CYBER INSURANCE READINESS CHECK · OCTOBER 2026

Ready for your cyber insurance application? 18 questions to find out.

Answer each question the way an insurance application or ransomware supplement would ask it. Insurer must-haves count for more. Total your score on the last page, then close the must-have gaps before your renewal.

01
Answer
The security questions that show up on cyber insurance applications and ransomware supplements.

02
Score
The controls insurers treat as must-haves count most. Your grade updates as you go.

03
Fix
Get the gaps to close before your renewal, most important first — and print or save them for your broker.

COMPANY _____ DATE _____

COMPLETED BY _____ REVIEWED WITH _____

866.24.CALIT info@calitgroup.com calitgroup.com/cyber-insurance-readiness-check

01 MFA & admin access

The first thing most insurers ask about. Missing MFA is a common reason for higher premiums, exclusions or a declined application.

1 Is MFA required for every user’s email, including on phones and webmail?

Insurer must-have · worth 6 points

WHAT INSURERS WANT TO SEE
Every mailbox in Microsoft 365 or Google Workspace, with legacy sign-in methods that skip MFA turned off.

IF NOT, FIX IT
Turn on MFA for every mailbox and block legacy authentication, so a stolen password alone can’t open email.

Our answer: ☐ Yes (6) ☐ Partly / not sure (3) ☐ No (0)

2 Is MFA required for all remote access — VPN, remote desktop and cloud apps?

Insurer must-have · worth 6 points

WHAT INSURERS WANT TO SEE
Anyone connecting from outside the office proves who they are with a second factor.

IF NOT, FIX IT
Require MFA on the VPN, remote desktop gateways and every cloud app that holds company data.

Our answer: ☐ Yes (6) ☐ Partly / not sure (3) ☐ No (0)

3 Is MFA required for every administrator account, including backup and email admin consoles?

Insurer must-have · worth 6 points

WHAT INSURERS WANT TO SEE
Domain admins, Microsoft 365 or Google admins, firewall and backup consoles.

IF NOT, FIX IT
Put MFA on every privileged account and admin console — attackers go after these first.

Our answer: ☐ Yes (6) ☐ Partly / not sure (3) ☐ No (0)

4 Do staff work without administrator rights, with admin accounts kept separate?

Important · worth 4 points

WHAT INSURERS WANT TO SEE
Everyday accounts can’t install software; IT uses separate admin accounts only for admin work.

IF NOT, FIX IT
Remove everyday admin rights and give IT separate, MFA-protected admin accounts.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

5 Is vendor and outside remote access controlled — named accounts, MFA, and on only when needed?

Important · worth 4 points

WHAT INSURERS WANT TO SEE
Software vendors and outside IT sign in with their own MFA-protected accounts, and their remote-access tools aren't left running all the time.

IF NOT, FIX IT
Give each vendor a named, MFA-protected account, turn off always-on remote tools and log every session.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

02 Devices & patching

Endpoint detection and response, timely patches, no unsupported systems and encrypted laptops.

6 Is endpoint detection and response (EDR) on every computer and server, watched 24×7?

Insurer must-have · worth 6 points

WHAT INSURERS WANT TO SEE
EDR such as SentinelOne on 100% of endpoints, with a security team responding to alerts around the clock.

IF NOT, FIX IT
Deploy managed EDR on every endpoint and server, monitored by a 24×7 SOC.

Our answer: ☐ Yes (6) ☐ Partly / not sure (3) ☐ No (0)

7 Are critical security patches installed within 30 days — and urgent ones within days?

Important · worth 4 points

WHAT INSURERS WANT TO SEE
Operating systems, browsers and common apps patched on a schedule, with anything overdue tracked.

IF NOT, FIX IT
Automate patching for operating systems and third-party apps, and track anything that falls behind.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

8 Are you free of unsupported (end-of-life) systems and software?

Important · worth 4 points

WHAT INSURERS WANT TO SEE
No Windows versions, servers or apps that no longer get security updates — or they're isolated from the network.

IF NOT, FIX IT
Replace or isolate unsupported systems; insurers often ask about them by name.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

9 Is remote desktop (RDP) closed to the internet?

Insurer must-have · worth 6 points

WHAT INSURERS WANT TO SEE
Nobody can reach a computer's remote desktop directly from the internet; remote access goes through a VPN or gateway with MFA.

IF NOT, FIX IT
Close any internet-exposed remote desktop and move remote access behind an MFA-protected VPN or gateway.

Our answer: ☐ Yes (6) ☐ Partly / not sure (3) ☐ No (0)

10 Are firewalls, VPNs and other internet-facing devices patched within days of an urgent fix?

Insurer must-have · worth 6 points

WHAT INSURERS WANT TO SEE
Edge devices — firewalls, VPN gateways and remote-access appliances — get critical updates quickly, and ones that no longer receive updates are replaced.

IF NOT, FIX IT
Put internet-facing devices on a fast patch cycle and replace any that are past end of support — attackers scan for them first.

Our answer: ☐ Yes (6) ☐ Partly / not sure (3) ☐ No (0)

11 Are laptops encrypted and can a lost one be wiped remotely?

Good practice · worth 2 points

WHAT INSURERS WANT TO SEE
BitLocker or FileVault on every laptop, managed centrally.

IF NOT, FIX IT
Encrypt every laptop and enroll devices in management so a lost one can be locked and wiped.

Our answer: ☐ Yes (2) ☐ Partly / not sure (1) ☐ No (0)

03 Backups & recovery

Backups ransomware can't reach, and proof that you can restore from them.

12 Are backups kept offline, immutable or otherwise out of ransomware's reach?

Insurer must-have · worth 6 points

WHAT INSURERS WANT TO SEE
A copy that can't be encrypted or deleted from your network, with separate credentials and MFA.

IF NOT, FIX IT
Keep an off-site or immutable backup copy that ransomware and stolen admin passwords can't reach.

Our answer: ☐ Yes (6) ☐ Partly / not sure (3) ☐ No (0)

13 Have you tested restoring from backup in the last six months?

Important · worth 4 points

WHAT INSURERS WANT TO SEE
An actual restore of files or a server, with the time it took written down.

IF NOT, FIX IT
Test restores on a schedule and record how long recovery takes.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

04 Email, people & payments

Phishing and payment fraud drive a large share of claims.

14 Do you have advanced email filtering and SPF, DKIM and DMARC set up?

Important · worth 4 points

WHAT INSURERS WANT TO SEE
Filtering for malicious links, attachments and impersonation, plus domain records that stop spoofing.

IF NOT, FIX IT
Add advanced email security and move your domain's DMARC policy to enforcement.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

15 Does everyone get security awareness training every year and phishing tests every quarter?

Important · worth 4 points

WHAT INSURERS WANT TO SEE
Completion and phishing results tracked, so you can show them.

IF NOT, FIX IT
Start annual security awareness training with quarterly simulated phishing.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

16 Do you confirm every new payment request or change in bank details by phone?

Insurer must-have · worth 6 points

WHAT INSURERS WANT TO SEE
A call-back to a number you already have, never one in the email — and a second approver for large payments.

IF NOT, FIX IT
Write a payment verification procedure: call-back on a known number and dual approval above a set amount.

Our answer: ☐ Yes (6) ☐ Partly / not sure (3) ☐ No (0)

05 Monitoring & response

Someone watching around the clock, and a plan for the day something gets through.

17 Are security logs collected and watched by someone 24×7?

Important · worth 4 points

WHAT INSURERS WANT TO SEE
A managed SIEM or security operations center reviewing alerts at night and on weekends.

IF NOT, FIX IT
Get 24×7 monitoring: a managed SIEM with a SOC that reviews and acts on alerts.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

18 Do you have a written incident response plan, tested in the last year?

Important · worth 4 points

WHAT INSURERS WANT TO SEE

Who to call first — including your insurer's claims line — and what to do in the first hour.

IF NOT, FIX IT

Write a one-page incident response plan and run a tabletop exercise with leadership once a year.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

SCORECARD

Total your score.

Add the points for each area, out of 86. Any “No” on a insurer must-have item is worth fixing first, whatever the total.

AREA	QUESTIONS	SCORE
01 · MFA & admin access	5	/ 26
02 · Devices & patching	6	/ 28
03 · Backups & recovery	2	/ 10
04 · Email, people & payments	3	/ 14
05 · Monitoring & response	2	/ 8
Total	**18**	**/ 86**

A · 78+
Ready — keep the evidence handy

B–C · 56+
Close the gaps before you apply

D · 43+
Expect hard questions or higher premiums

F · under 43
Coverage at risk — start now

WANT AN ENGINEER TO CHECK IT FOR REAL?

Want help before your renewal?

Configured, not just installed
A self-check shows what’s in place. We check whether it’s set up well and actually monitored.

Discreet
We can work around your current provider and sign an NDA.

Plain-language report
We check each control for real, close the gaps and help you answer the security section of your application accurately — with evidence.

No obligation
Use the results with us, your current provider or anyone else.

Book at calitgroup.com/contact

866.24.CALIT

A general guide based on common insurance application questions — not insurance or legal advice.