

Cyber Insurance Readiness Checklist

ITBizTek - Toronto & GTA Small Business Guide, 2026

What insurers commonly look for before they'll quote or renew

1 Multi-factor authentication on email and remote access

Insurers commonly ask whether MFA is turned on for email, VPN, and any remote admin access, not just for a subset of accounts.

2 Backups that are tested and kept offline or immutable

A backup that lives on the same network as everything else can be encrypted right along with it. Insurers often want to know backups are separated and that a restore has actually been tested.

3 Endpoint protection beyond basic antivirus

Many applications now ask specifically about endpoint detection and response (EDR), which watches for suspicious behaviour rather than only matching known virus signatures.

4 A written incident response plan

Even a short document naming who does what in the first hours of an incident is frequently on the application checklist.

5 A regular patching and update schedule

Unpatched software is one of the most common ways attackers get in. Insurers often ask how often systems are updated and who is responsible for it.

6 Employee phishing awareness training

Since many claims start with a clicked link or a fake invoice, some insurers ask whether staff get any regular training on spotting phishing attempts.

7 Controls on admin and privileged accounts

Applications often ask how many people have administrator access and whether that access is reviewed periodically.

8 Email authentication (SPF, DKIM, DMARC)

These records help stop attackers from sending email that looks like it came from your own domain, a common tactic in business email compromise.

9 A current inventory of devices and software

Knowing what is actually connected to the network, and what is running on it, is a basic starting point most applications ask about in some form.

Not sure where your business stands? ITBizTek helps Toronto and GTA businesses get cyber insurance ready.