

Before you sign your cyber insurance application

What each security question really commits you to, where honest answers go wrong, and a 30-minute self-check before you sign.

9-minute read

30-minute self-check

Updated October 2026

What each security question actually commits you to, where honest people get caught, and what to check first.

WHY THIS MATTERS MORE THAN THE PREMIUM

The application is not a survey. It becomes part of the policy, and you sign a declaration that the answers are true.

- **In Quebec**, the Civil Code (arts. 2408-2411) requires you to declare every fact you know that is likely to materially influence the insurer's decision or premium. If an answer turns out to be wrong, the insurer can have the policy annulled if it would not have covered you had it known. Absent fraud, it can instead cut the claim payout in proportion to the premium it should have charged. Your answers have to stay true during the policy too: you must promptly tell your insurer about changes that increase the risk (art. 2466).
- **Elsewhere in Canada**, provincial insurance law and the policy wording work in a similar direction: a material misrepresentation can void coverage.
- **What it looks like in practice:** in *Travelers v. International Control Services* (U.S., 2022), the applicant said MFA protected administrative and privileged access. After a ransomware attack, Travelers alleged that MFA protected only the firewall. ICS agreed to rescind the policy, treating it as if it had never existed, and the court dismissed the case. It was settled, not decided on the merits, and it is a US case, but the mechanics are the same here. The answer that loses the claim is usually a "yes" that was true for *some* systems.

The rule we give clients: answer for your weakest system, not your best one. If the true answer is "mostly," answer "no" and attach an explanation. A "no" with a remediation date may raise your premium, add an exclusion or get you declined. A false "yes" can wipe out your coverage after the incident.

THE QUESTIONS AND THEIR TRAPS

The wording below follows patterns common to real cyber insurance applications. Your insurer's wording will differ, so read theirs word by word.

1. Multi-factor authentication

Typical wording: "MFA enforced to secure **all** remote access to your network." "MFA enforced to secure internal use of privileged accounts (administrator accounts, **service accounts**, etc.)." "MFA enforced for email access via webmail portal,

mailbox applications and **non-corporate devices** for all employees.”

The traps

- ◇ **“All remote access” includes your MSP and vendors.** Your IT provider’s remote management tool (ConnectWise, N-able, TeamViewer, AnyDesk), the HVAC or accounting vendor’s VPN account, the old “temporary” remote desktop for the contractor: if any of these get in without MFA, the answer is no. Ask your MSP in writing how *their* access to you is protected.
- ◇ **“Remote access” is broader than the VPN.** One carrier defines it as access to “a device, corporate web based service or network from any location.” Cloud apps reachable from home count.
- ◇ **Some mail logins still skip MFA.** SMTP AUTH with a plain password (often left on for scanners, printers or a line-of-business app), app passwords, on-premises Exchange, and mail hosted outside Microsoft 365/Google can all accept a password without a second factor. “MFA on email” is only true if those paths are off or restricted to named devices.
- ◇ **Service accounts and break-glass admins.** Applications ask about privileged accounts “including service accounts.” Most small environments have at least one domain admin or backup service account with no MFA and a password that hasn’t changed in years.
- ◇ **Certificates and shared keys aren’t MFA.** At least one carrier states that modern MFA “does not include static authentication methods such as certificates or pre-shared keys.”
- ◇ **“Enforced” means a policy, not registration.** If users registered MFA but a Conditional Access exception excludes them (the CEO, “because it’s annoying”), the answer is false.

Self-check: export your MFA registration report and your Conditional Access policies (or Google 2SV enforcement). List every exclusion. List every way an outsider reaches a machine inside your network. Check whether SMTP AUTH is enabled anywhere in your tenant.

2. Backups

Typical wording: checkboxes such as “Copy of backups are kept **offline** or **air-gapped**,” “Backup solution with **immutable** backups,” “Backup servers are **not joined to a Windows domain**,” “**MFA required** for access to backups,” “Backup servers and user accounts use **unique credentials**.”

The traps

- ◇ **Offline, immutable and cloud are three different answers.** *Offline* = disconnected, so the attacker cannot reach it. *Immutable* = online, but cannot be changed or deleted until a retention date, even by an admin. *Cloud* = stored somewhere else, which says nothing about whether a stolen admin password can delete it. A Synology NAS on the same network with a scheduled USB copy is none of the three.
- ◇ **Domain-joined backup servers.** If the backup server logs in with the same Active Directory the attacker just took over, the attacker owns the backups. This is a common way ransomware crews delete backups before encrypting.
- ◇ **“Tested” means a restore, not a green checkmark.** Underwriters increasingly ask when you last did a restore, and how long it took. Your backup software reporting “job succeeded” is not a restore test.

- ◇ **SaaS data.** Microsoft 365 and Google Workspace retention is not a backup in the sense insurers mean. If your files live in SharePoint/OneDrive, say how they're backed up.

Self-check: Can a domain admin password delete your backups? If you're not sure, assume yes. When did you last restore a full server, and how long did it take? Write down the date and the duration.

3. Endpoint protection (EDR / MDR)

Typical wording: "What Endpoint Security Technology do you have in place? Next Gen Antivirus / Endpoint Detection & Response (EDR) / Managed Detection & Response (MDR) / Extended Detection & Response (XDR)," with a field to name the product and vendor. Other carriers ask whether EDR is deployed on **all** endpoints and servers and whether alerts are **monitored 24/7**.

The traps

- ◇ **EDR is a tool; 24/7 monitoring is a service.** If the question says "monitored 24/7" and the alerts go to your IT person's inbox, the answer is no. A 24/7 yes means an MDR provider, or an MSP with a real round-the-clock SOC. Get it in the contract.
- ◇ **"All endpoints" means all.** Compare the EDR console's device count against your asset inventory. The gap is almost always servers (especially the old one nobody touches), and that's where attackers land.
- ◇ **Defender is not automatically EDR.** Microsoft Defender Antivirus in Business Basic/Standard is not Defender for Endpoint or Defender for Business. Check the licence, not the logo.
- ◇ **Name the product correctly.** Underwriters check product names against what they consider EDR.

Self-check: EDR device count ÷ total devices (including servers) = __%. Who gets paged at 3 a.m. on a Sunday? A name, not "the MSP."

4. Exposed remote desktop and edge devices

Typical wording: "Do you allow remote access via RDP?" / "Is RDP exposed to the internet?" Some carriers skip the question and **scan you from outside** before quoting, so an exposed RDP port shows up whatever you answer.

The traps

- ◇ **The insurer may already know the answer.** If you say "no RDP" and their scan finds port 3389 open on an IP you forgot, you have a misrepresentation on file before you sign.
- ◇ **The VPN box counts too.** Unpatched firewalls and VPN appliances (Fortinet, SonicWall, Cisco, Ivanti, Citrix) have been among the most exploited entry points of the last few years. Insurers ask about patching for exactly this reason.

Self-check: Look at yourself from the outside before the insurer does. A vulnerability assessment shows you what they will see.

5. Patching and end-of-life systems

Typical wording: “How quickly are critical patches applied?” “Do you run any unsupported or end-of-life software?”

The traps

- ◇ **Your patch policy is judged on the worst machine.** The Windows Server 2012 box running the old accounting software, or a Windows 10 machine past end of support (October 2025), makes “no unsupported software” false. The exceptions are machines enrolled in Microsoft’s Extended Security Updates, or machines that are isolated and disclosed.
- ◇ **Firmware counts.** Firewalls, VPNs, NAS devices and printers are “systems.”

Self-check: list every system on an unsupported OS or firmware. For each one: ESU enrolled? Isolated? Replacement date?

6. Training and phishing

Typical wording: “Do you conduct employee security training or phishing training, for all employees, at least annually?”

The trap: “All employees” includes the owner and the part-timers. Keep completion records; that’s the evidence they’ll ask for.

7. Payment verification

Typical wording: “Prior to executing an electronic payment, do you verify the validity of the funds transfer request or payment change request, with the requestor, via a separate means of communication?”

The traps

- ◇ **Calling the number in the email is not a separate channel.** The verification has to use a number you already had on file.
- ◇ **It has to apply to everyone, including the boss.** BEC fraud works by impersonating the boss who “needs this done now.”
- ◇ **Social engineering fraud is often a sub-limit.** Many policies cap payment-fraud losses well below the main limit, or exclude them without a verification procedure. Read the funds transfer / social engineering section and its limit.

Self-check: Is the call-back rule written down, and would your accounts payable clerk follow it if the owner said to skip it?

8. Prior incidents and “knowledge”

Typical wording: “In the past three years, have you experienced any cyber security incident...” and “Do you... have knowledge of any actual or alleged security breach... that may reasonably be expected to give rise to a claim?”

The traps

- ◆ **A prior BEC or a compromised mailbox counts as an incident**, even if no money moved and nobody reported it.
- ◆ **“Knowledge” is wide.** If IT flagged suspicious logins last month, disclose them. Known-but-undisclosed incidents are among the cleanest grounds for denying a claim.
- ◆ **Your Law 25 register is a record of what you knew.** The Commission d'accès à l'information can ask for it, and it may come out in a claim dispute. If an incident is in your register, it should be on your application.

PRE-APPLICATION SELF-CHECK (30 MINUTES WITH YOUR IT PROVIDER)

Answer each with evidence, not memory.

- 1 ☐ MFA enforced on every mailbox, with password-only paths (SMTP AUTH, app passwords, legacy servers) off or restricted. **Evidence:** Conditional Access policy export + list of exclusions (should be empty or break-glass only).
- 2 ☐ MFA on every path into the network, including MSP tools and vendor accounts. **Evidence:** written inventory of remote access paths and how each is protected.
- 3 ☐ MFA on all admin accounts, including service and break-glass accounts. **Evidence:** list of privileged accounts.
- 4 ☐ At least one backup copy that a stolen domain admin password cannot delete (offline or immutable, separate credentials, MFA on the console). **Evidence:** screenshot of immutability/retention lock settings.
- 5 ☐ A full restore tested in the last 12 months. **Evidence:** date, system, time to restore.
- 6 ☐ EDR on 100% of workstations *and servers*. **Evidence:** console count vs. inventory.
- 7 ☐ Named 24/7 monitoring if you'll claim it. **Evidence:** MDR/SOC contract.
- 8 ☐ No RDP, SMB or admin panels exposed to the internet; edge devices patched. **Evidence:** external scan.
- 9 ☐ Unsupported systems listed, isolated or ESU-enrolled, with replacement dates.

- 10 ☐ Annual training for all staff, with completion records.
- 11 ☐ Written call-back rule for payment and banking changes.
- 12 ☐ Every incident in the last 3 years (including mailbox compromises) listed for disclosure.
- 13 ☐ Incident response plan with the insurer's breach line in it (see our first-hour card).

Any box you can't tick: answer "no" and attach a short note with a remediation date. Underwriters see "no, fixed by March 31" every day. A "yes" they disprove after a claim is the expensive version.

WHAT UNDERWRITERS ACTUALLY ASK FOR

More and more, a "yes" needs proof, at application, at renewal or after a claim:

- Screenshots of MFA / Conditional Access policies and registration reports.
- EDR console exports showing coverage, and the name of the 24/7 provider.
- Backup configuration (immutability, retention, separate credentials) and a restore test record.
- Their own outside-in scan results, which you'll be asked to explain or fix before binding.
- Supplemental ransomware questionnaires that go deeper on the same controls.

Keep a folder of this evidence, dated, next to your signed application. If you ever file a claim, it's the first thing your breach coach will want.

This guide is not legal or insurance advice. Your broker should review your answers before you sign.

We review applications with clients before they sign. Get in touch.

Get a second pair of eyes.

Talk directly to the expert who would lead the work.

 **PRIVATEER**
CYBERSECURITY
privateer.ca · info@privateer.ca