POLICYSCORE

Before your cyber insurance renewal

Six things cyber insurance applications commonly ask about, in plain language. Check each box you can prove, and start with the ones you can't.

1 MFA in three places

- [ ] Email, including webmail and phones
- [ ] All remote access: VPN, remote desktop and your IT provider's remote support tools
- [ ] Admin and privileged accounts, including backup and cloud consoles (the one people forget)

2 Backups you can restore

- [ ] At least one copy offline, immutable or otherwise out of an attacker's reach
- [ ] Backup logins separate from your everyday admin accounts
- [ ] A restore actually tested, with the date and how long it took written down

3 The payment call-back

- [ ] Before changing any vendor's bank details, call back on a number you already had
- [ ] The procedure is written down
- [ ] Whoever pays the bills knows it

4 The old PC in the corner

- [ ] List any system that can't get security updates anymore
- [ ] Keep it off the internet if you can
- [ ] Put a replacement or isolation plan on the calendar, with a date

5 Proof for every "yes"

- [ ] MFA: an enrollment report or screenshot
- [ ] Backups: a restore test log
- [ ] Policies: a signed copy

6 Timing

- [ ] Answer the questionnaire internally first
- [ ] Share results with your broker early, not the week it's due
- [ ] Fix the gaps you can before you sign

Shared with you by: _____

See your insurance red flags in 16 free questions: **policyscore.io/insurance**

General information, not insurance advice. Carriers make their own decisions and questions vary by carrier. PolicyScore is a self-assessment tool, not a certification or insurance product. © 2026 Quarterdeck Software LLC.