, and solutions that allow you to understand, measure and manage your cyber risks.

There are further resources available from governments and international bodies, which often publish standards and checklists that can be cost-effectively applied to secure your organization's cyber risk environment.

For Canadian resources, consider visiting the Government of Canada's Canadian Centre for Cyber Security which offers guidance, advice and information on potential cyber risks, and how both individuals and organizations can stay safe online.

Additionally, the Office of the Privacy Commissioner of Canada (OPC) provides resources on protecting personal data and privacy.

Organizations can also connect with informal networks, such as peer organizations and trade bodies. These can often help with sharing best practice and offering warnings of emerging risks.

TIP #5: MAINTAIN BEST PRACTICES ALL YEAR LONG

In the ever-changing landscape of cyberthreats, there is no finish line.

It is essential not to overlook the importance of maintaining your best cyber risk resilience practices and using threat intelligence to stay ahead of potential risks.

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.