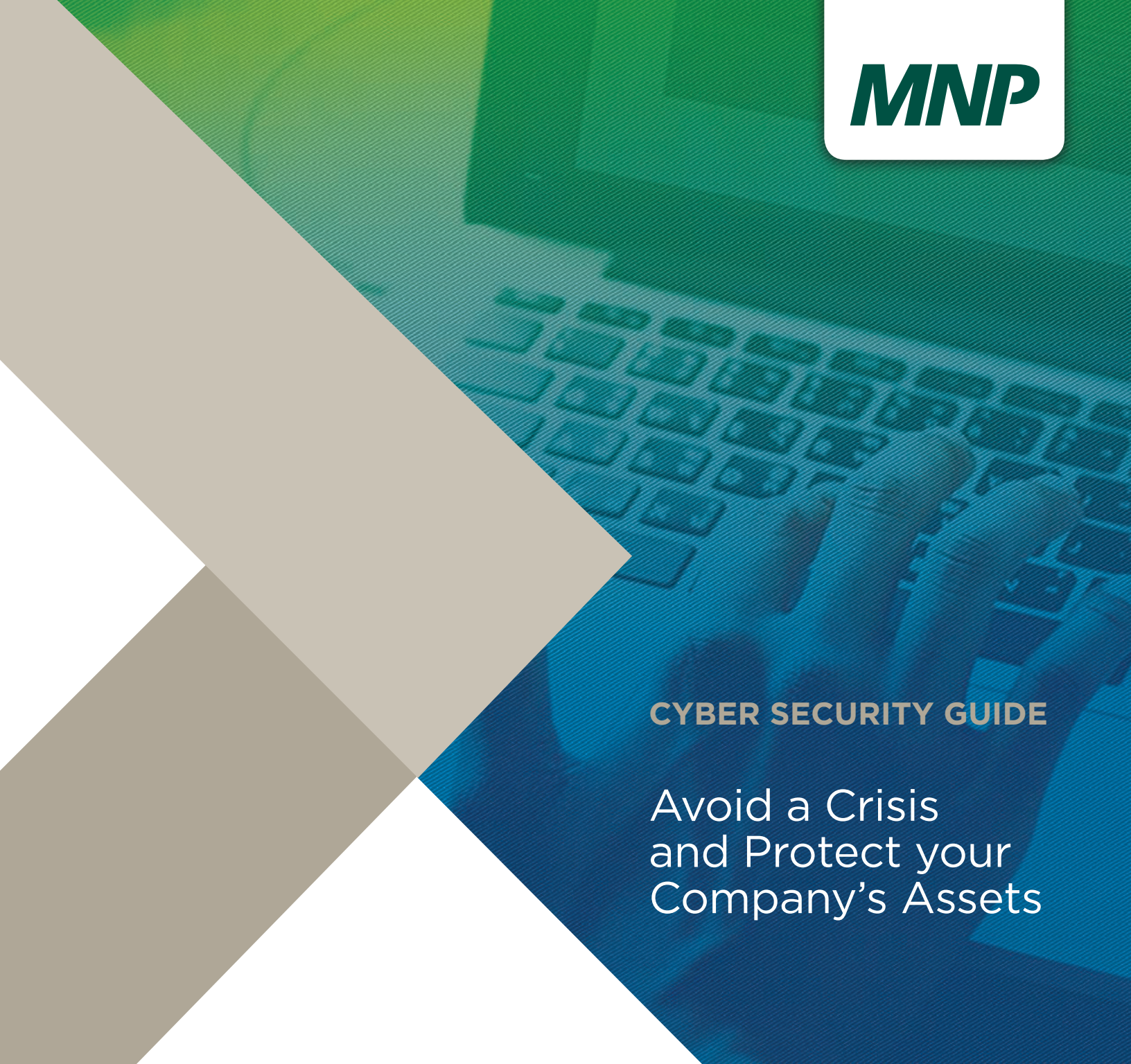

MNP

CYBER SECURITY GUIDE

Avoid a Crisis and Protect your Company's Assets

IN AN **INCREASINGLY CONNECTED** WORLD, **SECURITY** HAS BECOME AN **URGENT ISSUE** FOR VIRTUALLY **EVERY COMPANY.**

IT SEEMS THAT THERE ARE WEEKLY HEADLINES ABOUT HACKERS BRINGING AN ORGANIZATION TO ITS KNEES. THE STOLEN FUNDS, BAD PUBLICITY, AND EMBARRASSING REVELATIONS ARE FRONT PAGE NEWS. WITHOUT ADEQUATE PROTECTION, CYBER SECURITY THREATS CAN PUT AN ORGANIZATION'S OPERATIONS, REPUTATION – EVEN ITS EXISTENCE – AT RISK.

WHEN SHOULD YOUR ORGANIZATION BE THINKING ABOUT CYBER SECURITY?

When you want to become a key supplier for another organization

When you want to obtain financing

When you want to orchestrate a merger, sale or acquisition

When you want to meet compliance requirements (ISO, IIROC, PCI, etc.)

When you manage sensitive and personal information

When you have created and want to protect Intellectual Property (IP) and trade secrets

BOTTOM LINE: WHEN YOU WANT TO MAKE MONEY, SAVE MONEY AND MITIGATE RISK.

Vigilant cyber security assessment, planning, monitoring and response are now critical to protect the bottom line. In this MNP Cyber Security Guide, we explain why and set out a strategy for action.

THE **DANGER** TO BUSINESSES AND THEIR CUSTOMERS FROM **CYBER ATTACKS** AND **DATA BREACHES** HAS BECOME PERVASIVE. THE NEW WORLD REALITY IS **"ADVANCED PERSISTENT THREATS"** – COORDINATED CYBER CRIMINAL EFFORTS USING **HIGHLY ADVANCED TECHNIQUES**.

THE EVOLVING CYBER THREAT LANDSCAPE

COMMON TYPES OF CYBER ATTACKS

PHISHING – attackers send emails with the intent of tricking users into disclosing personal or business information by opening an attachment with malicious code or clicking on a link to a false website. "Whaling" is a type of phishing that targets "big fish" such as C-suite executives. Such tactics rely on social engineering: exploiting people's natural inclination to trust others so they reveal confidential information.

MALWARE — malicious software such as spyware, ransomware, worms, viruses and Trojan horses is embedded in networks or devices, causing damage to files.

RANSOM ATTACKS – criminals threaten to launch a Distributed Denial of Service (DDoS) attack, which disrupts company systems or networks by denying service to users unless the organization pays a ransom fee. Or they infect a network with ransomware that encrypts files, then demand a ransom fee to unlock the files.

COMPROMISED CREDENTIALS — thieves access a company's network through usernames and passwords and then sell personal information on the "underground" Internet.

SQL INJECTIONS — hackers access corporate databases by inserting malicious code into Structured Query Language (which manages information in databases), bypassing firewalls and other security measures.

Not only is the threat of cyber attack rising but so is the damage they cause. A 2016 Cost of Data Breach Study found that it took Canadian companies more than five months to detect that a breach occurred and nearly two months to contain the incident.

Poor security and incident response planning can lead to painful, even catastrophic, financial and reputational losses: remediation, disruption to operations, lost productivity, damage to information assets, infrastructure, reputation and brand, and sometimes litigation.

Moreover, large companies are not the only organizations cyber criminals attack. Studies show that victims are increasingly targeting small businesses – sometimes used as conduits to strikes on larger targets. Last year, about half of worldwide Internet attacks were against small enterprises with less than 250 employees.

The security breaches at Target and Home Depot a couple of years ago, for example, were carried out by criminals who secured credentials and security access from third-party vendors. The resulting data breaches affected over 100 million customers in the US and Canada.

Data breaches and security incidents increasingly put not just individual companies but entire supply chains at risk. From vendors, manufacturers, contractors, distributors and resellers to customers, every member of the supply chain is only as strong as the weakest link when it comes cyber crime vulnerability.

Organizations need to build a strong security posture by implementing strategies that address threats across the entire chain. Doing so also provides an opportunity to improve risk management, provide better service and reduce costs.

HOW NEW LEGISLATION WILL IMPACT YOUR ORGANIZATION

Business leaders should prepare for the new normal. Cyber security laws and regulations are being introduced in Canada and worldwide that will impact organizations of every type and size.

Governments and the private sector are increasingly working together to respond to cyber risks. In some cases they are taking direct action to secure public and private networks and systems. In other instances they are encouraging the development of voluntary frameworks and best practices.

The Government of Canada recently finished public consultations related to protecting Canadians and critical infrastructure from cyber threats. Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. These consultations will inform the government's coming cyber security policies and programs. It is also establishing cross-sector mechanisms to promote sharing of threats and defensive techniques.

The scope of cyber crime in Canada has been difficult to measure given the absence of mandatory data breach notification requirements under Canada's privacy laws (with the exception of Alberta). Until now. The new Digital Privacy Act, which was adopted in June 2015, has introduced into Canada's private sector privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA), mandatory breach notification where an incident results in significant harm, as well as major fines for failing to do so.

BREACH NOTIFICATION REQUIREMENTS UNDER THE DIGITAL PRIVACY ACT

When an organization possesses personal information that is lost or stolen it must notify the individuals involved if they have been put at "real risk of significant harm" as a result. This includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss and identity theft. When assessing risk, organizations need to consider the sensitivity of the information and the probability it may be misused.

The company must also notify the Office of the Privacy Commissioner of Canada (OPC) and any third parties (such a financial institution or a law enforcement agency) if they may be able to assist in reducing risk or mitigating harm.

Companies are also required to maintain a record of all potentially harmful breaches involving personal information and be prepared to provide a copy to the OPC upon request.

Breach reporting is currently voluntary until the provisions come into force, likely in 2017. At that time, fines can be levied for failing to meet these requirements – up to $100,000 per offence.

Before breach notification regulations come into force, management teams should review privacy policies and security safeguards. Since violations could lead to costly fines, appropriate policies and procedures should be in place to detect and respond to privacy incidents. As well, legal strategies may be required since mandatory notifications could increase the risk of litigation and class actions.

WHY YOUR COMPANY NEEDS A STRONG SECURITY POSTURE

In addition to the upcoming changes to PIPEDA, there are other factors driving the need for business leaders to immediately establish a strong "security posture" for their companies. This refers to the overall security approach, from planning to implementation, which management takes to protect an enterprise from internal and external threats.

40 THE AVERAGE NUMBER OF CYBER ATTACKS ORGANIZATIONS IN CANADA EXPERIENCE EVERY YEAR

26% THE PROBABILITY OF A BREACH HAPPENING TO YOUR COMPANY IN THE NEXT 24 MONTHS

$4M THE AVERAGE TOTAL COST OF ONE BREACH

A strong security posture has become a fundamental requirement of operating a business. Not only is it necessary to address the direct risk of cyber attack, organizations are now also seeking to ensure that the third parties with which they do business meet acceptable standards of security.

They are using tools such as security questionnaires and audits, and in the US, obtaining scores from new security ratings services, patterned after credit ratings agencies. Some companies now require vendors with access to sensitive information to carry cyber insurance.

More government entities, financial institutions, insurers, and potential investors, customers and partners are requiring cyber security reassurances from associated parties to ensure they do not put their own assets at risk. They are using such tools as security questionnaires and audits, and in the US, obtaining scores from new security ratings services, patterned after credit ratings agencies. Some companies now require vendors with access to sensitive information to carry cyber insurance.

There are also new standards that businesses are expected to meet such as the cyber security framework of the National Institute of Standards and Technology (NIST). At the international level, there is growing demand for ISO 27001 certification, the principal information security standard.

SIX STEPS TO AVOID A SECURITY CRISIS AND PROTECT YOUR ASSETS

While the cyber landscape is complex and continually evolving, by taking a few decisive steps, management teams can build a robust security posture that supports business goals and resilience.

Start from the premise that systems will be breached. This perspective influences the decisions you will make related to preventing, mitigating and recovering from a breach.

Adopt the attitude that security is security. Whether physical or cyber, there is no difference when it comes to potential for attack. Cyber assaults can be launched by exploiting lapses in physical security and vice versa – an attacker can exploit cyber vulnerabilities to access a physical location.

Know that cyber security is not solely a technology issue. Breaches are more often caused by human error than technology failure. Addressing enterprise security requires addressing the full spectrum of risks across the organization – those from people, processes and technology. At the heart must be effective governance to manage the combined impact of those risks.

1 **MAKE MANAGEMENT OVERSIGHT OF SECURITY A PRIORITY.** Governance should encourage a culture of continuous risk management and oversee an enterprise security strategy aligned with business objectives.

2 **ENSURE TOP-DOWN, ORGANIZATION-WIDE REPORTING AND COMMUNICATION.** All business units need to work together and communicate the organization's compliance and risk management efforts. A cross-organizational team that meets regularly to coordinate security issues encourages everyone in the organization to take ownership.

3 **EDUCATE EVERY EMPLOYEE.** Lack of employee awareness can be the most significant threat to company security. Every employee needs to understand their responsibilities for security. This requires ongoing training regarding how to protect the information and other assets with which they are entrusted.

4 **SCRUTINIZE THE SECURITY POSTURE OF THIRD PARTIES.** Cyber criminals often attack small companies because they represent an access point to larger targets. Be sure the security of third parties with which you do business meets your standards.

5 **COLLABORATE.** As the complexities of cyber threats escalate, external collaboration with security specialists is crucial. Tap into leading-edge expertise to identify vulnerabilities and develop appropriate plans and controls that support corporate strategies.

6 **PLAN FOR THE INEVITABLE.** Regularly review and test security policies, plans and processes. Run drills of your response plan and refine them as needed to maintain best practices and reinforce business resilience.

AN **INTEGRATED SECURITY TEAM** THAT **PROTECTS BUSINESS VALUE** AND **MITIGATES RISKS**

MNP IS HERE TO HELP **BUSINESSES DEVELOP** AND IMPLEMENT **STRONG, INTEGRATED SECURITY PRACTICES** THAT PROTECT VITAL ASSETS

THE GOAL OF OUR CYBER SECURITY TEAM IS TO PROVIDE BUSINESS LEADERS WITH REASSURANCE THAT COMPANY VALUE IS PROTECTED SO THEY HAVE THE CONFIDENCE TO ACT ON NEW OPPORTUNITIES AND DRIVE GROWTH AND SUCCESS.

IS YOUR COMPANY PREPARED TO HANDLE A CYBER SECURITY BREACH?

- Are you confident about the overall security preparedness of your organization?
- Is your management team knowledgeable about cyber security?
- Have you identified and protected your digital "crown jewels?"
- Has management taken any recent actions to protect the enterprise from growing cyber security threats?
- Do you have governance mechanisms in place to ensure controls are effective?
- Does the organization have clear roles and responsibilities for identifying, monitoring and responding to cyber security incidents?
- Do you conduct regular security assessments?
- Is your company managing risks from third-party vendors?
- Do you have crisis plans in place in the event of a cyber breach?

IF YOU ANSWERED "NO" TO ANY OF THE QUESTIONS ABOVE, IT'S TIME TO HAVE A CONVERSATION WITH ONE OF OUR PROFESSIONALS TODAY.

Danny Timmins
National Cyber Security Services Leader
T: 905.607.9777
E: danny.timmins@mnp.ca

Peter Guo
B.C. Enterprise Risk Services Leader
T: 604.637.1513
E: peter.guo@mnp.ca

This guide was published in cooperation with Miller Thomson.

MNP