CYBER RISK SELF-CHECK · OCTOBER 2026

How exposed is your business? 12 questions to find out.

Answer each question about the controls attackers — and cyber insurers — care about most. High-priority controls count for more. Total your score on the last page, then start with the gaps marked high priority.

01
Answer
Tick yes, partly or no for each control.

02
Score
Add the points by area, out of 50 in total.

03
Fix
Close the high-priority gaps first, then the rest.

COMPANY _____ DATE _____

COMPLETED BY _____ REVIEWED WITH _____

866.24.CALIT info@calitgroup.com calitgroup.com/cyber-risk-check

01 Identity & access

Stolen passwords are the most common way in. Lock the front door first.

1 Is multi-factor authentication (MFA) required for everyone’s email and remote access?

High priority · worth 6 points

WHAT GOOD LOOKS LIKE
A code or app approval in addition to the password — for every user, not just some.

IF NOT, FIX IT
Turn on MFA for every user’s email, VPN and remote access. It blocks the vast majority of account takeovers.

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

2 Do staff work without administrator rights on their computers?

Important · worth 4 points

WHAT GOOD LOOKS LIKE
Admin access kept to separate accounts used only by IT.

IF NOT, FIX IT
Remove everyday admin rights and use separate admin accounts. It stops most malware from installing itself.

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

3 Do you use a password manager instead of shared or reused passwords?

Good practice · worth 2 points

WHAT GOOD LOOKS LIKE
No spreadsheets, sticky notes or one password for everything.

IF NOT, FIX IT
Roll out a business password manager so every account gets a unique password and shared logins are controlled.

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

02 Devices

Every laptop and server is a target — protected, patched and recoverable.

4 Is every computer protected by EDR that someone watches around the clock?

High priority · worth 6 points

WHAT GOOD LOOKS LIKE
Endpoint detection and response (like SentinelOne), monitored 24×7 — not just free antivirus.

IF NOT, FIX IT
Put managed EDR on every computer and server, with a 24×7 SOC watching the alerts.

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

5 Are Windows, Mac and app updates installed automatically within 30 days?

Important · worth 4 points

WHAT GOOD LOOKS LIKE
Including third-party apps like browsers, Zoom and Adobe.

IF NOT, FIX IT
Automate operating-system and third-party patching, and track anything that's falling behind.

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

6 Are laptops encrypted and can you wipe a lost one remotely?

Good practice · worth 2 points

WHAT GOOD LOOKS LIKE
BitLocker or FileVault, managed centrally.

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

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

03 Email & people

Most attacks start with an email. Filter what you can, train for the rest.

7 Do you have email security beyond what comes built in?

Important · worth 4 points

WHAT GOOD LOOKS LIKE
Advanced filtering for phishing links, attachments and impersonation.

IF NOT, FIX IT
Add advanced email security that checks links and attachments and flags impersonation of your executives and vendors.

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

8 Does your team get security awareness training every year and phishing tests every quarter?

Important · worth 4 points

WHAT GOOD LOOKS LIKE
Annual training plus simulated phishing emails every quarter, with results tracked.

IF NOT, FIX IT
Start annual security awareness training with quarterly simulated phishing so your team learns to spot and report scams.

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

04 Backup & recovery

When everything else fails, backups are what you go back to.

9 Are servers and Microsoft 365 or Google Workspace backed up off-site, where ransomware can't reach them?

High priority · worth 6 points

WHAT GOOD LOOKS LIKE
Off-site or immutable copies — not just a USB drive or sync folder.

IF NOT, FIX IT
Back up servers and cloud email and files off-site, with copies ransomware can't encrypt or delete.

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

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

Important · worth 4 points

WHAT GOOD LOOKS LIKE
Actually restoring files or a server, not just checking that backups ran.

IF NOT, FIX IT
Schedule restore tests and document how long recovery takes, so you know the backups work before you need them.

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

05 Response & oversight

Someone has to be watching — and know what to do when something happens.

11 Do you have a written plan for a cyber incident — who to call and what to do first?

Important · worth 4 points

WHAT GOOD LOOKS LIKE
Including your insurer, IT provider, bank and legal contacts.

IF NOT, FIX IT
Write a one-page incident response plan with names, numbers and first steps, and walk through it once a year.

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

12 Does someone review security alerts, vulnerabilities and firewall activity regularly?

Important · worth 4 points

WHAT GOOD LOOKS LIKE
A person or team actually looking — ideally 24×7 — not just alerts going to an inbox.

IF NOT, FIX IT
Get 24×7 monitoring with a team that reviews alerts and vulnerability scans and acts on them.

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

SCORECARD

Total your score.

Add the points for each area. Any “No” on a high-priority control is worth fixing first, whatever the total.

AREA	QUESTIONS	SCORE
01 · Identity & access	3	/ 12
02 · Devices	3	/ 12
03 · Email & people	2	/ 8
04 · Backup & recovery	2	/ 10
05 · Response & oversight	2	/ 8
Total	**12**	**/ 50**

A · 45+
Strong — keep it verified

B–C · 33+
Solid, with gaps to close

D · 25+
Significant exposure

F · under 25
High risk — start now

WANT AN ENGINEER TO CHECK IT FOR REAL?

A free, on-site network health assessment

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
Risks ranked by priority, quick wins and longer-term fixes — yours to keep.

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

Book at calitgroup.com/network-health-assessment

866.24.CALIT

A quick, general guide based on your answers — not a security audit, and not legal or insurance advice.