GROUP 4 NETWORKS

What Every Business Owner Must Know About Protecting Critical Data

A plain-English guide for Toronto and GTA business owners: how data is really lost, what actually protects it, and the questions to put to your IT provider.

Group 4 Networks | Managed IT and Cybersecurity, Toronto & the GTA
(416) 623-9677 | g4ns.com | Free guide: g4ns.com/report

Why this guide exists

Most business owners do not think about their data until the day it is missing: the file server will not start, the accounting file is encrypted, an employee deleted a client folder, or a laptop was left in a taxi. By then the only question that matters is, "Can we get it back, and how long will it take?"

This guide is written for owners and office managers, not IT people. It explains the realistic ways small and mid-sized organizations lose critical data, what a sound protection plan contains, and how to check whether yours would hold up. If you can answer "yes" to every item on the checklist in section 9, you are better protected than most.

> **Critical data** is anything that would stop the business, cost you clients, or create a legal problem if it disappeared or fell into the wrong hands: client files, financial records, email, contracts, case or patient records, and the systems that hold them.

In this guide

1. The eight most common ways critical data is lost
2. The 3-2-1 backup rule, and the fourth copy most people miss
3. Microsoft 365 is not a backup
4. A backup you have never restored is a hope, not a backup
5. Stop the break-in: accounts, email and devices
6. Your people are part of the system
7. Canadian obligations: PIPEDA, PHIPA and your clients
8. If something goes wrong: the first 60 minutes
9. The 15-point protection checklist
10. Ten questions to ask your IT provider

1. The eight most common ways critical data is lost

Cause	What it looks like in a real office
Ransomware	Files become unreadable overnight and a ransom note appears. Modern attackers also hunt for your backups and delete them first.
Compromised email account	A staff member enters a password on a fake Microsoft sign-in page. The attacker reads mail, sends invoices from your address and may delete evidence.
Accidental deletion	Someone deletes a shared folder or overwrites a spreadsheet. Often noticed weeks later, after short retention has expired.
Hardware failure	A server disk, NAS or laptop drive fails. Disks do not warn you politely.
Lost or stolen device	A laptop or phone with client data leaves the building and the disk is not encrypted.
Backups that quietly stopped	The backup job has been failing for months. Nobody was watching, and nobody has tried a restore.
Departing or disgruntled staff	Access is not removed on the last day, or files are copied or deleted on the way out.
Fire, flood, theft, power events	The server and the "backup" sit in the same room, so one event removes both.

Notice how few of these are exotic. Most are ordinary mistakes and ordinary failures. That is good news, because ordinary risks can be managed with ordinary, affordable controls.

2. The 3-2-1 backup rule, and the fourth copy most people miss

The long-standing rule of thumb for backups is **3-2-1**:

- **3** copies of your data (the working copy plus two backups)
- **2** different types of storage (for example, a local appliance and the cloud)
- **1** copy off site, away from the office

Add the "immutable" copy

Ransomware now targets backups directly. At least one backup copy should be **immutable** (it cannot be changed or deleted for a set period, even by an administrator whose password was stolen) or fully offline. This single control is what turns "we are shut down for weeks" into "we restore and carry on."

Two numbers to agree on in advance

- **How much data can we afford to lose?** (Recovery Point Objective) If the answer is "no more than a few hours of work," a nightly backup is not enough.
- **How long can we afford to be down?** (Recovery Time Objective) Restoring a few files and rebuilding a whole server are very different jobs. Ask for a number, in writing.

3. Microsoft 365 is not a backup

This is the most common and most expensive misunderstanding we see. Microsoft keeps its service running and provides recycle bins and limited retention. That is availability, not a backup of your business data. If an account is compromised, a user empties the recycle bin, or a sync error removes files, recovery can be limited or impossible after the retention window.

- Back up **Exchange mailboxes, OneDrive, SharePoint and Teams** to a separate location with its own login.
- Confirm how far back you can restore (days, months, years) and who is allowed to restore.
- Do not assume a sync client such as OneDrive is a backup. It copies deletions as faithfully as it copies files.

4. A backup you have never restored is a hope, not a backup

Backup software can report "success" while the data is unusable or incomplete. The only proof is a test restore.

- **Monthly:** restore a handful of random files and open them.
- **Quarterly:** restore a full folder tree or a mailbox to a different location.
- **Annually:** rehearse a full server recovery and record how long it really took.
- **Daily:** somebody (or something) must check backup results and act on failures. A failed job nobody reads is the same as no job.

> **Ask to see it.** A good provider will happily show you the last successful backup, the last test restore and the retention settings. If they cannot, treat that as your answer.

5. Stop the break-in: accounts, email and devices

Most incidents start with a stolen password or a malicious email. Prevention is cheaper than recovery.

Accounts and email

- **Multi-factor authentication (MFA) for everyone**, including the owner and every shared or service account. Prefer an authenticator app or passkey over SMS where possible.
- **Block legacy sign-in methods** that bypass MFA, and use Conditional Access policies to restrict risky sign-ins.
- **Email protection** beyond the default filter: link and attachment scanning, impersonation protection, and correctly configured SPF, DKIM and DMARC for your domain so criminals cannot easily send mail as you.
- **Limit administrator rights.** Daily work should not be done from an account that can change everything.
- **Offboarding on day one.** Disable accounts, reset sessions and recover devices the day someone leaves.

Computers and servers

- **Modern endpoint protection** that watches behaviour, not just known viruses, and is monitored by a person or service, not just installed.
- **Regular patching** of Windows, Microsoft 365 apps, browsers and third-party software, with a reporting trail.
- **Full-disk encryption** on every laptop and mobile device that holds business data.
- **Secure remote access** (a properly configured VPN or zero-trust tool, never an open remote desktop port).
- **A managed firewall** that is updated and reviewed.

6. Your people are part of the system

Technology reduces risk, but staff still decide whether to click, reply or approve a payment. Short, regular security awareness training works better than one long annual session.

- Run **simulated phishing** emails and use the results to coach, not to punish.
- Agree a simple rule for payment and banking changes: **verify by phone using a number you already have**, never one from the email.

- Make it easy and blame-free to report a suspicious message or a mistaken click. The faster you hear about it, the smaller the damage.
- Keep a short written policy for acceptable use, remote work and personal devices.

7. Canadian obligations: PIPEDA, PHIPA and your clients

Protecting data is not only good practice; for many organizations it is a legal and contractual duty.

- **PIPEDA** requires organizations to safeguard personal information appropriately and, where a breach creates a real risk of significant harm, to report it to the Privacy Commissioner, notify affected individuals and keep a record of breaches.
- **PHIPA** (Ontario) applies to health information custodians such as clinics and dental offices, with its own safeguarding and breach-notification duties.
- **Law firms and professional offices** have professional-conduct duties around client confidentiality, and clients increasingly ask for proof of security controls in their own questionnaires and contracts.
- **Cyber insurance** applications now commonly ask whether you use MFA, tested backups and endpoint protection. Wrong answers can void a claim.

This section is general information for business owners and is not legal advice. Speak with your lawyer or privacy officer about your specific obligations.

8. If something goes wrong: the first 60 minutes

Decide this before you need it, and keep a printed copy somewhere other than the affected computers.

1. **Disconnect, do not power off.** Unplug the affected computer from the network (cable or Wi-Fi). Leave it running so evidence is preserved.
2. **Call your IT provider immediately** and tell them exactly what you saw. Do not try to "clean it up" yourself.
3. **Change passwords** for affected accounts from a different, known-clean device, and ask your provider to revoke active sessions.
4. **Do not pay or reply** to a ransom demand before taking advice.
5. **Write down the timeline:** what happened, when, and who saw it.
6. **Notify your insurer** if you have cyber cover; policies often require prompt notice.
7. **Assess privacy obligations** with your lawyer if personal information may be involved.

9. The 15-point protection checklist

Score yourself honestly. Each "No" or "Not sure" is a conversation to have this month.

	Question
☐	Do we have at least three copies of critical data, one of them off site?
☐	Is at least one backup immutable or offline, so ransomware cannot delete it?
☐	Are Microsoft 365 mailboxes, OneDrive, SharePoint and Teams backed up separately?
☐	Has someone successfully restored data from backup in the last 90 days?
☐	Does a named person or service review backup results every day and act on failures?
☐	Do we know, in writing, how long a full recovery would take and how much data we could lose?
☐	Is MFA enforced for every user, including the owner and admin accounts?
☐	Is our email domain protected with SPF, DKIM and DMARC, and is advanced email filtering in place?
☐	Is endpoint protection installed, monitored and reporting on every computer and server?
☐	Are operating systems and applications patched on a schedule, with proof?
☐	Are laptops and mobile devices encrypted and able to be wiped if lost?
☐	Do staff receive regular security awareness training and phishing tests?
☐	Are accounts and devices recovered on the day an employee leaves?
☐	Is there a written incident response plan that everyone can find?
☐	Do we know which insurance, client and legal obligations apply to the data we hold?

How did you do? 13–15 yes: strong foundation, keep testing. 8–12: real gaps worth closing soon. Under 8: treat this as urgent; the most likely outcome of an incident today is a long outage.

10. Ten questions to ask your IT provider

1. Show me where my data is backed up, how often, and how long it is kept.
2. When was the last successful test restore, and what exactly was restored?
3. Is any backup copy immutable or offline? Who could delete it, and how?

4. Is Microsoft 365 data backed up separately from Microsoft?
5. How quickly will you be told if a backup fails, and what happens next?
6. Who monitors our security alerts, and what is the response time at 2 a.m. on a Sunday?
7. Is MFA enforced for everyone, and which sign-in methods bypass it?
8. How do you prove patching is current across every machine?
9. What is our written recovery time, and has it ever been rehearsed?
10. Where is our data stored, and does it stay in Canada?

A confident provider answers these with documents and screenshots, not reassurance.

Want a second opinion? Book a free 30-minute data protection review.

Group 4 Networks will walk through this checklist with you, show you where the gaps are and give you a plain-English, prioritized list of fixes. There is no obligation and no pressure.

Book online: calendly.com/group4networks/30min
Call: (416) 623-9677 | **Web:** g4ns.com

© Group 4 Networks. This guide provides general information to help business owners understand data protection. It is not legal, insurance or professional advice, and it does not guarantee any particular outcome. Your environment may need different controls.