



2727 COWORKING / RESEARCH & PRACTICAL GUIDANCE

Cyber Insurance for Small Businesses: Controls First

Find a practical home for your work at 2727 Coworking in Montreal. Explore private offices, day workspaces and meeting rooms, plus business-address and virtual-mailbox services for your company.

Published by 2727 Coworking · 2026-10-29 · cyber insurance small business canada · small business cybersecurity canada baseline controls · phishing small business canada

Original article: <https://2727coworking.com/articles/cyber-insurance-security-basics-small-business-canada-cyber-centre-baseline>



In this article

1. Why controls come before the policy
2. Step 1: The Cyber Centre's 13 baseline controls
3. Step 2: What a cyber policy is for
4. Step 3: What insurers will ask you
5. Step 4: Questions to ask before you sign
6. Step 5: Quebec's legal duties after an incident
7. A 30-day starter plan

Why controls come before the policy

Small businesses usually think about cyber insurance after a scare: a client's email account is hijacked, a laptop is stolen, a ransomware note appears on the shared drive. The insurer's first question at that point is not "how much cover do you want?" but "what controls do you have?"

The numbers suggest most small firms are not ready for that question. In a survey commissioned by the Insurance Bureau of Canada (IBC) and published October 1, 2025, only 47% of small and medium-sized business respondents said their business was prepared for a cyber attack or data breach, fewer than half (48%) had implemented any form of cyber defence, just 22% carried cyber insurance and only 12% had a dedicated stand-alone cyber policy (IBC, [October 2025](#)). The same release cites research from BDC that 73% of small businesses have experienced a cyber security incident.

This guide puts the free homework first: the federal Cyber Centre's baseline controls. Then it covers what a cyber policy typically pays for, what insurers ask, and the Quebec legal duties that apply whether or not you are insured.

This article is general information, not insurance or legal advice.

Step 1: The Cyber Centre's 13 baseline controls

The Canadian Centre for Cyber Security publishes *Baseline Cyber Security Controls for Small and Medium Organizations* (version 1.2). Its stated aim is to apply "the 80/20 rule (achieve 80% of the benefit from 20% of the effort)" to the cyber security of small and medium organizations ([Cyber Centre, Baseline controls](#)). It lists 13 controls:

#	Control	What it means for a 1-10 person business
3.1	Develop an incident response plan	A one-page "who calls whom" plan, written before anything happens
3.2	Automatically patch operating systems and applications	Turn on automatic updates everywhere; replace devices and software the vendor no longer supports
3.3	Enable security software	Anti-malware that updates and scans automatically; built-in firewalls on
3.4	Securely configure devices	Change default passwords, disable features you do not use
3.5	Use strong user authentication	Two-factor authentication wherever possible
3.6	Provide employee awareness training	Recognising malicious emails and links, password habits
3.7	Backup and encrypt data	Regular backups of essential data, encrypted, with offline copies
3.8	Secure mobility	Decide who owns phones and how they are protected
3.9	Establish basic perimeter defences	Protect internet-connected networks, starting with a firewall
3.10	Secure cloud and outsourced IT services	Know what your providers protect and what you must
3.11	Secure websites	Protect the site and the data it handles

#	Control	What it means for a 1-10 person business
3.12	Implement access control and authorization	Least privilege; remove access people no longer need
3.13	Secure portable media	USB drives and SD cards are easily lost; encrypt or avoid them

The guidance is meant for organizations without a large IT team, and it says so in its recommendations. For example, on patching it recommends that small and medium organizations "enable automatic updates for all software and hardware if such an option is available - or consider replacing products with ones that provide the option," instead of the full patch management programs it advises for large enterprises (same source).

The five controls with the biggest payoff for a small team

1. Two-factor authentication (3.5). The Cyber Centre recommends two-factor authentication "wherever possible," and says organizations should require it for important accounts such as financial accounts, documenting any case where they decide not to. It also recommends changing passwords only when there is suspicion or evidence of compromise, rather than on a fixed schedule (same source). Start with email, banking, payroll, accounting software and your domain registrar.

2. Backups with an offline copy (3.7). The baseline recommends backing up essential business information regularly to an external secure location, storing backups encrypted with restricted access, and considering offline storage at a secure offsite location or documenting a rationale for not doing so. It specifies that long-term backups (for example weekly) must be offline, while frequent backups (for example daily) may be online (same source). A cloud sync folder is not a backup if ransomware can encrypt it too.

3. Automatic updates (3.2). Turn them on for laptops, phones, routers and browsers. Replace the old router that no longer receives updates.

4. Awareness training (3.6). The baseline lists practical topics: password policies, identifying malicious emails and links, approved software, appropriate internet use and safe social media use (same source). A 30-minute session each year, plus a rule that any payment-detail change is confirmed by phone, covers most invoice-fraud attempts.

5. An incident response plan (3.1). The Cyber Centre's advice is to assume incidents will occur and to have a plan to respond and recover, as part of business continuity planning (same source). Our [small business continuity plan template](#) has a section you can adapt.

If your team works remotely or in shared spaces, our [remote work security checklist](#) applies these controls to home networks and public Wi-Fi.

Step 2: What a cyber policy is for

A cyber policy pays for the costs that controls fail to prevent. Get Cyber Safe, the federal awareness campaign, and IBC list the costs a stand-alone cyber policy can help cover ([Get Cyber Safe](#)):

Coverage category	What it pays for
Network systems and electronic data restoration	Restoring or recovering damaged or corrupted data after a breach, denial-of-service attack or ransomware
Security breach remediation and notification	Notifying affected people and mitigating harm, for example credit monitoring
Forensic investigation	A firm to investigate the cause and scope of a breach
Legal costs and civil damages	Legal representation and possible damages related to a privacy or network security breach

IBC lists the risks more broadly: losses related to personal data security breaches, cyber extortion, technology disruptions and more (IBC, [Does your small business qualify for cyber insurance?](#)).

Why your existing business policy may not be enough

IBC's guidance is direct: "most property or liability policies don't expressly cover cyber risks, or have very limited coverage," so a stand-alone cyber policy may be worth considering, alongside preventive measures (same IBC page). If you already have a commercial general liability or package policy, ask your broker in writing which of the four categories above it covers, and up to what amount. Our [freelancer insurance guide](#) explains the other policies a small business typically carries.

Step 3: What insurers will ask you

IBC built a free 10-question self-assessment tool that helps owners learn about the security protocols and best practices most cyber insurers look for, and that poses some of the questions insurers may ask during the application. Examples of what it asks owners to consider: their cyber risk, whether they collect and store customers' personal information, what security procedures they have, and how often employees receive cyber safety training. IBC notes that the tool "cannot provide an actual risk assessment," but it can help gauge readiness (IBC).

Before you call a broker, prepare answers to questions like these, mapped to the baseline:

Likely application question	Baseline control	Your evidence
Is two-factor authentication on for email and remote access?	3.5	Screenshot of admin settings
How often do you back up, and is a copy offline?	3.7	Backup schedule, last restore test date
Are devices updated automatically?	3.2	Device list with OS versions
Do employees receive security training?	3.6	Date of last session, attendance
Do you have an incident response plan?	3.1	The plan document
Do you store customers' personal information? Where?	3.10, 3.12	Data inventory
Who has admin access?	3.12	List of admin accounts

Answer honestly. A policy's value depends on the application being accurate; if your controls are not in place yet, the better move is usually to implement them and then apply.

Step 4: Questions to ask before you sign

Policy wordings differ, and no public source sets a standard small-business cyber policy. Questions to ask your broker:

1. Which of the four coverage categories (data restoration, notification, forensics, legal and damages) are included, and what is the limit for each?
2. Is there a deductible or waiting period before business interruption cover starts?
3. Does the policy cover social engineering or invoice fraud (a client paying a fraudster after a fake email)?
4. Does it cover incidents at your cloud or IT providers?
5. Which controls are conditions of coverage (for example, two-factor authentication must be on)?
6. Does the insurer provide an incident hotline, and must you use its vendors?
7. Does it cover regulatory investigations and the costs of notifying people under Quebec law?

Step 5: Quebec's legal duties after an incident

Insurance or not, a Quebec business that holds personal information has legal duties when something goes wrong. Under the *Act respecting the protection of personal information in the private sector* ([P-39.1](#), [LégisQuébec](#)):

- **What counts.** A "confidentiality incident" is access, use or communication of personal information not authorized by law, or the loss of personal information or any other breach of its protection (s. 3.6). The Commission d'accès à l'information (CAI) gives examples including an employee consulting information without authorization, sending it to the wrong recipient, and a cyberattack such as phishing or ransomware ([CAI, Incidents de confidentialité](#)).
- **Act to reduce harm.** If you have cause to believe an incident occurred, you must take reasonable measures to reduce the risk of injury and to prevent new incidents of the same nature (s. 3.5).
- **Notify when the risk is serious.** If the incident presents a risk of serious injury, you must promptly notify the CAI and the persons whose information is concerned (s. 3.5). In assessing that risk you must consider the sensitivity of the information, the anticipated consequences of its use and the likelihood it will be used for injurious purposes, and consult the person in charge of the protection of personal information (s. 3.7).
- **Keep a register.** You must keep a register of confidentiality incidents, and send a copy to the CAI at its request (s. 3.8). That applies to every incident, not only the serious ones.
- **Providers do not take the duty off you.** The CAI states that a business that entrusts personal information to a third party remains responsible for its obligations in case of an incident: measures, register and notices ([CAI](#)).

The CAI suggests assessing an incident quickly with six questions: who is affected, how many people, what information, when it happened and was discovered, where (inside the business or at a provider), and why the security measures failed (same CAI page). Put those questions in your incident response plan.

If you have not set up the rest of Law 25 compliance, start with our [Law 25 checklist for micro-businesses](#).

A 30-day starter plan

Week	Actions
1	Turn on two-factor authentication for email, banking, accounting and domain accounts. List every admin account.
2	Set up automatic updates on all devices. Replace unsupported routers or laptops. Configure encrypted backups with a weekly offline copy; test one restore.
3	Write a one-page incident response plan, including the CAI's six questions and who keeps the incident register. Run a 30-minute phishing awareness session.
4	Take IBC's self-assessment, gather the evidence in the table above and request quotes from a broker. Compare wording, not just price.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. <https://www.ibc.ca/news-insights/news/canadian-small-businesses-are-underprepared-for-cyber-attacks-survey-shows>
2. <https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations>
3. <https://www.getcybersafe.gc.ca/en/blogs/cyber-insurance-can-help-reduce-online-risks-businesses-all-sizes>
4. <https://www.ibc.ca/news-insights/in-focus/does-your-small-business-qualify-for-cyber-insurance>
5. <https://www.legisquebec.gouv.qc.ca/en/document/cs/P-39.1>
6. <https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/incidents-confidentialite-mesures-securite-entreprises>

THE PUBLISHER

About 2727 Coworking

2727 Coworking is a Montreal workspace and business-address provider. We serve people who need a place to focus, meet, run a small business or establish a professional mailing presence. Our website offers English and French information about workspace options and services, alongside educational resources for operating a business in Canada.

A workspace that fits the day

Our workspace options include private offices, day passes and desks, and a conference room. These formats help individuals and teams compare a dedicated office with more flexible ways to work or hold a meeting. Prospective members can explore the virtual tour, review current pricing and book a visit before choosing a workspace.

Business addresses and mail

2727 Coworking provides business-address and virtual-mailbox services. Our resources explain the documents and practical questions involved, including guidance for people outside Canada. Service eligibility, included features, availability and access arrangements should be confirmed on the applicable service page or with our team.

Resources for Canadian small businesses

We publish guides, research and planning tools about workspace decisions, business addresses and starting a business in Canada. Our incorporation research includes information for people inside Canada and abroad, with jurisdiction-specific material to help readers identify the next questions to investigate. These educational resources complement our workspace and address services; they are not individualized legal, tax or immigration advice.

Visit or contact 2727 Coworking

Explore [private offices](#), [day passes and desks](#), [the conference room](#), [business addresses](#) and [virtual mailboxes](#). [Book a visit](#) or [contact the team](#) to discuss your needs.

A business address alone does not establish tax residence, immigration status, banking approval or eligibility for a government program.

Website: <https://2727coworking.com>

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.