cybersavvy

Cyber Savvy Checklist

Do not ignore the risks of cyber threats to your small or medium-sized business. Being cyber savvy starts by implementing cyber safety best practices.

While it is important to speak with a cyber security specialist to discuss the full range of strategies that are appropriate for your business, the checklist below can help you get a better understanding of whether you are taking the right steps to help safeguard your business from cyber risk

What cyber risks might your business currently face?

Conducting a self-assessment of your business is the first step in developing a sustainable and effective cyber security plan. This begins by understanding your business' existing systems, assets, data and capabilities to identify and manage cybersecurity risk.

The person responsible for information technology, such as the CEO or Chief Information Security Officer, should inventory and track all hardware and software, review vendor systems, inventory data inflows and outflows, do penetration testing and remove end of life technology.

Is your business taking the right steps to protect against cyber risk?

Do you have the appropriate safeguards in place to manage the security of your systems and data?

You can start by:

- only allowing authorized software on your systems
- securing how your system is configured
- monitoring all access logs (consider real time logging)
- actively monitoring user accounts and revoke access when necessary
- using screen lockouts, multi-factor authentication, and encrypted credentials
- using encryption, patch management, firewalls and intrusion detection
- providing security awareness training for staff and practice incident response

Does your business have a way to detect cyber threats?

Do you have the appropriate procedures in place to monitor and identify the occurrence of a cybersecurity incident?

This may include:

- developing a security operations centre (SOC)
- auditing your storage of data and monitoring unusual access
- using malware protection
- using Security Information Event Management (SIEM) log analysis tools

Do you have a plan to respond to cyber threats?

Do you have an incident response plan that outlines the appropriate procedures that will be needed for your business to take action when a cybersecurity incident is detected?

This may include:

- incident containment and mitigation strategies to reduce the impact of an incident (impact to other drives and backups)
- informing internal stakeholders, relevant authorities, impacted individuals as needed and your insurer
- performing digital forensic analysis to understand the root cause
- learning from the incident and implementing controls to prevent it from happening again

Do you have a plan to help your business recover from a successful cyberattack?

Have you outlined the specific activities that would need to take place to restore any capabilities or services that are impaired due to a cybersecurity incident and to maintain plans for future resilience?

An effective cyber security risk management plan will enable your business to answer the following questions:

- Will you be able to start recovery if systems are impacted?
- How will you start the recovery with no access to systems or data?
- How will you communicate with no system access to employees, customers and authorities (who has the contact directory – on paper)?
- How will you manage media and reputation and restoring customer trust?

Have you considered cyber insurance for your business?

While cyber insurance is not a replacement for robust cyber risk management, it is a tool that can help manage losses resulting from a successful cyberattack. Any cyber insurance policy should complement an organization's security processes and technologies, as part of its risk management plan.

Are you a business owner with general questions about how you can reduce your cyber risk or about getting a cyber insurance policy? Insurance Bureau of Canada (IBC) can help. Contact IBC's free Consumer Information Centre by calling 1-844-2ask-IBC (1-844-227-5422) or visit us at IBC.ca.