KPMG

Cyber watch report

Be in a defensible position.
Be cyber resilient.

The cyber threat landscape is highly irregular and ever-changing.

Five key trends affecting Canadian organizations

Canadian businesses and public organizations realize their crown jewels are essential assets that are targets for threat actors ranging from individual hackers to criminal groups and state-sponsored players. To be in a cyber defensible position, organizations need to take a proactive and comprehensive approach to cyber risk management - one that protects, detects and responds to new adversaries and tactics. Below are the five key trends we see that apply to Canadian organizations, based on industry intelligence and interactions with clients.

1

Extortion-driven attacks and ransomware attempts will increase.

Threat actors employ ransomware to infiltrate and encrypt files, devices and networks, then demand payment for their release. Alternatively, organizations can fall prey to proactive ransom attacks in which no breach has occurred, but cyber criminals threaten to disrupt systems, operations and steal data if online payment is not made. Even data that has been backed up can be infected and rendered useless, and the latest ransomware encrypts websites.

Other forms of attack include "shameware": viruses that use laptop cameras and microphones to record behaviour, with perpetrators hoping to find details that can be used for blackmail.

KPMG expects ransomware and extortion-driven attacks to increase in Canada, particularly within the public, legal and financial services sectors, given the private and sensitive nature of the information these organizations hold. As with many cyber security threats, small and medium-sized enterprises with fewer IT resources and potentially fewer safeguards in place may be especially vulnerable. The prevalence and complexity of extortion-driven attacks are increasing rapidly.

KPMG's defensible position: Companies must protect their assets, operations and reputation by employing a back-up strategy and conducting regular employee awareness campaigns. Most ransomware spreads via emails with contagious attachments or bad hyperlinks, so it is imperative to educate employees. A dedicated clean machine should be used to periodically check backups. If data has been properly backed up, recovery consists of removing the ransomware and transferring data from the backup storage. Establish a good response process, know whether your organization is prepared to pay a ransom, and consider the legal risks.

2 Pressure to disclose breaches and threat responses in a timely manner will intensify.

Consumers, governments, privacy commissioners and courts will increasingly pressure Canadian entities to be more transparent about their cyber security readiness, responsiveness and breach notification protocol.

In 2015, Canada amended the federal Personal Information Protection and Electronic Documents Act (PIPEDA) in response to increased privacy breaches. KPMG anticipates an increase in breach management and notification costs in 2016 due to the Digital Privacy Act's mandatory breach notification requirement. This act will require organizations to notify affected consumers about security breaches that pose a risk of significant harm.

Europe's new data privacy law, General Data Protection Regulation, brings in wide-ranging rules including a requirement to notify customers within 72 hours of a breach involving data that is not encrypted. This law applies to Canadian firms operating in Europe, with fines for non-compliance ranging from 2% to 5% of global revenues.

KPMG's defensible position: Canadian companies that operate across borders must stay on top of evolving regulatory, legislative and contractual/commercial requirements. These vary from province to province, state to state and country to country. Suppliers, partners and consumers as well as regulators and governments are increasing their focus on data security, privacy and incident notification/response. Organizations must be proactive to ensure they comply with laws and preserve their reputation and trust with customers.

3 Widespread use of mobile devices and adoption of the Internet of Things (IoT) brings a parallel increase in risk.

As mobile devices and "smart" devices connected to the Internet become dominant in Canadian society and in the workplace, they will naturally be prime targets for attacks. Vulnerabilities were discovered in mainstream mobile platforms in 2015 and organizations are now spending more resources on mobile device management.

Meanwhile, IoT devices are expected to play a huge role in managing our houses, appliances, vehicles, personal data and public infrastructure. As more players, service providers and third-party suppliers become part of the mobile and IoT ecosystem, and as tech firms rush to be first to market, these parties may not have completed sufficient security testing.

In the absence of generally accepted security standards for these devices, Canadians will start to demand assurances that all suppliers have suitable security and privacy policies and safeguards in place.

KPMG's defensible position: Companies should conduct regular threat and vulnerability testing, and stay abreast of developments and evolving standards for mobile and IoT data security to avoid costly or disruptive surprises down the road. It is much more cost effective to be secure by design. Retrofitting systems for security typically costs 30 to 35 times more than the cost if security had been built in from the start.

4 Organizations will make greater use of real-time intelligence tools to monitor live attacks.

Global cyber threats can happen at lightning speed, 24 hours a day. Customers expect security, privacy, and trust assurances around their information, and attacks can quickly cripple an organization's operations and reputation. It is imperative to detect threats as early as possible, and disarm them proactively.

We believe Canadian organizations will make increasing use of real-time intelligence tools because speed is of the essence. Organizations are also making use of behavioral analytics to help identify potential attacks from inside, and using informal threat intelligence networks, such as peer groups, to share information about issues, vulnerabilities and remediation actions.

KPMG's defensible position: Real-time intelligence solutions give organizations visibility into global cyber threats as they happen to help block attacks, uncover hidden breaches and track emerging threats. Organizations must integrate threat intelligence into incident response and work with their threat intelligence vendor to assess whether the intelligence is actionable. A combination of protection, early warning signals and instant remediation against sophisticated attacks is a proactive stance.

5 Organizations will focus much more on risks posed by third-party vendors and suppliers.

The threat surface of every organization has increased. There is no longer a clear delineation between "internal" and "external" threats. Even large, well-secured organizations are at risk if attackers can steal information or obtain corporate network access through smaller, less-secure vendors, suppliers and contractors. Businesses and individuals store reams of confidential business and personal data in the cloud, making cloud service providers increasingly attractive targets for cyber criminals.

As Canadians begin to demand security, privacy, and trust assurances, organizations will need assurances that their third-party suppliers have suitable policies and safeguards in place to prevent cyber incidents. They will also seek assurance that cloud providers are updating their security maturity as appropriate, based on the latest threats, vulnerabilities and tools.

KPMG's defensible position:
A customized evaluation that combines threat intelligence with specific testing can provide a realistic picture of an organization's security posture, including gaps with third-party vendors and suppliers. Cyber intelligence management providers can help assess third parties by providing real-time visibility of global cyber attacks. Organizations can also turn to remote process monitoring or audits and accreditation to assess the security standards of their vendors.

Be in a defensible position. Be cyber resilient.

Canadian organizations are challenged by the complexity of the shifting cyber security landscape, but awareness of risks and obligations at senior levels is growing. In 2016, we expect boards, audit committees, executives and public officials to ask more pointed questions to ascertain whether their organization is in a defensible position. Oversight is a key component of a defensible position, so proper metrics and oversight should be in place for audit committees and boards.

To become cyber resilient, companies need to get a clear view of their specific cyber security risks and probable impacts, assess and prioritize enterprise improvement activities, and ensure current risk assessments, budgets and IT initiatives are appropriate. Cyber security is not a debate about IT issues, however. It should be a business-led discussion about protecting corporate value.

KPMG's Cyber Team works with organizations to help prevent, detect and respond to cyber threats.

We can help your organization be cyber resilient in the face of challenging conditions.

Contact us

Alberta
Jeff Thomas
T: 403 691 8012
E: jwthomas@kpmg.ca

Atlantic Provinces
Louie Velocci
T: 902 492 6012
E: lvelocci@kpmg.ca

British Columbia
Shaun Wilson
T: 604 6913188
E: shwilson@kpmg.ca

British Columbia
Erik Berg
T: 604 6913245
E: erikberg@kpmg.ca

Ontario
Kevvie Fowler
T: 416 777 3742
E: kevviefowler@kpmg.ca

Ontario
Paul Hanley
T: 416 777 8501
E: pwhanley@kpmg.ca

Québec
Francis Beaudoin
T: 514 840 2247
E: fbeaudoin@kpmg.ca