Secur-IT
Data Solutions

# Cyber Insurance Readiness Checklist

**Will your business qualify? The controls insurers now require, in plain English.**

*A practical self-check for Ontario and GTA businesses. General guidance, not insurance or legal advice.*

## Why this matters now

Cyber insurance is no longer a formality. Underwriters now verify specific security controls before they will offer coverage or a manageable premium, and they will check whether those controls were actually working if you ever file a claim. If you cannot evidence them, you risk being declined, paying far more, or having a claim denied.

*The good news: the controls insurers ask about are the same controls a managed security provider runs for you every day. Work through this checklist. Each "No" is a gap to close before your next renewal.*

Secur-IT
Data Solutions

# The readiness checklist

## 1. Identity and access

- ☐ **MFA everywhere:** Multi-factor authentication is enforced everywhere: email, VPN, remote access, cloud apps, and all admin accounts.
- ☐ **Least privilege:** Access is least-privilege by role, and accounts are removed promptly when people leave.

## 2. Endpoint protection and detection

- ☐ **EDR / MDR:** Endpoint Detection and Response (EDR) or Managed Detection and Response (MDR) is active on every device.
- ☐ **24/7 monitoring:** Someone is watching alerts 24/7 and can respond, not just collecting them.

## 3. Backups and recovery

- ☐ **Immutable backups:** Backups are immutable or offline, segmented from the network so ransomware cannot reach them.
- ☐ **Tested restores:** Restores are tested on a schedule, not just assumed to work.

## 4. Patching and vulnerabilities

- ☐ **Timely patching:** Operating systems and software are patched promptly, especially critical and internet-facing systems.
- ☐ **Vulnerability scans:** Vulnerability scans run on a schedule and findings are fixed and tracked.

## 5. Email, phishing, and people

- ☐ **Awareness training:** Email filtering is in place, and staff get security awareness training that is recorded.

## 6. Incident response

- ☐ **IR plan:** A documented incident response plan exists, defines roles and escalation, and has been tested (a tabletop at least annually).

## 7. Logging and monitoring

- ☐ **Central logging:** Security logs are centralized and retained long enough to investigate an incident.

## 8. Remote management hardening

- ☐ **RMM / MDM:** Remote management and device-management tools (RMM/MDM) are hardened and protected with MFA, since attackers increasingly target them.

**How to read your result:** mostly “Yes” means you are in good shape to qualify, keep the evidence tidy. A mix means real gaps that underwriters will flag, fixable in weeks. Mostly “No” means start now, before renewal, with MFA, EDR/MDR, and tested backups first.

Secur-IT Data Solutions

## How Secur-IT Data helps

We run these controls for Ontario businesses as a managed service: 24/7 monitoring and MDR, endpoint protection, backups, patching and vulnerability management, incident response, and awareness training. We also help you answer the underwriting questionnaire accurately and produce the evidence insurers ask for, so renewal is not a scramble. Toronto-based, Canadian-owned, and your data stays in Canada.

**Not sure where you stand? Book a free security assessment at securitdata.ca**

---

*General information, not insurance or legal advice. Coverage terms and underwriting requirements vary by insurer and policy. Confirm your specific requirements with your broker or insurer.*