Board of Directors’ Cyber Security Roadmap

A Top-Down Approach for Risk Management and Resilience

Cyber security threats are continually evolving and reshaping the business landscape. Beyond affecting your organization’s ability to conduct business, breaches can compromise intellectual property, employee and customer information and cause lasting legal and reputational damage.

As attacks continue to grow in frequency and sophistication, directors play a critical role in creating a culture and policy framework of effective cyber risk management. From the executive suite to the mail room, effectively preventing and responding to an incident begins at the boardroom table.

ACCOUNTING › CONSULTING › TAX MNP.ca

MNP

Setting the Tone: Six Principles to Live By

Cyber Risk is Enterprise Risk

Technology is now embedded within every business. Incorporate cyber security planning and expertise into all enterprise risk planning to understand the likelihood, source and steps to avoid (or reduce the harm of) a potential breach.

Cyber Risk Requires Cyber Perspective

Invite cyber security experts to join the board and include cyber discussions as a regular agenda topic at board meetings. Create a technology committee where priorities, trends, concerns and emerging controls are discussed and evaluated.

Cyber Risk Management Begins with Policy

Create and promote a culture of cyber incident prevention by emphasizing privacy protection, good technology hygiene and risk awareness throughout the organization.

Cyber Risks Have Legal Implications

Be aware of any legislative changes and legal cases pertaining to privacy, cyber security, reporting guidelines and repercussions of businesses who have experienced a cyber breach.

Cyber Risks and Attacks are Always Evolving

Focus on the fundamentals and strive for excellence in your cyber security maturity program, while staying on the lookout for new breach techniques, incidents and risks; especially those occurring within your industry or sector.

Cyber Risks Are Not All Equal

Setting the Stage: Six Steps to Secure the Business

Establish Effective Policies and Procedures

Align your organization with applicable privacy laws and create comprehensive privacy protection rules and best practices for all team members.

Create (and Test) an Incident Response Plan

Ensure everyone understands how to identify a breach, who to communicate with about a known or suspected breach, how to contain the breach and what to do in the aftermath.

Conduct a Maturity Threat Assessment

Periodically review your controls (i.e. policies, technology) to determine whether they’re suitable and effective for your enterprise risk profile.

Review Your Technology Infrastructure

Periodically assess your technology framework (i.e. firewalls, anti-malware, software versions, etc.) to determine whether they will protect against a breach.

Penetration Test Your Systems

Proactively hunt for vulnerabilities in your technology systems to understand the effectiveness of your cyber controls and the potential damage of a breach.

Manage Your Third-Party Vendors

Understand how any arm’s-length organizations protect your data, your liability and how they will protect you in the event their systems are breached.

MNP Can Help

Our team has extensive experience advising business leaders and boards of directors on cyber security risks, trends and opportunities and have helped many Canadian organizations improve their resilience to attacks. We offer sector- and business-specific insights on best practices and technologies, along with a wide range of services to help identify vulnerabilities, implement controls, respond and restore services after a breach.

For more information, contact:

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

Know which cyber risks you want to avoid, need to mitigate, are willing to accept or transfer through insurance — along with your strategy for each.