WHITE PAPER · 2026 EDITION

The SMB Cybersecurity Playbook

What actually protects a small Canadian firm in 2026 — and what to do first

For owners and managing partners of professional firms in the Greater Toronto Area

CanopyTech Resources Ltd.

Managed IT Services · Greater Toronto Area
canopytech.ca · 647-478-8449

CONTENTS

What's inside

A working guide, not a product brochure — organised so you can read it end to end or jump to the section you need.

A note on the numbers in this paper

Every statistic is sourced to published research from CIRA, IBM, Verizon, the FBI's IC3 or the Office of the Privacy Commissioner of Canada, and listed in full on the references page. Where a figure is an average across all organisation sizes, we say so.

INTRODUCTION

Small doesn't mean safe anymore

There is a comfortable assumption still circulating in boardrooms across the GTA: that cyber criminals go after banks, hospitals and national retailers, and that a thirty-person accounting firm in North York is too small to bother with. It was never quite true. In 2026 it is actively dangerous.

Modern attacks are not hand-crafted. They are industrialised. Credential-stuffing kits, phishing-as-a-service subscriptions and AI-generated lures let one operator run campaigns against tens of thousands of mailboxes for the cost of a monthly software licence. Nobody chose your firm. Your firm simply answered.

And when the attack lands, the smaller organisation has the worse day. Verizon's 2025 **Data Breach Investigations Report** found ransomware present in **88% of breaches at small and medium businesses**, against 39% at large enterprises. Big companies get breached and absorb it. Small companies get breached and stop trading.

> **Who this is for**
>
> Owners, managing partners and operations leads at professional firms — law, accounting, finance, engineering, consulting — who own the security decision without being security specialists, and who have a real budget rather than an unlimited one.

This paper is deliberately practical: how attacks begin, what to teach your people, which technical controls earn their cost, what privacy law and your insurer now require, and a checklist you can work through this quarter. It offers no shopping list, because no product solves this. Sequence and discipline do.

Start with three questions

Every effective security program — at a bank or at a twelve-person firm — answers the same three questions before it spends a dollar:

1. **What are our assets?** Which systems, files and relationships would hurt most if they were encrypted, stolen or made public? Client files? The trust ledger? Your email history?
2. **What are the threats?** Who would plausibly come after those assets, and how? A ransomware crew wants leverage. A wire-fraud crew wants your payment instructions. They behave differently.
3. **Where are we vulnerable?** Which specific gaps — a shared admin password, an unpatched firewall, backups nobody has restored from — connect a threat to an asset?

Answer those three honestly and your budget allocates itself. Skip them and you will buy tools that protect things nobody was coming for.

01 WHERE CANADIAN SMBS ACTUALLY STAND

The 2026 numbers

Canadian data has caught up with the anecdotes. The picture it paints is not that attacks are exotic — it is that they are routine, expensive, and increasingly automated.

43%
of Canadian organisations reported a cyber attack in the past 12 months

88%
of SMB breaches involved ransomware, vs. 39% at large enterprises

$6.98M
average cost of a Canadian data breach in 2025, up 10.4% year over year

The Canadian Internet Registration Authority's 2025 survey put attacks on Canadian organisations at 43% over twelve months, with roughly a quarter reporting a ransomware incident specifically. IBM's 2025 **Cost of a Data Breach** report placed the Canadian average at CA$6.98 million — and breaches that began with phishing averaged CA$7.91 million, the most expensive entry point of all.

Those averages are skewed by large enterprises, so do not read CA$6.98 million as your invoice. Read the ratio instead: the cost of a breach is a large multiple of the cost of preventing it, at every size of business. For a firm of twenty to fifty people, the realistic bill is legal counsel, forensic investigation, client notification, staff downtime, and the clients who quietly don't renew.

What changed: the attacker's cost curve collapsed

Three shifts over the last two years explain why small firms are now firmly in scope.

- **Generative AI removed the tells.** The misspellings and stilted grammar that we trained a generation of employees to look for are gone. A phishing email in 2026 is fluent, correctly formatted, and references your industry accurately.
- **Credentials became the front door.** Verizon's 2025 report found stolen credentials were the single most common initial access route, used in roughly a fifth of breaches — and that more than half of ransomware victims had employee credentials already circulating in infostealer logs before the attack.
- **Voice and video became forgeable.** The FBI's 2025 Internet Crime Report logged business email compromise losses above US$3 billion, and for the first time tracked AI-assisted fraud as its own category. A cloned voice on a follow-up call is now a standard step in wire-fraud playbooks.

> **The uncomfortable implication**
>
> If credentials are the primary way in, then the most valuable thing you can do this month is not buy another security product. It is make sure a stolen password, on its own, is worthless — which means multi-factor authentication everywhere, without exceptions for executives.

The readiness gap

The same CIRA survey found that seven in ten Canadian organisations are worried about AI-powered threats, and that **98% now provide cybersecurity training** to staff. Awareness is not the missing piece. Recovery is: of the organisations hit by ransomware, **74% paid the ransom**.

Read that number carefully. Three quarters of Canadian ransomware victims concluded that paying criminals was their best available option — which almost always means the clean backup either didn't exist, had been encrypted along with everything else, or would have taken longer to restore than the business could survive. That is not an awareness failure. It is a recovery failure, and Section 06 is devoted to it.

What a bad week actually costs a firm your size

Headline averages are abstract. Here is the shape of the bill for a professional firm of twenty to fifty people, in roughly the order it arrives:

- **Downtime.** Staff cannot bill while systems are down. Multiply your average daily billable revenue by the number of days to recover — this is usually the largest single line, and it is the one good backups shrink most.
- **Incident response.** Forensic investigators and breach counsel are engaged at emergency rates, and you rarely get to choose them slowly.
- **Notification and remediation.** Reporting to the Privacy Commissioner, notifying affected individuals, and in many cases funding credit monitoring.
- **Client attrition.** The quietest line and often the largest over twelve months. Clients seldom announce that they left because of a breach.
- **Premium increases.** Expect a materially different conversation at your next cyber insurance renewal.

None of these are exotic. All of them are cheaper to prevent than to absorb — which is the entire argument for the next six sections.

02 HOW ATTACKS REALLY START: YOUR PEOPLE

Six tactics worth teaching by name

Almost every breach at a small firm begins with a person doing something reasonable. Not careless — reasonable. Someone paid an invoice, held a door, approved a login prompt, or helped a colleague who turned out not to be a colleague. Social engineering works because it borrows the behaviours that make an office function.

Give your team the vocabulary. People are markedly better at resisting a manipulation they can name than one they only vaguely sense. These are the six worth covering.

1. Phishing

Email, text, chat or ad impersonating a system or person you trust.

Still the highest-volume tactic and the most expensive entry point in IBM's Canadian data. The 2026 version is well-written and specific: a fake DocuSign request referencing a real matter, a Microsoft 365 login page that is pixel-accurate, a Teams message from a spoofed internal address. Urgency is the constant — the message always needs you to act before you think.

2. Pretexting and business email compromise

A fabricated identity and situation built to justify an unusual request.

The attacker impersonates a partner, the bookkeeper, a client's controller, or the IT provider. Frequently they are inside a real mailbox they have already compromised, replying within a genuine thread. The ask is almost always money or credentials: updated banking details, an urgent transfer while someone is travelling, a payroll change. This is the tactic that empties bank accounts.

3. Deepfake voice and video

A cloned voice or face used to reinforce a fraudulent instruction.

Thirty seconds of audio — a conference talk, a voicemail greeting, a podcast — is enough to clone a managing partner's voice convincingly. The pattern is a fraudulent email followed by a phone call that 'confirms' it, which defeats the exact verification step most firms rely on. The FBI began tracking AI-assisted fraud as its own category in 2025 precisely because of this.

4. MFA fatigue and push bombing

Repeated approval prompts sent until someone taps Approve to make them stop.

This one only exists because MFA works. Having stolen a valid password, the attacker triggers dozens of push notifications — often at 2 a.m. — betting that the target approves one out of exhaustion or confusion. Sometimes paired with a call from 'the help desk' apologising for the glitch and asking you to approve the next one.

5. Baiting, including malicious QR codes

Something enticing or convenient that delivers malware or a credential-harvesting page.

The classic version is a USB drive left in a lobby. The 2026 version is a QR code — on a parking meter, a fake invoice, a conference badge, a poster in your own elevator lobby — that opens a credential page on a personal phone, outside every filter and control your firm operates.

6. Tailgating and physical access

An unauthorised person following an employee into a restricted space.

Unglamorous and still effective, particularly in shared multi-tenant buildings. Someone with full hands asks you to hold the door; ten minutes alone with an unlocked workstation or an open server cupboard is enough. Courtesy is the exploit.

The one rule that covers all six

Verify unusual requests through a channel the requester did not choose. If the instruction arrived by email, confirm it by phone on a number you already had. If it arrived by phone, confirm it in person or by internal chat. Never use the contact details supplied in the message itself. Make this an explicit, written policy for any payment change or credential request — no matter who appears to be asking, and explicitly including the owner.

03 SPOTTING IT IN THE MOMENT

Red flags, by channel

Detection advice ages badly, because attackers read the same advice. Treat what follows as prompts for suspicion rather than a checklist that guarantees safety — and pair it with the verification rule from the previous section, which does not age.

In email

- A sender display name you recognise attached to an address you don't — check the address itself, and check it on mobile where it is usually hidden.
- Near-miss domains: **rn** in place of **m**, **.co** in place of **.ca**, an extra hyphen, a plausible subdomain.
- Time pressure, secrecy, or both — 'before end of day', 'don't loop in accounting yet'.
- A new or changed set of banking details. This is the single highest-risk email your firm receives, and it must always trigger an out-of-band callback.
- Attachments asking you to enable macros, or a login prompt appearing after you open a document.
- A reply that continues a real thread but subtly changes the reply-to address.

On the web

- Hover before you click on desktop; on mobile, press and hold to preview the destination.
- A login page reached by clicking a link rather than typing the address or using a bookmark. Treat every one of these as hostile by default.
- HTTPS and a padlock prove encryption, not honesty — most phishing sites have both.
- Pop-ups claiming your device is locked or infected and demanding payment or a phone call. Never call the number.

On the phone

- Any caller who needs you to act immediately, or who discourages you from verifying.
- An unexpected call from 'IT' or 'the bank' about an alert you did not raise.
- A familiar voice making an unfamiliar request — in 2026, a recognised voice is no longer identification. Hang up and call back on a known number.
- Requests for an MFA code. No legitimate organisation will ever ask you to read one out.

> **Make reporting the easy option**
>
> The costliest breaches are the ones an employee noticed and didn't mention. If reporting a suspicious email is slower or more embarrassing than deleting it, people will delete it. Give staff a one-click report button, thank everyone who uses it — publicly — and never criticise a false alarm. A firm that reports ten harmless emails to catch one real one is winning.

What to do when you're not sure

Uncertainty is the normal state, and staff need a script for it. Post these five steps somewhere people will actually see them:

1. **Stop.** Don't click, don't reply, don't forward it to a colleague to ask what they think — forwarding spreads the risk.
2. **Don't delete it.** If it turns out to be real, your IT provider will need the original message and its headers to see what else was targeted.
3. **Report it** using the button or address your firm has designated, even if you are 90% sure it's nothing.
4. **If you already clicked or entered credentials,** say so immediately. Speed matters far more than embarrassment: an account locked within minutes usually costs nothing, and the same account left running overnight can cost everything.
5. **Change the password and revoke active sessions** — from a different device, once IT confirms it's safe to do so.

Notice that four of the five steps are about what happens *after* a mistake. That is deliberate. Perfect detection is not achievable; fast, blame-free reporting is.

04 TRAINING THAT ACTUALLY CHANGES BEHAVIOUR

A realistic program for a firm without a security team

Annual compliance training, watched at 2x speed in December, changes nothing. What works is short, frequent, and specific to the way your firm actually operates.

The minimum viable program

1. **Day one.** Every new hire gets a 30-minute session before they are handed credentials: the six tactics, the verification rule, how to report. Part of onboarding, not a follow-up task.
2. **Every quarter.** A 15-minute refresh built around something real — an attack that hit a firm like yours, or a phishing attempt your own filters caught last month. Real beats generic.
3. **Every month.** Simulated phishing, sent to everyone including partners. Measure the trend, not the individual. Anyone who clicks gets a two-minute explainer, not a reprimand.
4. **Twice a year.** A 45-minute tabletop with your leadership team: ransomware hits on a Friday afternoon — walk through who you call and in what order. Most firms find their real gaps here.

Four rules that make it stick

- **Never punish a report.** The moment someone is embarrassed for raising a false alarm, your reporting rate drops to zero and you lose your best detection system.
- **Leadership goes first.** If partners are exempt from training or from MFA, the program is decorative — and attackers specifically target the exempt accounts.
- **Use your own examples.** Redacted real attempts against your firm carry more weight than any stock training library.
- **Measure the right thing.** Report rate matters more than click rate.

> ### If you don't have the resources to build this
>
> Most managed IT providers, CanopyTech included, run security awareness training and phishing simulation as part of a managed service. It is one of the least expensive lines on an IT budget and one of the few that measurably reduces incidents. Ask your provider what they already include.

05 THE TECHNICAL STACK, IN PRIORITY ORDER

Six layers that earn their cost

No single product secures a business. But the layers are not equal in value, and small firms routinely buy layer five before layer one. What follows is ordered by damage prevented per dollar spent — work down it, not across it.

LAYER 1

Identity and access

Highest impact, lowest cost

Since stolen credentials are the leading way in, identity is where the money goes first. That means multi-factor authentication on email, VPN, remote desktop and every administrative account, with no exemptions; phishing-resistant methods (passkeys, hardware keys, or number-matching rather than simple push approval) wherever supported; conditional access rules that block sign-ins from countries you don't operate in; and a password manager so nobody is reusing one password across twelve services. Administrative rights go to named IT staff only — not to every partner by default.

LAYER 2

Endpoint detection and response

Replaces traditional antivirus

Signature-based antivirus catches known malware. It does not catch an attacker using legitimate administrative tools with valid credentials, which is how modern intrusions actually unfold. EDR watches behaviour rather than files, and can isolate a compromised machine from the network automatically. Deploy it on every endpoint and server — partial coverage is how attackers pick their landing spot. If nobody in your firm is watching the alerts overnight, buy it as a managed service (MDR); an unmonitored console is not a control.

LAYER 3

Email security and authentication

Where most attacks arrive

Advanced filtering that inspects links at the moment of click, not only on delivery. External-sender banners on every inbound message. And SPF, DKIM and DMARC properly configured on your own domain — published at enforcement, not at the 'none' setting most firms stop at — so criminals cannot send mail that appears to come from your firm to your own clients. That last one protects your reputation as much as your network.

LAYER 4

Patching and asset inventory

Unglamorous, non-negotiable

Attackers exploit known vulnerabilities in software you already own. Automate operating system and third-party application patching; prioritise anything internet-facing — firewalls, VPN appliances, remote access gateways — within days, not months. This depends on knowing what you own: an asset inventory is not bureaucracy, it is the prerequisite. You cannot patch a server you forgot about, and neither will anyone else.

LAYER 5

Network, remote access and encryption

Contain the blast radius

A properly configured firewall with current firmware and a support contract. Segment guest Wi-Fi, staff devices and servers so a compromised laptop cannot reach your file server directly. Retire any internet-exposed remote desktop immediately. Full-disk encryption on every laptop and phone — in Canada, an encrypted stolen laptop is frequently the difference between a reportable privacy breach and an inconvenience.

LAYER 6

Logging and monitoring

So you find out from your logs, not your clients

Retain authentication and security logs from Microsoft 365, your firewall and your endpoints for at least 90 days, and have something — or someone — alerting on the obvious signals: impossible travel, mass file deletion, new mailbox forwarding rules, after-hours administrative changes. Mailbox forwarding rules in particular are the classic sign of a quiet, ongoing compromise.

A note on AI tools

Staff pasting client information into consumer AI assistants is now a live data-handling problem, and IBM's 2025 research put a measurable premium on breaches involving unsanctioned 'shadow AI'. You do not need to ban the technology — that just pushes it onto personal devices. Provide a sanctioned business-tier tool, write one page on what may and may not go into it, and say so plainly.

06 **BACKUP AND RECOVERY**

The layer that saves you

Every control above reduces the chance of an incident. Backup determines whether an incident is a bad week or the end of the business. It is the one layer with no substitute, and the one most often found broken at exactly the wrong moment.

Assume prevention fails — because eventually it does. The question that matters at 6 a.m. on the morning your files are encrypted is not how they got in. It is: how recent is the clean copy, how long until we're working again, and are we certain the copy restores?

The 3-2-1-1-0 rule

- **3** copies of your data.
- **2** different types of storage media.
- **1** copy off-site.
- **1** copy immutable or offline — written so that it cannot be altered or deleted, even by an administrator account. This is the specific control that defeats ransomware, because modern ransomware crews hunt for and destroy your backups before they encrypt anything.
- **0** errors on a verified test restore. Untested backups are a belief, not a control.

Decide your two numbers before you buy anything

Recovery point objective (RPO): how much data can you afford to lose? A nightly backup means losing up to a full day of work. Most professional firms find that unacceptable once they say it out loud, which argues for backups every few hours.

Recovery time objective (RTO): how long can you be down? Restoring a server from a file backup can take days. Image-based backups that can be spun up as a virtual machine — on the backup appliance or in the cloud — bring that down to hours, letting staff keep working while the primary system is rebuilt. Price the difference against a day of lost billable hours and the answer is usually obvious.

> ### Microsoft 365 and Google Workspace are not backed up for you
>
> This is the single most common and most costly misunderstanding we encounter. Microsoft and Google guarantee the availability of their platform — not the recoverability of your data. Retention windows are short and finite. If a compromised account deletes a mailbox or a shared drive, or ransomware encrypts synced files, recovery beyond that window is your responsibility. Third-party SaaS backup is inexpensive and, for a firm that runs on email and shared documents, essential.

Test it like you mean it

Schedule a restore test every quarter and treat it as a real exercise. The firms that suffer most in a ransomware event are almost never the ones without backups — they are the ones whose backups had been silently failing for four months.

1. Recover one specific file from roughly six weeks ago. Time it.
2. Stand up a full server from an image backup and confirm the application actually runs. Time that too.
3. Restore a deleted mailbox or shared folder from your Microsoft 365 or Google Workspace backup.
4. Write down the date, who performed it, what was recovered, and how long each step took.
5. Note anything that failed or surprised you, and fix it before the next test.

That record is the single most useful security document a small firm can hold. It satisfies your insurer, it answers the hardest question on most client security questionnaires, and it converts your backup from an assumption into a verified control.

> **One question worth asking your IT provider today**
>
> "When did we last complete a full restore test, and can I see the record?" If the answer takes more than a day to produce, you have found your first gap — and it is the one that matters most.

07 OBLIGATIONS

Privacy law, insurance, and your clients

Cybersecurity stopped being purely an IT question some time ago. For a Canadian professional firm it is now simultaneously a legal obligation, an insurance condition, and a term of doing business with larger clients.

PIPEDA: what Canadian law requires of you

Under the federal **Personal Information Protection and Electronic Documents Act**, breach reporting has been mandatory since 2018. If a breach of security safeguards creates a **real risk of significant harm** to an individual, you must report it to the Office of the Privacy Commissioner, notify the affected individuals, and notify any organisation that could reduce the harm — all as soon as feasible.

Two obligations catch firms out. First, you must keep a record of **every** breach of security safeguards for **24 months**, including the ones you assess as not meeting the reporting threshold — the Commissioner can ask to inspect those records. Second, knowingly failing to report or to keep records carries fines of up to **$100,000** per violation. Firms in Quebec, Alberta and British Columbia should also confirm their obligations under provincial privacy legislation, which differ.

> **Practical takeaway**
>
> You need a written incident response plan that names who assesses harm, who contacts the OPC, who contacts clients, and where the breach log lives. Two pages is enough. Writing it during an incident is not.

What insurers now demand

Cyber insurance in 2026 is underwritten on controls, not just revenue. Applications ask specific technical questions, and your answers are an attestation — a control you claimed but did not actually have in place is the most common reason a claim gets disputed after an incident. The controls that come up on nearly every application:

- MFA on email, remote access and all administrative accounts.
- EDR deployed across all endpoints — explicitly, not traditional antivirus.
- Immutable or offline backups, with a documented restore test in the recent past.
- A written incident response plan.
- Documented security awareness training with participation records.
- Timely patching, especially of internet-facing systems.

Read that list against the previous three sections. It is the same list. Insurers converged on it because it is what the claims data supports — which makes a cyber application a free, reasonably rigorous audit of your posture, whether or not you end up buying the policy.

Your clients are asking too

If you serve enterprise, public-sector or regulated clients, expect security questionnaires at onboarding and renewal, and expect contractual terms on encryption, breach notification timelines and subcontractor controls. Firms that can answer those quickly and credibly win work that firms who can't will never hear about. Increasingly, security posture is a sales asset.

There is a useful side effect here. The same evidence pack answers all three audiences at once: your regulator, your insurer and your clients are asking for versions of the same thing. Assemble it once and maintain it, rather than reconstructing it under deadline three times a year.

Assemble the evidence pack once

Keep the following in one place, dated, and refreshed at least annually. It takes an afternoon to create and it will save you days:

- A current asset and software inventory, including every SaaS application in use.
- Screenshots or reports proving MFA and EDR coverage — with the exception list, if any, and the reason each exception exists.
- Your most recent restore test: what was recovered, by whom, how long it took.
- Training completion records and phishing simulation results.
- The incident response plan, with the date of its last tabletop exercise.
- The 24-month breach log required under PIPEDA — including the entries you assessed as not reportable.

> **If you do only one thing after reading this section**
>
> Pull up your cyber insurance application — the one you or your broker filled in last renewal — and check every technical answer against reality. Firms routinely discover they attested to controls their previous IT provider never finished implementing. Better to find that now than during a claim.

08 THE READINESS CHECKLIST

Twelve points. Score yourself honestly.

Work through this with whoever runs your IT. For each item, the honest answer is yes, no, or 'we think so' — and 'we think so' should be treated as no until someone has verified it.

- [ ] **Run a security risk assessment**
  Identify your critical assets, the threats that plausibly target them, and the vulnerabilities that connect the two. Everything else is prioritised from this.

- [ ] **MFA everywhere, with no exemptions**
  Email, VPN, remote access, and every administrative account. Phishing-resistant methods where supported. Especially for owners and partners.

- [ ] **EDR on every endpoint and server**
  Not traditional antivirus. Managed and monitored if nobody in-house is watching alerts outside business hours.

- [ ] **Backups following 3-2-1-1-0**
  Including one immutable or offline copy, and a documented, timed restore test within the last 90 days.

- [ ] **Back up Microsoft 365 or Google Workspace separately**
  Your provider guarantees platform availability, not the recoverability of your data.

- [ ] **Automated patching, with internet-facing systems first**
  Firewalls, VPN appliances and remote access gateways patched in days. Maintain an asset inventory so nothing is missed.

- [ ] **A written out-of-band verification policy**
  Any payment change, banking detail update or credential request is confirmed by phone on a previously known number. No exceptions for leadership.

- [ ] **Security awareness training on a real schedule**
  Day one for new hires, quarterly refreshers, monthly phishing simulations. Keep participation records — your insurer will ask.

- [ ] **SPF, DKIM and DMARC at enforcement**
  So criminals cannot send mail that appears to come from your firm to your own clients.

- [ ] **Segmented network and encrypted devices**

  Guest, staff and server traffic separated. Full-disk encryption on every laptop and phone. No internet-exposed remote desktop.

- [ ] **A two-page incident response plan**

  Who assesses harm, who calls the OPC, who calls clients, who calls the insurer, where the 24-month breach log lives. Tested in a tabletop twice a year.

- [ ] **Least-privilege access, reviewed quarterly**

  Administrative rights to named IT staff only. Departing employees deprovisioned same-day — including from every SaaS application.

> **How to read your score**
>
> Ten or more confident yeses puts you ahead of most firms your size. Six to nine is typical and workable — close the gaps in the order they appear above, since the list is already prioritised. Fewer than six means an incident is a question of timing, and the first three items should be booked this month.

Turning the checklist into a plan

A list of gaps is not yet a plan. Put dates and owners against every 'no', sequence them in the order above, and set a review for ninety days out. Most of what is on this list is inexpensive and can be done in stages — the expensive part is always the incident you didn't prevent.

If your IT is outsourced, take this page to your provider and ask them to mark each item honestly, including the ones they are already contracted to deliver. A good provider will welcome the conversation. If yours can't answer, that is itself useful information.

SOURCES

References

Figures cited in this paper are drawn from the following published research. Where averages are quoted they reflect all organisation sizes unless stated otherwise, and should be read as indicators of scale rather than as predictions for any individual firm.

- Canadian Internet Registration Authority (CIRA), **2025 Cybersecurity Survey** — 43% of organisations targeted and 24% hit by ransomware in the preceding 12 months, of whom 74% paid; 70% concerned about AI-powered threats; 98% providing security training. Conducted by The Strategic Counsel, August 2025, among 500 Canadian cybersecurity decision-makers.
- IBM Security, **Cost of a Data Breach Report 2025** — Canadian average breach cost of CA$6.98M (up 10.4% year over year), phishing-initiated breach cost of CA$7.91M, and the measured cost premium associated with unsanctioned AI use.
- Verizon, **2025 Data Breach Investigations Report** — ransomware present in 88% of SMB breaches versus 39% at large enterprises; stolen credentials as leading initial access vector; prevalence of prior credential exposure among ransomware victims.
- Federal Bureau of Investigation, **2025 Internet Crime Report (IC3)** — business email compromise losses and the first formal tracking of AI-assisted fraud.
- Office of the Privacy Commissioner of Canada — **PIPEDA** breach of security safeguards reporting, the real risk of significant harm threshold, 24-month record-keeping requirement and penalties.

This paper is general guidance, not legal advice. Confirm your specific privacy and regulatory obligations with qualified counsel.

NEXT STEP

Start with the assessment, not the shopping list

You cannot protect everything equally, and you shouldn't try. The firms that spend their IT budget well are the ones that know which assets matter, which threats are realistic, and where the actual gaps are — before anyone quotes them on software.

Free Cybersecurity Risk Assessment

We map your assets, threats and vulnerabilities, then hand you a prioritised, budget-aware plan. No obligation, no pressure to switch providers.

- An inventory of what you actually have, and where your data lives
- The gaps ranked by risk — not by what we'd like to sell you
- A plain-English plan you can action in stages, at your budget
- Answers to the security questions on your insurance renewal

Book a free 30-minute call

CALL 647-478-8449

EMAIL info@canopytech.ca

WEB canopytech.ca

CanopyTech Resources Ltd.