10 WAYS TO PROTECT YOUR BUSINESS FROM CYBER-ATTACKS

As our dependency on technology increases, ensuring your business is cyber-secure is more important than ever. According to the Canadian Centre for Cyber Security's National Cyber Threat Assessment 2020, "…cybercrime remains the most common threat faced by Canadian organizations of all sizes."

Improve your company's cybersecurity with these best practices.

1 USAGE POLICIES

Outline how employees and other stakeholders may use work devices and manage information to help your staff understand how to avoid data breaches and cyberattacks.

Detail what are acceptable and unacceptable uses of the internet, email and company devices, who the policy applies to and disciplinary actions that will be taken if misused.

2 PASSWORD POLICY

Strong passwords are a must. A password policy should address using different passwords for different platforms and changing them regularly. A strong password is at least 8 characters, includes at least one number and symbol and a mix of lowercase and uppercase letters.

The Canadian Centre for Cyber Security recommends creating a passphrase.

3 REDUCE ADMINISTRATIVE ACCESS

Keep administrative access restricted to select individuals.

4 DATA BACKUPS

Regularly backup your data and store in a secure and encrypted location (online or physically) so it may be readily recovered. Test backups to ensure they are uncorrupted.

1 in 5 small businesses will experience a cyberattack.

5 SOFTWARE UPDATES

Regularly update your operating system, anti-virus and firewalls to protect against new threats.

6 EMPLOYEE TRAINING

Educate staff on cyber risks and company cybersecurity policies. Training should include:

- How to recognize common cyberattacks such as phishing schemes;
- What to do in response to a cyberattacks; and,
- Company cybersecurity policies (including passwords, securing devices, etc.).

7 DEVICE SECURITY

Implement automatic lock screens and train employees to lock devices when unattended. Implement “clean desk policies” to discourage employees from leaving sensitive information on their desk.

Consider two-factor authentication (2FA) – especially when employees work remotely. This requires employees to verify their login through a secondary system such as an authenticator app. For remote staff, having a VPN (Virtual Private Network) may offer additional protection.

8 ONGOING RISK ASSESSMENTS

Assess your cyber risks on an ongoing basis to adapt to changing threats.

9 RESPONSE PLAN

Have a written plan in place to lessen the impact of a cyberattack. Include business interruption contingencies, a list of who may be affected by a breach and key contacts within and outside the company.

Keep a detailed log of incidents and responses and incorporate lessons learned into your best practices.

10 INSURANCE

A proper cyber insurance policy may help your business recover from a cyberattack and might include:

- Cyber-attack response expertise – Professional support to guide you through a cyber-risk event.
- Business interruption - If revenue falls due to a cyber-attack.
- Loss or corruption of data – Addresses expenses of recovering data.
- Privacy breach –Helps cover liability expenses involving compromised third party data.
- Legal Expenses – Expenses to retain cyber/privacy legal expertise.
- Reputational injury –Costs to manage reputational damage, including hiring PR professionals.
- Cyber extortion – Ransomware is a source of severe cyber claims. Expenses include IT forensic costs and potential payment of ransom demands.

Cyber liability insurance coverage will differ from market to market. Contact y our insurance professional to review your specific needs.

MEGSON FITZPATRICK INSURANCE
Business Division
710 Redbrick Street, 1st Floor
Victoria, BC V8T 5J3

Toll Free | 1.888.595.5212
Office | 1.250.595.5212
Fax | 1.250.595.2900

www.megsonfitzpatrick.com