

CYBER INSURANCE

Demystifying Cyber Insurance Questionnaires

What insurers ask, what they mean, and how to answer honestly without losing coverage.

Cyber insurance applications are full of technical questions, and the answers matter. Inaccurate answers can raise premiums, lead to denied coverage, or put a future claim at risk. This guide translates the questions insurers ask most and lists what you should have in place before you sign.

How to use it: tick what you have in place today. Anything left unticked is a conversation worth having.

01 Identity and access

- ☐ **Multi-factor authentication on email**
Usually the first question. Insurers mean every mailbox, not just executives.
- ☐ **Multi-factor authentication on remote access and admin accounts**
VPN, remote desktop, cloud consoles, and backup systems.
- ☐ **Separate administrator accounts**
Daily work is done without admin rights.
- ☐ **Prompt removal of access for departed staff**
Often asked as "do you have an offboarding process".
- ☐ **Privileged access reviewed at least annually**
Know who holds the keys.

02 Protection and detection

- ☐ **Endpoint detection and response (EDR) on all devices**
Traditional antivirus alone may not satisfy this question.
- ☐ **24/7 monitoring of security alerts**
Insurers want someone watching after hours.
- ☐ **Email filtering with attachment and link scanning**
Phishing is the top claim driver.
- ☐ **Patching within a defined window for critical updates**
Be ready to state your actual timeline.
- ☐ **No end-of-life systems, or documented isolation of the ones you have**
Old servers are a common surprise exclusion.
- ☐ **Security awareness training with phishing simulations**
Keep completion records.

03 Recovery and response

- ☐ **Backups with an offline, immutable, or separate-credential copy**
Ransomware targets connected backups first.
- ☐ **Restores tested on a schedule**
Insurers ask whether you have tested, not just whether you back up.
- ☐ **Written incident response plan**
Including who calls the insurer and breach counsel.
- ☐ **Payment and wire verification procedure**
Social engineering coverage often requires it.
- ☐ **Vendor and remote access controls**
Third-party access is a frequent breach path.

Red flags we see most

- You answered "yes" to multi-factor authentication but some mailboxes are exempt.
- Backups use the same admin password as the network.
- You have never tested a restore.
- Nobody at the company can explain the answers on last year's application.

Where to start

Fill out the questionnaire with your IT partner in the room. If an honest answer is "no", fix the gap before renewal instead of guessing.

Want a second set of eyes?

Book a free 30-minute IT assessment. A senior technician walks through this checklist with you and tells you what to fix first. No sales script, no obligation.

Book a free assessment

(813) 999-0086

swfit.io/free-consultation