Strengthening your Digital Defenses

Cybersecurity Basics

The average cost of a data breach to a Canadian business is $6.5M in 2023[1]. All businesses, regardless of size or sector, are potential targets. Investing in the right technology and adopting the latest cybersecurity best practices can help safeguard your business against cyberattacks.

Empower your business with these practical steps to establish a strong plan.

Invest in network security

80% of North American small and medium sized businesses are at risk from cyber threats[2].

Firewalls

Firewalls monitor the traffic into and out of your network, acting as gatekeepers that warn against Internet traffic from untrusted sources and possible malware associated with your applications.

Security software

Anti-malware and anti-virus software defend systems against viruses, ransomware, spyware, and other types of malicious software used by bad actors.

Continuous monitoring tools

Endpoint detection and response software monitors your systems and access points, automatically detecting and reporting anomalies to help prevent attacks.

Commit to endpoint security

97% of Canadian small and medium sized businesses reported being targeted by phishing attacks[3].

Patches and updates

Updating firmware — the software that controls essential hardware functions — and implementing patches for the operating system software and applications ensures that devices have the most up-to-date protection against evolving cyberattacks.

Backups

Backing up critical data and systems offline regularly can help minimize losses resulting from a cyberattack.

Encryption

Modern computers, such as PCs powered by Intel vPro®, use encryption to protect memory, firmware, and operating systems from being altered. Encryption can protect data, making it very difficult to access through lost or stolen devices.

Implement cloud security

1 in 2 Canadian businesses are unable to protect themselves from a cloud security breach[4].

Cloud access security broker (CASB)

CASB software strengthens security for cloud applications, provides visibility into employee usage, and gives more control over the security of cloud-based data.

Multi-factor authentication (MFA)

Multi-factor authentication helps ensure that only the right people can access your devices and systems by requiring an additional step beyond passwords to verify identity.

Engage your employees

75% of small and medium sized businesses reported at least one behavior that could potentially compromise their employer's cybersecurity or data[5].

Set Expectations

Educating employees about their role as the first line of defence against cyberattacks helps foster a culture of security that can help protect your business.

Training

Train employees to identify suspicious emails, phone calls, and websites and secure their personal information on social media.

Internal Policies

Create company-wide policies such as a technology usage policy, access control policy and a clean workplace policy to protect your business by establishing clear requirements and expectations for your employees.

Learn how Intel vPro® can help you prepare for a cybersecure future.
Visit Intel vPro® Platform Security to explore more.

1 — IBM, Cost of Data Breach Report, 2023
2 — CyberCatch, Small and Medium-sized Businesses Vulnerabilities Report, 2022
3 — CyberSavvy, Insurance Bureau of Canada Cyber Security Survey, 2023
4 — IDC, The State of Cloud Security in Canada, 2022
5 — CyberSavvy, Report Card, 2023

To learn more, visit cfib.ca/Cybersecurity

Brought to you by CFIB | intel vPRO

Strengthening your Digital Defenses

Checklist

The majority of cyberattacks can be prevented with modern devices and a few basic cybersecurity best practices.[1]

Know your environment

Take an inventory of your business's hardware and software assets and cloud-based applications for insight into where threats may exist.

Implement a technology usage policy

Create a policy that highlights the appropriate and secure use of technology including password guidelines, technology usage off-site and data privacy.

Implement multi-factor authentication (MFA)

Implement an additional layer of authentication to ensure the right people are accessing the right system.

Choose the right technology

Business-grade computers, such as PCs powered by Intel vPro®, are designed and built to protect against today's cyber threats. Choose devices with built-in security and capabilities to detect and prevent cyberattacks and reduce lost time due to inefficiencies.

Take advantage of built-in features

Enable the security features such as firewalls and encryption built-in to operating systems and devices, such as those powered by Intel vPro®.

Invest in security software

Install modern security software, such as anti-malware and anti-virus, to help defend systems against malicious software, including viruses, ransomware, and spyware. Configure the software to send alerts when threats are found.

Replace older devices

Older devices have vulnerabilities that leave your business open to greater risk. Plan and budget to replace older equipment with modern devices with built-in security features.

Configure automatic updates

Set a schedule for routinely implementing firmware, OS, and software updates. These patches often include critical security updates to help protect your business.

Create a security-first environment

Cybersecurity is no longer for IT only — it's everyone's responsibility. Provide adequate training to educate employees on their role in protecting the business.

Plan ahead

Use CFIB's Cybersecurity Incident Response Plan (CIRP) to detail who to alert and how to respond to a potential attack to minimize the impact on your business.

Learn how Intel can help you prepare for a cybersecure future.
Visit Intel vPro® Platform BIOS Security to explore more.

1 — Microsoft, Digital Defence Report, 2022.