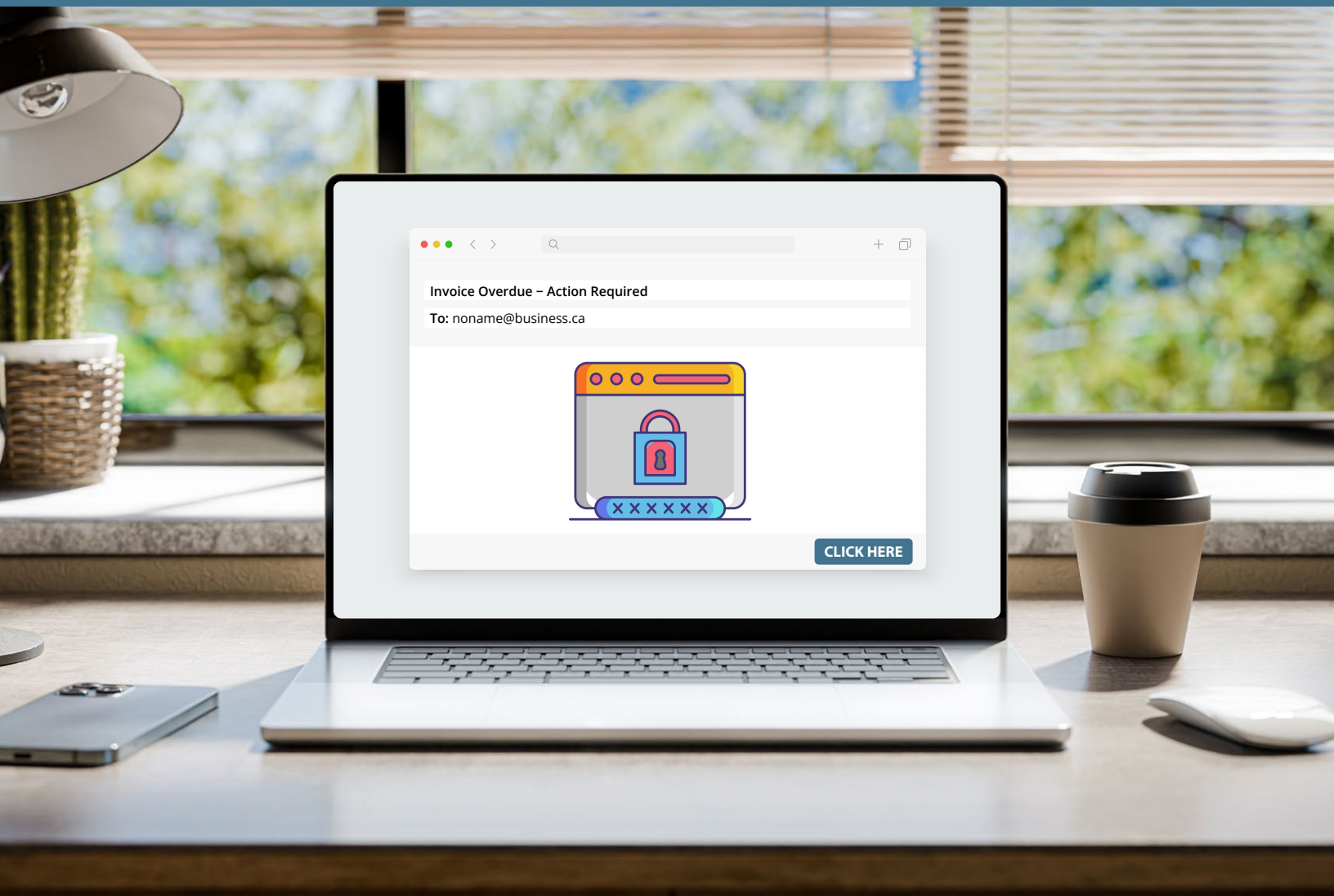
cybersavvy

Cyber criminals love small businesses

Learn how to help protect your small business with this Cyber Savvy insurance guide



Help protect your business from cyber crime

A single data breach could cost your business as much as **$7 million**. That's the latest Canadian average from a 2025 IBM report. For a small business, this isn't a single bill. **It's a combination of costs:** hiring expensive IT experts to fix the breach, legal fees if customers sue, fines from regulators and lost sales while your systems are down.

All it takes is one click. What might look like an attached invoice or a security alert could launch your business into a full-blown crisis with financial loss, lawsuits and a damaged reputation.

Could your business survive?

Cyber crime is a lucrative operation, and artificial intelligence tools are making it even more efficient. It's more important than ever for businesses and organizations to take proactive measures to protect themselves.

With this handbook, you will learn how to build a strong cyber security plan and help protect your company with the right cyber insurance policy, giving you a robust defence strategy.

Canada ranks second in the world for countries most affected by ransomware attacks, with 216 victims in the first half of 2025.

Toronto Star, Aug. 5, 2025

Do I need cyber insurance?

As a business owner, you probably already have insurance coverage relevant to your operations, including insurance for general liability, property and maybe even professional indemnity. These policies protect against physical damage, legal claims and operational risks. But they typically provide little or no coverage for digital risks such as data breaches, technology disruptions and cyber extortion. That's where a cyber insurance policy comes in.

Think of it this way: Imagine a thief breaks into your office overnight. Your traditional business insurance would help you cover the costs of the broken door and the stolen equipment.

But what if a thief doesn't break your door, but instead breaks into your digital systems? They could steal your confidential customer data, lock you out of your own network and demand a ransom, or cause a technology failure that shuts down your operations. Most traditional policies may not cover these kinds of digital risks. That's what cyber insurance is for – it's designed to protect you from a digital break-in.

What does cyber insurance typically cover?

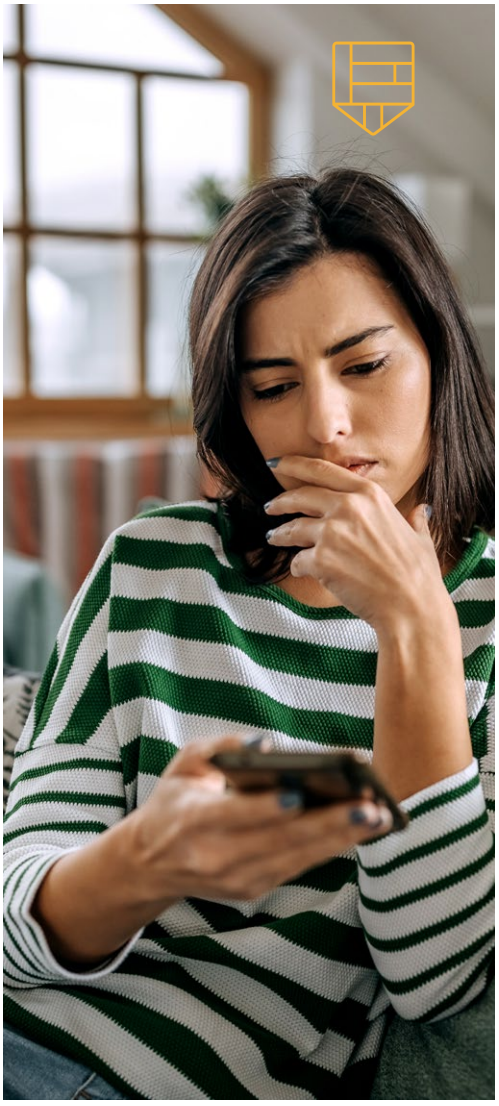
Cyber insurance can cover losses resulting from a range of cyber events, including:

- The loss of and/or unauthorized access to, or disclosure of, confidential or personal information;
- A technology failure or denial-of-service attack; and
- A demand for payment under threat of causing harm to your data (for example, disabling your operations or compromising your confidential data).

This list is not exhaustive because cyber coverage can vary from insurer to insurer and is constantly evolving. You can work with your insurance representative to find the right coverage for your specific needs.

Cyber insurance can help you cover several costs relating to cyber events including:

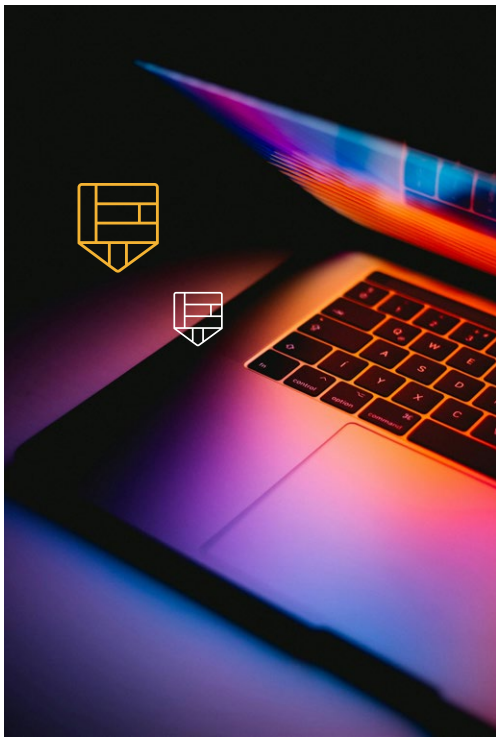
- Notification to affected parties;
- Mitigation of potential harm from a privacy breach, such as providing credit monitoring to affected individuals;
- Finding out what happened: A cyber forensics expert will be needed to help investigate the root cause and scope of the data breach; and
- Legal costs and civil damages related to a privacy or network security breach.



There are generally three types of cyber insurance:

- Stand-alone cyber insurance policies (dedicated policies specifically for cyber risks) are currently the most comprehensive option available in Canada and are separate from other insurance policies you may have.
- A traditional property and liability insurance policy may include limited coverage for some cyber events. Cyber coverage in these types of policies typically has low limits that may not cover the full cost of a breach or cyber attack.
- Endorsements (a type of add-on coverage also known as a rider) can add, remove or exclude certain cyber coverages, altering a cyber or traditional insurance policy to meet specific needs.

While a strong cyber plan can block many threats, no defence is perfect. Cyber insurance acts as your safety net for when an attack gets through. The first step to getting the right coverage is to understand your unique risks and start building your plan.



Is your business at risk of a cyber attack?

Your business is unique and may not have the same level of cyber risk as others.

While every company could be vulnerable to some degree, those handling sensitive customer data, processing online payments or relying heavily on digital infrastructure are especially exposed. When the stakes are higher, so is the need for robust cyber security and insurance protection.

You might be more at risk than you think. Do you:

- Store a customer email list in an online marketing platform?
- Process sales using a payment service provider?
- Keep employee records (like SINs for payroll) on a computer?

If you answered yes to any of the above, you're handling sensitive data.

To find out about some of the possible strengths and weaknesses of your business and its readiness to ward off a cyber breach, take Insurance Bureau of Canada's (IBC's) Cyber Insurance Assessment questionnaire. These 10 questions can help you learn about cyber security protocols and the best practices that most cyber insurers look for when assessing risk.

For example, you will be asked to consider:

- If you collect and store customers' personal information;
- What security procedures you have in place; and
- How frequently your employees receive cyber safety training.

These questions are similar to those you might see on a cyber insurance application.

While this free tool can't provide an actual risk assessment, it can help you find out if you're a good candidate for cyber insurance and help determine which areas your business may need to focus on to bolster cyber security.

The self-assessment is available at:

CyberSavvyCanada.ca

How do I apply for cyber insurance?

If you are considering cyber insurance for your business, you'll likely be required to fill out an application that insurers can use to assess the risks to your organization and appropriately price your policy.

To help you prepare, here are examples of what you could be asked when applying:

How would you describe your business?

1. How would you describe the operation(s) of the organization?
2. How many employees/contractors do you have working for the organization(s)? List the employee count per division.
3. Who are your customers? Are they consumers, government or other businesses?

What information does your business collect, and do you need to collect this information? Specifically, how many records from the following list do you retain in your organization?

1. Credit and debit card account numbers
2. Financial data for others
3. Government-issued identification (driver's licence, passport, social insurance number)
4. Personal information: name, address and contact details for individuals
5. Medical or health information for individuals
6. Trade secrets or intellectual property
7. Other organizations' corporate information.

TIP: Consider reducing the amount of information you collect to reduce your exposure to privacy losses and breaches.

What cyber security plans and protocols does your business have in place?

1. Have you developed a privacy security plan for the organization? Does this plan comply with existing government regulations for the handling and disclosure of personal or confidential information?
2. When was the last security and/or privacy audit performed, and were all the recommendations completed? If not, why weren't they completed?
3. Are you providing cyber security and/or privacy training for all staff?

What cyber security controls do you have in place to help reduce cyber risk for your business?

1. What physical controls are used to prevent access to the facility/office(s)?
2. What are the current security measures used to prevent access to IT systems and servers?
3. What technology is used for encryption and authentication, and what antivirus software and firewalls does your business have?

The self-assessment is available at:

CyberSavvyCanada.ca

What if I share information with my vendors? Could I be sued if they lose my data?

As a business owner, you are responsible for ensuring that sensitive data is kept safe, even when it's in the hands of third parties, such as your vendors. For example, if you share your customers' information with a software company and that company gets hacked, you could be held liable for any resulting damages to your customers. The good news is that you can manage this risk and take steps to better protect your organization.

A key step is having the supplier complete a security practice questionnaire. Questions should include business information, such as the name of the holding or parent company, the physical location of the supplier, and where their systems and data are stored.

The questionnaire should also review the vendor's risk management practices.

For example, it could ask:

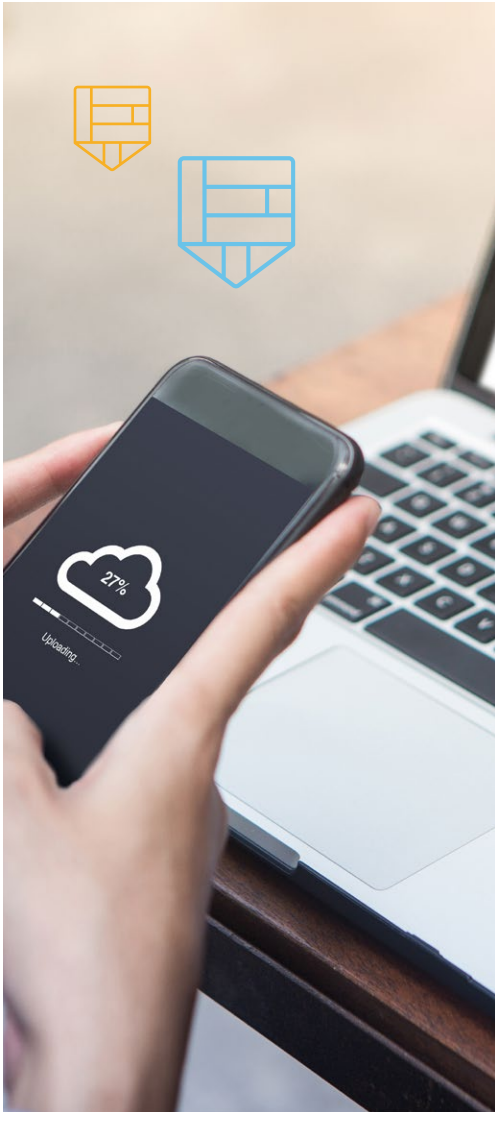
- Does the vendor have a formalized risk governance plan and risk assessment?
- Do subcontractors have access to the vendor's data or facilities?
- Does the vendor have a designated individual or team responsible for overseeing and implementing the cyber training for their staff and a security policy?

For additional verification, after reviewing the supplier's responses, consider requesting supporting documentation as evidence.

Make sure you reassess your vendors from time to time for cyber controls and maintain up-to-date records of all vendors providing services to your business.

In some cases, you should integrate vendors into your cyber incident response plans, including breach notification processes and lists of key contacts.

Consider having an off-boarding process for vendors whose contracts are ending to ensure they no longer have access to your systems or data. If necessary, also ensure they destroy sensitive records.

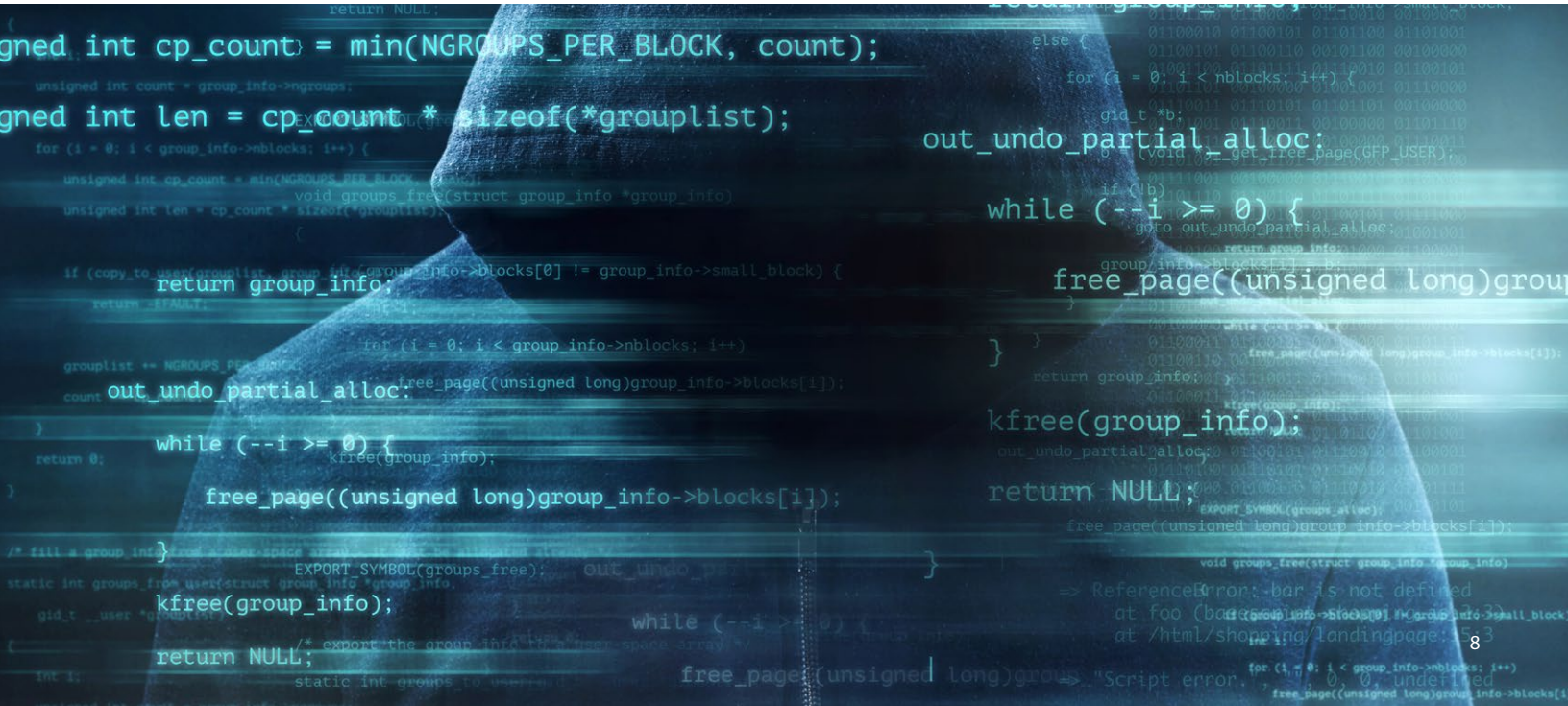


Worst-case scenario: What to do immediately after a cyber attack

Unfortunately, even with your best efforts, cyber crimes can still happen. If it happens to your business, acting quickly is your best defence. **Prepare now by learning these crucial steps to take if you experience a cyber security breach:**

- Change passwords and security questions on the compromised account and all related accounts.
- Determine what data has been affected, such as financial or personal information. Include overseas exposure: Networks and data might be subject to foreign regulations, such as the General Data Protection Regulation.
- Consider whether personal health information may have been collected or compromised.
- Incorporate advanced security measures such as endpoint detection and response and multi-factor authentication to manage employee access.
- Report the incident to:
    - Your cyber insurer, which can help with the steps to take to protect your data;
    - The account provider as well as to providers of associated or connected accounts;
    - Law enforcement;
    - The Canadian Centre for Cyber Security (contact@cyber.gc.ca) to report organizational identity theft;
    - The *Canadian Anti-Fraud Centre* online or at 1-888-495-8501 if it's an identity theft incident; and
    - Innovation, Science and Economic Development Canada if you have information about malicious software, electronic threats or spam.

Sources: Canadian Centre for Cyber Security and Innovation, Science and Economic Development Canada



How your insurer can help you recover from a cyber attack

A cyber breach is a complex event that few businesses can manage on their own. Your insurance representative can help by providing information and access to a network of cyber breach recovery specialists. Your cyber insurance policy might even cover some or all the costs of a cyber incident, from prevention, to containment, to recovery.

Here are some of the ways a cyber insurance policy can provide you with the support you need to reduce the impact of an attack and help your business recover:

- Your insurer may connect you with, or require you to use, approved experts such as a network and data forensics team to determine what information has been compromised. Some comprehensive policies might cover these experts' fees.
- Insurance companies often keep a list of their trusted service providers. Having access to this list can help you speed up the process of securing the right professionals, so you don't have to spend precious time figuring out what services you need and then searching for qualified individuals.
- A comprehensive cyber policy may cover certain expenses in the aftermath of a cyber attack, which can include defence costs and settlements from third-party lawsuits brought by impacted customers, subject to policy terms and limits. It could also cover some expenses for professionals to help recover your business' reputation and regain customer trust.

Safeguard your organization from cyber risk

Everyone has a role to play in reducing cyber threats in the workplace. While cyber insurance is an important backstop for a business in the event of a cyber breach, it should be thought of as only one component within a broader cyber risk mitigation strategy aimed at reducing the organization's vulnerability to online threats.

Cyber protection doesn't need to be costly or complicated. Following these tips from Get Cyber Safe Canada can help enhance your cyber security:

- ***Create a cyber security policy.*** Set clear rules for how your team handles data and devices.
- ***Train your team.*** Teach employees to spot scams and give them regular opportunities to practise safe online habits.
- ***Use business-grade security tools.*** Protect your systems with professional antivirus software and firewalls.
- ***Secure your network.*** Lock down your Wi-Fi and separate your sensitive IT systems from any systems that are accessible to the public.

- ***Back up critical data.*** Regularly save your data as required by applicable legislation. (Note: Make sure you're following your province's requirements on where data can be stored and backed up.)
- ***Limit access to sensitive information.*** Give employees access only to the information they need to perform their role.
- ***Keep software and systems updated.*** Always install updates to fix security vulnerabilities.
- ***Use multi-factor authentication (MFA).*** Add extra log-in protection beyond passwords.
- ***Secure mobile devices.*** Enforce strong security settings on the phones and tablets that employees use for work.
- ***Create an incident response plan.*** Prepare a step-by-step guide for handling cyber attacks.

Learn more with the

[Get Cyber Safe Guide for Small Businesses]

Creating a cyber security plan

Creating a cyber plan is an important step that small and medium-sized businesses can take to help improve their resilience to cyber breaches and reduce their overall cyber risk.

Get started by identifying valuable information and systems, understanding major threats and applying risk management best practices to your business.

The checklist below from the *Canadian Centre for Cyber Security* outlines the measures to consider when developing your cyber plan.

- ***Develop an incident response plan.*** If you have a plan, you can quickly respond to incidents, restore critical systems and data, and keep service interruptions and data loss to a minimum.
- ***Patch operating systems and applications.*** When software issues or vulnerabilities are identified, the software vendors release patches to fix bugs, address known vulnerabilities, and improve usability or performance.
- ***Use strong user authentication.*** Implement user authentication policies that balance security and usability. Ensure your business devices authenticate users before they can gain access to your systems. Wherever possible, use MFA.
- ***Back up and encrypt data.*** Copy your business information and critical applications to one or more secure locations, such as a cloud or an external hard drive. (Note: Make sure your backups are done in accordance with applicable privacy and data laws.)
- ***Activate security software.*** Activate firewalls and install antivirus and anti-malware software on all your business devices to thwart malicious attacks and protect against malware.
- ***Train your employees.*** Tailor your training programs to include information about your organization's cyber security protocols, policies and procedures. Having an informed workforce can reduce the likelihood of cyber incidents.

Secure cloud and outsourced services. Get to know a service provider before you contract them.

Secure websites. Protect your website and the sensitive information it collects. Encrypt sensitive data, ensure your certificates are up to date, use strong passwords or passphrases on the back end of the site, and use https for your site.

Secure mobile devices. Choose a device deployment model. This helps ensure employees only use approved applications and only download applications from trusted sources on the devices they use for work.

Maintain access control and authorization for employees. Apply the principle of least privilege to help prevent unauthorized access and data breaches, which means employees should only have access to the information they require to do their job.

Establish basic perimeter defences. Defend your networks from cyber threats. For example, use a firewall to defend against outside intrusions by monitoring incoming and outgoing traffic and filtering out malicious activities.

Configure devices securely. Take the time to review the default settings for all devices used to conduct your business; never use default passwords, and make modifications as required.

Secure portable media. While storing and transferring data using a portable media device, such as a USB key, can be convenient and cost-effective, it can be prone to loss or theft.

Download the complete cyber security checklist at

CyberSavvyCanada.ca

Cyber Savvy checklist

Don't ignore the risks of cyber threats to your small or medium-sized business. Being cyber savvy starts by implementing best practices for cyber safety.

While there is no replacement for speaking with a cyber security insurance specialist to discuss the full range of strategies that are appropriate for your business, answering the checklist questions 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 existing business systems, assets, data and capabilities to identify and manage cyber security risk.

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

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

Does your business have a way to detect cyber threats?

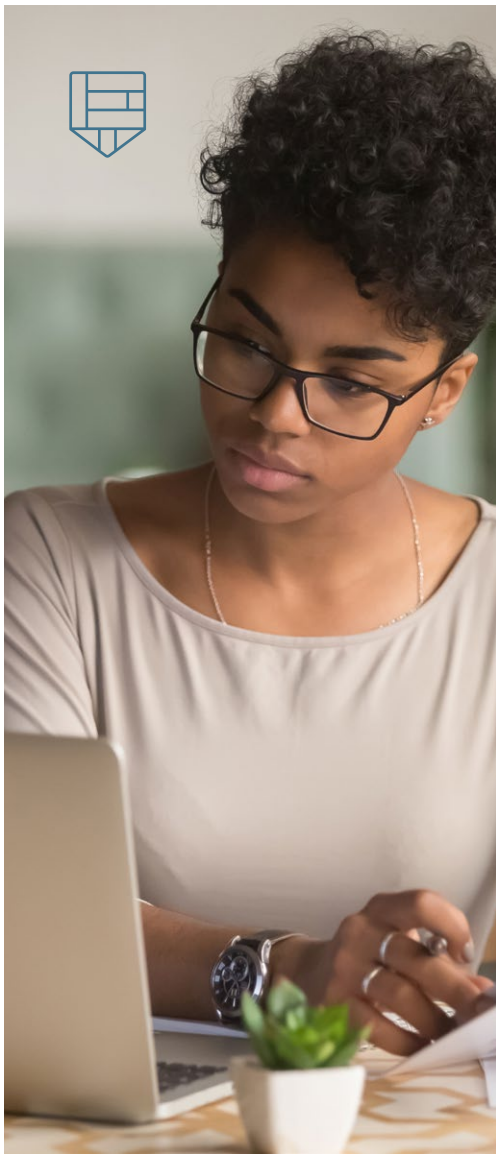
Do you have the appropriate procedures in place to monitor and identify the occurrence of a cyber security incident?

Do you have a plan to respond to cyber threats?

Do you have an incident response plan that outlines the appropriate procedures for your business to follow when a cyber security incident is detected?

Do you have a plan to help your business recover from a cyber attack?

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



Download the full cyber savvy checklist at CyberSavvyCanada.ca

About Insurance Bureau of Canada

Established in 1964, Insurance Bureau of Canada (IBC) is the national industry association representing Canada's private home, auto and business insurers. Its member companies make up the vast majority of Canada's highly competitive property and casualty (P&C) insurance market.

As the leading advocate for Canada's private P&C insurers, IBC collaborates with governments, regulators and stakeholders to support a competitive environment for the P&C insurance industry to continue to help protect Canadians from the risks of today and tomorrow.

IBC believes that Canadians value and deserve a responsive and resilient private P&C insurance industry that provides insurance solutions to both individuals and businesses.

For more information, visit **ibc.ca**. Follow us on **LinkedIn**, **X** and **Instagram**, and like us on **Facebook**. If you have a question about home, auto or business insurance, contact IBC's Consumer Information Centre at 1-844-2ask-IBC. We're here to help.

ibc.ca

This guide is available in an accessible format upon request by sending an email to info@cybersavvycanada.ca.