Secur-IT
Data Solutions

Cyber Security Health Check

The ten controls that decide whether your business is an easy target.

A practical self-check for Canadian small and midsize businesses. General guidance, not legal advice.

How to use this

These are the ten controls that stop most real attacks on small and midsize businesses. Work down the list and tick each one you can honestly say is fully in place. Every box you cannot tick is a gap an attacker would look for, and the place to start.

This is the same set of controls scored by the free 2 minute health check at securitdata.ca/cyber-security-health-check.

Secur-IT
Data Solutions

The ten point health check

1. Backups

- [ ] **Tested, immutable backups:** You have working, tested backups that are kept offline or immutable, so ransomware cannot reach or destroy your only copy.

2. Multi-factor authentication

- [ ] **MFA everywhere:** MFA is enforced on email and every critical account, not just some of them. This alone stops the majority of account takeovers.

3. Endpoint protection

- [ ] **Managed EDR:** You run modern endpoint protection (EDR) that detects behaviour and catches attacks in progress, not just basic antivirus that only knows old viruses.

4. Patching

- [ ] **Timely patching:** Systems and software are patched promptly, within days of a critical update, on a defined schedule. Unpatched systems are the most common way in.

5. Email security

- [ ] **Advanced email filtering:** Email is filtered for phishing, spoofing, and business email compromise, beyond the built-in provider filter. Most breaches still start with an email.

6. Monitoring

- [ ] **24/7 monitoring / SOC:** Someone is actually watching your systems for threats around the clock. Most attacks happen nights and weekends, outside business hours.

7. Incident response

- [ ] **Tested IR plan:** You have a written incident response plan for a breach tomorrow, and you have practised it. Roles and escalation are decided before you need them.

8. People

- [ ] **Ongoing awareness training:** Your team gets regular security awareness training and phishing tests. Your people are the most attacked layer, so keep it ongoing.

9. Vendors and third parties

- [ ] **Vendor access inventory:** You know which vendors and tools can access your data, and they are secured. Supply chain and third-party risk is rising fast.

10. Ownership

- [ ] **A clear owner:** Cyber security has a clear owner, a dedicated provider or team, so it stops falling through the cracks between whoever has time.

How to read your result: eight or more boxes ticked means you are ahead of most Canadian SMBs, keep it that way. A mix means real, fixable gaps worth closing now. Fewer than half means high exposure, start with backups, MFA, and managed EDR 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 detection, endpoint protection, tested backups, patching and vulnerability management, email security, incident response, and awareness training. Toronto-based, Canadian-owned, and your data stays in Canada.

Want a real set of eyes on your gaps? Book a free security assessment at securitdata.ca

General information only, not legal advice. Every business is different, confirm your specific requirements with a qualified security advisor.