



WHITEPAPER

Ransomware Readiness & Incident Response

A Practical Guide for Businesses Without a Security Team

Backups that actually restore • A one-page incident response plan • Who to call in the first hour • A tabletop exercise you can run yourself

Executive summary

Most businesses survive a ransomware attack not because they were never hit, but because they could restore their data and knew exactly what to do in the first hour. This guide gives organizations four practical tools to get there:

1. **A backup strategy that actually restores** — because a backup you have never tested is only a hope.
2. **A one-page incident response plan** — printed, signed off and kept where people can find it when systems are down.
3. **A first-hour contact sheet** — who to call, in what order, and what to tell them.
4. **A 60-minute tabletop exercise** — a scripted scenario your leadership team can run without outside help.

How to use this guide. Read Parts 1 and 2 with whoever manages your IT, whether in-house or a provider. Complete the incident response plan and contact sheet (Parts 3 and 4), print two copies, and store one off-site. Schedule the tabletop exercise (Part 5) within 30 days, then score yourself with the readiness scorecard. Revisit the whole package every six months or whenever key staff or systems change.

Who this is for: owners, executives, office and operations managers, and IT generalists at small and mid-sized Canadian organizations.

Why ransomware is a business problem, not just an IT problem

Ransomware stops a business from operating: no invoicing, no scheduling, no email, no access to client files. The encryption is only the visible part. By the time the ransom note appears, attackers have usually been inside the network for days or weeks.

How a typical attack unfolds

1. **Entry** — a phishing email, a stolen password without multi-factor authentication (MFA), or an unpatched remote access system or firewall.
2. **Quiet reconnaissance** — attackers map the network, find administrator accounts and locate the backups.
3. **Data theft** — sensitive files are copied out so they can be used for extortion later.
4. **Backup destruction** — attackers delete or encrypt any backups they can reach.
5. **Encryption and extortion** — systems are locked, and the business is threatened with publication of stolen data (“double extortion”) or pressure on its clients.

What it really costs. The ransom is often not the largest expense. Downtime, lost revenue, overtime, forensic investigation, legal advice, client notification, regulatory reporting and reputational damage typically add up to far more. Smaller organizations are frequently targeted precisely because attackers expect weaker defences and less ability to recover.

The good news: most attacks rely on a short list of common gaps. Closing those gaps, and being able to restore quickly if something gets through, removes most of the attacker’s leverage.

Part 1: Backups that actually restore

A backup only counts if attackers can't delete it and you have proven you can restore from it within a time your business can survive. Many organizations discover during an attack that their backups were connected to the network, encrypted along with everything else, or never completed.

The 3-2-1-1-0 rule

Rule	What it means	Why it matters
3 copies	Your live data plus two backups	One failure doesn't leave you with nothing
2 types of storage	For example, a local backup appliance and a cloud service	Avoids a single point of failure
1 off-site	At least one copy in a different location or cloud region	Protects against fire, flood and theft
1 offline or immutable	A copy that cannot be changed or deleted for a set period, even by an administrator	Attackers routinely target backups first
0 errors	Backup jobs are monitored and restores are tested	Proves the backups work

Decide what “fast enough” means

Before choosing tools, agree on two numbers for each critical system:

- **Recovery time objective (RTO)** — how long can you operate without this system? Four hours? Two days?
- **Recovery point objective (RPO)** — how much data can you afford to lose? One hour of work? One day?

Your accounting system might tolerate a one-day RPO; your client booking system might not. These answers determine how often you back up and how quickly you need to restore.

Don't forget cloud and SaaS data

Microsoft 365, Google Workspace and other cloud applications keep your data available, but they are not a complete backup. Deleted or encrypted files can sync across devices, and retention periods are limited. Use a dedicated third-party backup for email, shared drives and critical SaaS data.

Protect the backups themselves

- Use separate credentials for the backup system, not your everyday domain administrator account.
- Turn on MFA for the backup console and cloud backup accounts.
- Enable immutability or object lock wherever the product supports it.
- Keep backup servers off the main network where possible and restrict who can reach them.

- Set alerts for failed jobs, unusual deletions and changes to retention settings.

Test restores on a schedule

Test	How often	What it proves
Restore a single file or folder	Monthly	Backups are running and readable
Restore a full server or key application	Quarterly	You can rebuild a system and meet your RTO
Full recovery drill for critical systems	Annually	The whole business can come back, in the right order

Record each test: date, what was restored, how long it took and any problems found.

Backup checklist

- ☐ We have a written list of critical systems and data, with an RTO and RPO for each
- ☐ We follow the 3-2-1-1-0 rule
- ☐ At least one backup copy is immutable or offline
- ☐ Microsoft 365 or Google Workspace data is backed up by a separate service
- ☐ Backup systems use separate credentials protected by MFA
- ☐ Someone reviews backup reports and alerts every week
- ☐ We tested a restore within the last 90 days and documented the result
- ☐ We know the order in which systems must be restored

Part 2: Prevention essentials

You don't need an enterprise security budget to make your business a much harder target. These ten controls address the most common ways ransomware gets in and spreads. Ask your IT provider to confirm each one in writing.

#	Control	What good looks like
1	Multi-factor authentication (MFA)	On email, remote access, VPN, cloud apps, banking and every administrator account. Phishing-resistant options (passkeys, security keys) for executives and admins
2	Patching	Operating systems and applications updated within 14 days; internet-facing systems (firewalls, VPNs, remote access) within 48 hours of a critical fix
3	No exposed remote desktop	Remote Desktop Protocol (RDP) never open directly to the internet; remote access only through an MFA-protected VPN or secure gateway
4	Endpoint detection and response (EDR)	Modern EDR on every laptop and server, ideally monitored 24/7 by a managed detection and response (MDR) service
5	Least privilege	Staff don't use administrator accounts for daily work; admin rights are limited, separate and reviewed
6	Email filtering	Advanced filtering for malicious links and attachments, plus warning banners on external email
7	Security awareness training	Short, regular training and phishing simulations; a simple, blame-free way to report suspicious messages
8	Asset inventory	An up-to-date list of devices, software, cloud services and who has access to what
9	Network segmentation	Critical systems and backups separated so one infected laptop can't reach everything
10	Logging and alerting	Sign-in and security logs kept for at least 90 days and reviewed by someone who knows what to look for

Start here if you can only do three things this month: turn on MFA everywhere, make sure one backup copy is immutable, and close any remote desktop access exposed to the internet.

Part 3: One-page incident response plan

Print this page, fill in the blanks, and keep copies somewhere people can reach when computers and email are unavailable. During an attack, nobody reads a 40-page policy.

Organization: _____ **Plan owner:** _____ **Reviewed:** _____

Incident lead (makes decisions): _____ **Backup lead:** _____

1. Recognize the signs

Treat any of these as a possible attack and report it immediately: a ransom note on screen; files renamed with strange extensions or suddenly unopenable; many files changing at once; security software disabled; unexpected administrator accounts; or a warning from your IT provider, bank or a client.

2. Contain — first 15 minutes

- ☐ **Disconnect, don't power off.** Unplug network cables and turn off Wi-Fi on affected devices. Leaving them on preserves evidence in memory.
- ☐ Do **not** delete files, reinstall software or run "clean-up" tools.
- ☐ Do **not** contact the attackers or pay anything.
- ☐ Call the incident lead and your IT provider (see Part 4).
- ☐ If your IT provider advises it, disable remote access and isolate the backup system.
- ☐ Take photos of ransom notes and error screens with a phone.

3. Assess — first hour

- ☐ Which systems, sites and data are affected? Is it spreading?
- ☐ Is personal or client information involved?
- ☐ Are backups intact and isolated?
- ☐ Notify your cyber insurer **before** hiring outside help; many policies require it.

4. Communicate

- ☐ Switch to an out-of-band channel (personal phones, a pre-agreed messaging group) in case email is compromised.
- ☐ Tell staff what to do and what not to say. One person speaks for the organization.
- ☐ Prepare a holding statement for clients and suppliers; approve it with legal counsel.

5. Recover

- ☐ Rebuild or clean systems as directed by forensic specialists.
- ☐ Reset all passwords, starting with administrator and email accounts.
- ☐ Restore from known-clean backups in agreed priority order.
- ☐ Monitor closely for re-entry for at least 30 days.

6. Report and learn

- ☐ Assess privacy breach reporting obligations with legal counsel (see Canadian obligations).
- ☐ Report to the Canadian Centre for Cyber Security and local police.
- ☐ Hold a lessons-learned review within two weeks and update this plan.

Restore priority order

Priority	System or data	Target recovery time
1		
2		
3		

Approved by: _____ **Date:** _____

Part 4: The first hour — who to call

The order of your first few calls can decide whether you recover in days or weeks, and whether your insurance responds. Fill in this sheet now, while things are calm, and keep a printed copy with the incident response plan. Store numbers in personal phones too, since your phone system may be affected.

Call order

#	Who	Why call them	When
1	Incident lead (owner or senior executive)	Takes charge and authorizes decisions and spending	Immediately
2	IT provider or internal IT	Contains the spread and preserves evidence	Within 15 minutes
3	Cyber insurer's breach hotline	Most policies require prompt notice and use of approved forensic and legal firms; hiring your own first may affect coverage	Within the first hour
4	Breach counsel (often assigned by your insurer)	Directs the investigation, advises on reporting duties and ransom questions, and helps protect privileged communications	Within the first hour
5	Incident response / forensics firm	Investigates how attackers got in, what they took and when it's safe to restore	Usually arranged through insurer or counsel
6	Local police	Criminal matter; a police report may be needed for insurance	Same day
7	Canadian Centre for Cyber Security	National reporting and advice: 1-833-CYBER-88 (1-833-292-3788) or report online at cyber.gc.ca	Same day or next business day
8	Bank	Watch for fraudulent payments and changed banking details	Same day if finances may be affected

Emergency contact sheet

Complete, print and store with your incident response plan. Keep a copy off-site and in personal phones.

Role	Name / company	Phone (24/7)	Alternate contact	Policy / account #
Incident lead				
Backup incident lead				
IT provider / internal IT				
Cyber insurer breach hotline				
Insurance broker				
Breach counsel				
Forensics / IR firm				
Local police (non-emergency)				
Canadian Centre for Cyber Security	Cyber Centre	1-833-292-3788	contact@cyber.gc.ca	
Bank				
Internet and phone provider				
Key software vendors				
Communications / PR lead				

What to have ready when you call

- Time the incident was discovered and by whom
- What you are seeing (ransom note wording, affected systems, file extensions)
- What has already been done (devices disconnected, accounts disabled)
- Whether personal or client information may be involved
- Your insurance policy number and IT provider's contact details

A note on paying the ransom: paying does not guarantee your data back or that stolen data will be deleted, and it may be restricted where the attackers are sanctioned. Never decide on your own; involve your insurer and breach counsel.

Part 5: Tabletop exercise — “Monday Morning Lockout”

A 60-minute tabletop exercise is the cheapest way to find the gaps in your plan before an attacker does. It’s a guided discussion, not a technical test: nobody touches a computer.

Set-up

- **Who:** the owner or CEO, finance lead, operations lead, IT contact (internal or provider), and whoever handles communications. Four to eight people is ideal.
- **Facilitator:** anyone comfortable keeping time and asking questions. They read the injects aloud and don’t take part in decisions.
- **Note-taker:** records decisions, questions nobody could answer and action items.
- **Bring:** printed copies of your incident response plan and contact sheet. No laptops.
- **Ground rules:** there are no wrong answers; the goal is to find gaps, not assign blame. Answer based on what you would really do today.

Inject 1 — Monday, 7:45 a.m. (10 minutes)

The first employee to arrive can’t open files on the shared drive. Every file now ends in *.locked*, and a text file on the desktop says your data has been encrypted and stolen. Two more staff report the same thing.

- Who does this employee tell, and how?
- Who is in charge right now? What’s the first thing they do?
- Do we disconnect devices? Who decides, and does everyone know how?

Inject 2 — 8:15 a.m. (10 minutes)

Your IT provider confirms that the file server and most laptops are affected. Email still seems to work, but nobody is sure it’s safe.

- How do we communicate if we can’t trust email or Teams?
- Who calls the insurer? Does anyone know the policy number or hotline?
- What do we tell staff who are arriving for work?

Inject 3 — 9:30 a.m. (10 minutes)

The IT provider reports that the local backup appliance was also encrypted. A cloud backup exists, but nobody has tested a full restore from it.

- How long can we operate without our systems? Which system do we restore first?
- Can we keep serving clients manually? What paper processes do we have?
- What would this cost us per day?

Inject 4 — 11:00 a.m. (10 minutes)

The attackers email the CEO directly. They demand \$250,000 in cryptocurrency within 72 hours and attach a sample of client records as proof they have your data.

- Who decides whether to engage or pay? Who advises us?
- Does client personal information create reporting duties? Who determines that?
- What do we say to clients, and when?

Inject 5 — 2:00 p.m. (10 minutes)

A reporter calls reception asking about “a data breach at your company,” and a major client emails asking whether their information is safe.

- Who speaks for the organization? What are staff told to say?
- Do we have a holding statement ready?

Debrief (10 minutes)

- What went well?
- Where did we hesitate, disagree or not know the answer?
- What information did we need but not have?
- What three actions will we take in the next 30 days, and who owns each one?

Action log

Gap found	Action	Owner	Due date

Tip: run this exercise at least once a year, and again after major staff or system changes. Next time, vary the scenario: a compromised email account used to redirect a supplier payment, or a key cloud provider going offline.

Ransomware readiness scorecard

Score each statement: **2** = fully in place, **1** = partly or unsure, **0** = not in place. Be honest; “I think so” counts as a 1.

#	Statement	Score (0–2)
1	MFA is enabled on email, remote access, cloud apps and all admin accounts	
2	Security updates are applied promptly, especially on firewalls and remote access systems	
3	No remote desktop access is exposed directly to the internet	
4	Every device has EDR, and someone monitors its alerts	
5	Staff do not use administrator accounts for everyday work	
6	At least one backup copy is immutable or offline	
7	Microsoft 365 or Google Workspace data is backed up separately	
8	We successfully tested a restore in the last 90 days	
9	We have a written, printed incident response plan with a named incident lead	
10	Our emergency contact sheet is complete and stored outside our systems	
11	We have cyber insurance and know how to activate it	
12	We have run a tabletop exercise in the last 12 months	
	Total (out of 24)	

What your score means

Score	Readiness level	What to do next
20–24	Resilient	Keep testing. Focus on annual exercises and continuous monitoring
13–19	Exposed	You have foundations but real gaps. Prioritize any 0s in items 1, 3, 6 and 8 within 30 days
0–12	At risk	A single attack could halt operations for weeks. Start with MFA, immutable backups and the one-page plan this month

Canadian reporting obligations and resources

If a ransomware attack involves personal information, Canadian privacy law may require you to report it and notify affected people. Because attackers now routinely steal data before encrypting it, assume personal information is involved until an investigation shows otherwise. Confirm your specific obligations with legal counsel; this summary is general information, not legal advice.

Law	Applies to	Key obligation
PIPEDA (federal)	Private-sector organizations handling personal information in commercial activity, in most provinces	Report breaches that create a real risk of significant harm to the Office of the Privacy Commissioner of Canada, notify affected individuals as soon as feasible, and keep records of all breaches for 24 months
Quebec Law 25	Organizations handling personal information of people in Quebec	Report confidentiality incidents presenting a risk of serious injury to the Commission d'accès à l'information and affected individuals, and keep an incident register
Alberta PIPA	Private-sector organizations in Alberta	Report incidents with a real risk of significant harm to Alberta's Information and Privacy Commissioner
Provincial health privacy laws (e.g. Ontario PHIPA)	Health information custodians	Additional notification and reporting duties for health information
Contracts and sector rules	Businesses with client contracts or regulated clients	Many contracts require notice to clients within a set number of hours; check yours now, not during an incident

Where to report and get help

- **Canadian Centre for Cyber Security:** report online at cyber.gc.ca, call 1-833-CYBER-88 (1-833-292-3788) or email contact@cyber.gc.ca. The Cyber Centre is not a law enforcement agency, so also report to police.
- **Police:** your local police service, or 911 if there is an imminent threat to life. The RCMP also accepts reports of cybercrime and fraud.
- **Privacy regulators:** the Office of the Privacy Commissioner of Canada and your provincial commissioner, where applicable.

Privacy and cyber security legislation in Canada continues to evolve. Review this section at least annually.

Next steps: your 90-day readiness plan

Timeframe	Actions
First 30 days	Complete the scorecard. Enable MFA everywhere. Fill in the incident response plan and contact sheet, print them and store a copy off-site. Confirm at least one immutable backup exists
Days 31–60	Test a restore of a critical system and time it. Close exposed remote access. Confirm EDR coverage and who watches the alerts. Review your cyber insurance requirements with your broker
Days 61–90	Run the “Monday Morning Lockout” tabletop exercise. Work through the action log. Re-score yourself and share results with leadership

How Teleco can help. Not sure where you stand, or don’t have time to do this alone? The Teleco team can run your readiness assessment, test your backups, facilitate your tabletop exercise and help you close the gaps. **Book a free ransomware readiness consultation with Teleco:** [807-345-2900 / 1-800-465-3933 | [IT@teleco.ca] | [teleco.ca]

Glossary

- **EDR (endpoint detection and response):** security software that watches laptops and servers for suspicious behaviour and can isolate them automatically.
- **Immutable backup:** a backup that cannot be changed or deleted for a set period, even by an administrator.
- **MDR (managed detection and response):** a service where security specialists monitor your systems 24/7 and respond to threats.
- **MFA (multi-factor authentication):** a second check, such as an app prompt or security key, in addition to a password.
- **RPO / RTO:** how much data you can afford to lose, and how long you can be without a system.
- **Tabletop exercise:** a discussion-based rehearsal of how your team would respond to an incident.