CHECKLIST

Cyber Insurance Renewal Readiness Checklist

The control questions cyber insurance applications ask most often, in rough submission order, with the evidence each answer needs, the gap that usually turns up, and the answer worth aiming for at the next renewal.

WHO IT IS FOR

Whoever owns the cyber insurance renewal — often a finance or operations lead without a security team — working four to eight weeks ahead of the submission date.

LAST REVIEWED

14 September 2026

READING TIME

16 minutes

ON THIS PAGE

A cyber insurance application is an evidence request with a deadline attached. The wording changes between insurers and years, but the subject matter

barely moves: where multi-factor authentication reaches, who holds administrator rights, whether backups can be restored, what protects endpoints and email, how fast patches go on, and whether anyone has rehearsed a bad day.

This checklist takes those questions in roughly the order applications ask them. For each: what it is really testing, what counts as evidence rather than assertion, the common gap, and two answers — the one you can support today and the one you want to give at the next renewal. Keeping those two apart stops the application becoming a statement of intent.

Forms differ, so treat your broker's current application as the master document and this checklist as the working method behind it.

PART 1 OF 5

Before you start: gather what already exists

- Last year's completed application. This year's answers should match it or explain what changed.
- This year's form and the policy schedule, including any conditions attached. Read the conditions with your broker; underwriters often ask about them first.
- Who answered each section last time. Where that person has left, the question has no owner yet.
- Contracts with your managed service, backup and security providers, and a record of any incident, claim or notification since the last application.

PART 2 OF 5

The recurring control questions, in rough submission order

“Today” is the accurate answer from what you already hold. “Next renewal” is the position worth working towards over the policy year.

01

Is multi-factor authentication enforced for email, remote access, privileged accounts and backup consoles?

WHY IT MATTERS

The question is about reach, not existence: could one stolen password still open email, remote access, an administrator account or the backup console? Exceptions — service accounts, legacy protocols, a supplier's remote desktop connection — are where answers turn partial.

EVIDENCE THAT HOLDS UP

- A dated export of the MFA or conditional access policy, showing who and what it covers, and who is excluded.
- The exclusion list, with a reason and a compensating restriction for each account.
- Configuration showing that every remote access route and the backup console require MFA.
- **Assertion, not evidence:** a policy saying MFA is required, or IT saying it is "on everywhere".

WHERE IT USUALLY FALLS SHORT

MFA on staff email but not on the backup console, firewall management or your IT provider's accounts. Service accounts excluded years ago with no recorded reason.

WHAT YOU CAN SUPPORT TODAY

Answer route by route. List excluded accounts, what restricts them and when they will be covered. A qualified yes with a list survives follow-up questions; an unqualified yes may not.

WHAT TO AIM FOR AT RENEWAL

MFA on every route the form names, legacy authentication blocked, and a reviewed exception register with a dated export on file.

02

How are privileged and administrator accounts controlled?

WHY IT MATTERS

An attacker with administrator rights can usually switch off backups and endpoint protection. The underwriter wants a small, known group holding those rights, separate accounts for administrative work, and someone checking the list.

EVIDENCE THAT HOLDS UP

- A current list of administrator accounts across identity, servers, cloud services, firewall and backups, each with a named owner.
- Evidence that administrators use separate accounts for administrative work.
- The last privileged access review: who reviewed, the date, and what was removed.
- **Assertion, not evidence:** “only IT has admin rights”, with no list and no review date.

WHERE IT USUALLY FALLS SHORT

Nobody can produce the list quickly. Former staff or suppliers still hold rights, and everyday accounts or laptops carry permanent administrator privileges.

WHAT YOU CAN SUPPORT TODAY

Produce the list and remove what should not be on it before answering. If separate administrative accounts are not in place, say so and describe what limits the risk now.

WHAT TO AIM FOR AT RENEWAL

Separate administrative accounts, a recorded review on a regular cycle, and local administrator rights removed from standard devices.

03

Are backups kept offline or immutable, separated from the main network, and restore-tested?

WHY IT MATTERS

This is the ransomware question: could someone who controls your network also destroy your backups, and can you actually recover? A backup that reports success and a restore that works are different events, and the restore is the one that usually lacks evidence.

EVIDENCE THAT HOLDS UP

- Configuration or a provider statement showing an immutable or offline copy, with credentials separate from the main directory.
- A restore test record: date, what was restored, from which backup, time taken, result and who ran it.
- The systems in backup scope, including cloud email and file storage, and any deliberate exclusions.
- **Assertion, not evidence:** green job reports with no restore test, or “our provider handles it” with nothing from the provider.

WHERE IT USUALLY FALLS SHORT

Backups reachable with the administrator credentials an attacker would steal. A single-file restore long ago, never recorded. Cloud data assumed to be backed up by the platform provider.

WHAT YOU CAN SUPPORT TODAY

Describe the design as it is, and give the date and real scope of the last restore you can evidence. If none has been tested, do not imply otherwise; book one before submission if you can.

WHAT TO AIM FOR AT RENEWAL

An immutable or offline copy with separate credentials, a recorded restore test of a critical system on a planned cycle, and a written view of recovery time.

04

Is endpoint detection and response deployed on all devices and servers, and who acts on its alerts?

WHY IT MATTERS

Two tests in one: coverage and attention. A tool on most devices with nobody reading its alerts at night does far less than the answer implies.

EVIDENCE THAT HOLDS UP

- A coverage report from the endpoint console compared with the asset inventory, with any difference explained.
- The monitoring arrangement in writing: an internal rota, or a provider contract stating the hours covered and the actions they can take.
- A recent alert that was investigated and closed, with dates.
- **Assertion, not evidence:** the product name, or “all devices have antivirus”.

WHERE IT USUALLY FALLS SHORT

Console and inventory counts disagree. Servers or cloud workloads are left out. Alerts land in a mailbox nobody watches out of hours.

WHAT YOU CAN SUPPORT TODAY

State the coverage you can show and the monitoring hours as they really are. “Business hours, with alerts emailed overnight” is an answer, and better given than discovered.

WHAT TO AIM FOR AT RENEWAL

Coverage reconciled against the inventory with named exceptions, and alert response arranged in writing for the hours the business actually operates.

05

What protects email from phishing, malicious attachments and spoofing?

WHY IT MATTERS

Email remains a common way in. The question tests the layers between a malicious message and a member of staff, and whether your domain is protected against email that pretends to come from you.

EVIDENCE THAT HOLDS UP

- Filtering or advanced threat protection settings, showing link and attachment protection on all mailboxes.
- Your published SPF, DKIM and DMARC records, and whether the DMARC policy only monitors or actually enforces.
- How staff report a suspicious message, with an example of a report being handled.
- **Assertion, not evidence:** “our email provider includes filtering”.

WHERE IT USUALLY FALLS SHORT

DMARC left in monitoring mode for years. Advanced protection licensed for some mailboxes only, with shared mailboxes left out.

WHAT YOU CAN SUPPORT TODAY

State which protections cover which mailboxes, and your DMARC policy exactly as published. Anyone can look it up, so the answer has to match it.

WHAT TO AIM FOR AT RENEWAL

Protection on every mailbox, DMARC enforcing once legitimate senders are aligned, and a reporting button that staff actually use.

06

How quickly are security patches applied, and do you run any end-of-life systems?

WHY IT MATTERS

This tests whether published weaknesses stay open long enough to be exploited. Underwriters look for a normal cadence, a faster route for critical vulnerabilities on internet-facing systems such as firewalls and VPNs, and an honest account of anything that no longer receives security updates.

EVIDENCE THAT HOLDS UP

- A patching standard with target timeframes by severity.
- Dated patch compliance and vulnerability scan reports covering servers and network devices, with outliers visible.
- A list of end-of-life systems: why they remain, and what isolates them.
- **Assertion, not evidence:** “patches are applied monthly”, with no report showing that they were.

WHERE IT USUALLY FALLS SHORT

Laptops patch automatically while firewalls, servers and network devices wait for someone to remember. An end-of-life server runs software nobody wants to migrate, on the main network.

WHAT YOU CAN SUPPORT TODAY

Give the cadence you can evidence, not the one in the policy. Disclose end-of-life systems with their isolation and a retirement date.

WHAT TO AIM FOR AT RENEWAL

Target timeframes met and shown in dated reports, internet-facing devices included, and end-of-life systems retired or isolated with a dated plan.

07

Do staff complete security awareness training and phishing simulations?

WHY IT MATTERS

This tests whether people know what to do with a suspicious message, refreshed rather than covered once at induction. Completion records matter more than course content, and coverage of executives and finance staff matters because payment fraud targets them.

EVIDENCE THAT HOLDS UP

- Completion records by person and date for the current cycle, reconciled against the HR staff list.
- Phishing simulation dates, scope, and the follow-up given to people who clicked.
- A written call-back procedure for changes to supplier bank details, which is often asked about alongside training.
- **Assertion, not evidence:** “we held a session last year”, with no attendance record.

WHERE IT USUALLY FALLS SHORT

Executives, contractors or recent starters never enrolled. Simulations run once. Payment verification is a habit in finance rather than a written procedure.

WHAT YOU CAN SUPPORT TODAY

Give completion from the record, including who is not covered. If simulations have not been run, do not describe the training as though it included them.

WHAT TO AIM FOR AT RENEWAL

Training tracked by person, simulations on a regular cadence, and a written verification procedure for payment changes.

08

Do you have a documented incident response plan, and has it been tested?

WHY IT MATTERS

This tests whether, on the worst day, people know who decides, who to call and in what order — including the insurer's own incident reporting route. Untested plans fail on basics: out-of-date phone numbers, nobody authorised to take systems offline, a plan stored only on the network that is down.

EVIDENCE THAT HOLDS UP

- The plan, with a version, an approval date and a named owner.
- A contact sheet available offline, including the insurer's reporting route and any response provider the policy names.
- The last exercise record: date, scenario, attendees, findings, and the actions agreed and completed.
- **Assertion, not evidence:** a template that was never adapted, or "our IT provider would handle it".

WHERE IT USUALLY FALLS SHORT

A plan that predates the current IT set-up, has never been exercised, and does not mention the insurer, even though the policy may set conditions on how incidents are reported.

WHAT YOU CAN SUPPORT TODAY

Give the dates the plan was last approved and last exercised. If it has never been tested, a short tabletop exercise before submission is achievable and gives you a real date to report.

WHAT TO AIM FOR AT RENEWAL

A current plan naming the insurer's reporting route, tabletop exercises on a regular cycle with actions tracked to completion, and an offline copy of the contacts.

09

How do you control third parties with access to your systems or data?

WHY IT MATTERS

This tests whether a supplier could become the way in. Managed service providers, vendors with remote support tools and platforms holding sensitive data can all reach you directly if they are compromised. The question is whether you know who has access, how they connect, and whether that access is limited.

EVIDENCE THAT HOLDS UP

- A register of suppliers with system or data access, recording what each can reach and how.
- For critical suppliers, a dated review: questionnaire responses, or an independent assurance report or certificate with its scope checked against the service you use.
- Evidence that supplier access uses MFA, is limited to what is needed, and is removed when an engagement ends.
- **Assertion, not evidence:** “our suppliers are all reputable companies”.

WHERE IT USUALLY FALLS SHORT

A remote support tool installed years ago still gives a vendor standing access. The IT provider holds full administrator rights with no MFA requirement in the contract.

WHAT YOU CAN SUPPORT TODAY

List the suppliers with access and describe the controls on that access as they are. Where reviews are outstanding, say which suppliers come first and by when.

WHAT TO AIM FOR AT RENEWAL

A maintained supplier register, dated reviews of critical suppliers, MFA and least-privilege access on every supplier connection, and access removed when engagements end.

10

Do you collect and review security logs, and how long are they kept?

WHY IT MATTERS

This tests whether an attack in progress could be noticed, and whether anyone could establish afterwards what happened. Retention matters because an investigation that finds the relevant logs already overwritten is slower, more expensive and less certain.

EVIDENCE THAT HOLDS UP

- Which systems send logs to a central place — identity platform, email, firewall, endpoint tool, key servers — and which do not.
- Retention settings shown in configuration.
- Who reviews alerts raised from those logs, and how often, in writing.
- **Assertion, not evidence:** “everything is logged”, with no statement of where logs go or how long they are kept.

WHERE IT USUALLY FALLS SHORT

Logs stay on each system with default retention far shorter than anyone assumed. Audit logging on the email or identity platform was never switched on, or depends on a licence the organisation does not hold.

WHAT YOU CAN SUPPORT TODAY

Describe where logs are collected and the retention actually configured. If there is no central collection or regular review, say so plainly.

WHAT TO AIM FOR AT RENEWAL

Key logs collected centrally, retention chosen deliberately rather than inherited, and alerts reviewed on a defined schedule by a named person or provider.

11

Is your network segmented so that a compromise cannot spread freely?

WHY IT MATTERS

This tests how far an attacker can move once inside. On a flat network, one compromised laptop can reach every server, the backups and any operational equipment.

EVIDENCE THAT HOLDS UP

- A dated network diagram, checked against what is actually deployed, showing the main segments and how traffic between them is controlled.
- Firewall rules separating backups, servers and any production equipment from user devices.
- **Assertion, not evidence:** the diagram from the original installation, which no longer matches the network.

WHERE IT USUALLY FALLS SHORT

Segments were designed, then years of exceptions let most of them reach each other. Factory or building systems share a network with office machines.

WHAT YOU CAN SUPPORT TODAY

Describe the network as it is today. If it is largely flat, say so, and state what restricts access to backups and critical systems.

WHAT TO AIM FOR AT RENEWAL

Backups and critical systems separated from user devices by rules that are reviewed, operational equipment isolated, and a diagram kept current.

PART 3 OF 5

Questions that stall because nobody owns the answer

Most delays are not technical: the answer sits between two teams, or with a provider, and each assumes the other has it. Assign these early.

QUESTIONS THAT COMMONLY STALL A SUBMISSION, AND WHO USUALLY ENDS UP ANSWERING THEM

QUESTION	WHY IT STALLS	WHO USUALLY ENDS UP ANSWERING
When was a restore last tested?	IT assumes the backup provider tests restores; the provider waits to be asked.	Whoever manages the backup contract, with written confirmation from the provider.
Which accounts are excluded from MFA?	Exclusions were made by different people on different systems, and nobody holds one list.	The identity platform administrator, with each system owner confirming their exceptions.
Which suppliers have remote access?	Procurement holds the contracts and IT holds the access; neither holds both.	IT, working from the finance team's list of active suppliers.
When was the incident response plan last exercised?	The plan was written as a project and never given an operational owner.	An executive sponsor, with IT running the exercise.
Are any systems end-of-life?	The systems often belong to production, a laboratory or finance, not to IT.	The department that depends on the system, with IT describing how it is isolated.
Has everyone completed security training?	HR owns the staff list, IT owns the training platform, and the two lists disagree.	HR, reconciling against the training platform's export.
Any incidents, claims or notifications since the last application?	Nobody is sure what counts, and whoever handled an event may have left.	Finance or legal, checking incident records and insurer correspondence, with legal counsel where unclear.

PART 4 OF 5

Disclosing a gap with a remediation date

Some answers will be no or partial. Softening them usually backfires: an inaccurate answer can cause serious problems later, including when a claim is made. How disclosure duties apply to you depends on your policy wording, your application and the governing law, so take your broker's advice, and legal advice where it matters.

A useful disclosure says what is true today, what limits the risk meanwhile, what will close the gap, and who owns that by when. Only give dates you

expect to meet. The systems and dates below are invented.

EXAMPLE WORDING: OBSCURING A GAP, AND DISCLOSING IT

SITUATION	WORDING THAT OBSCURES	WORDING THAT DISCLOSES
Some service accounts are excluded from MFA	"MFA is enforced across the organisation."	"MFA is enforced for all staff on email, remote access and administration. Three finance system service accounts are excluded; they cannot sign in interactively and are restricted to the finance server. They move to a supported method by 31 March, owned by the IT manager."
A full restore has never been tested	"Backups are tested regularly."	"Backups run nightly, with an immutable copy held by our provider. A full restore of a critical system has not yet been tested; a finance system restore test is booked for 15 November."
An end-of-life server remains in use	Answering no to the end-of-life question, or leaving it blank.	"One server on an unsupported operating system runs production scheduling. It sits on a separate segment with no internet access, reachable only by two named administrators. Its replacement is funded for the second quarter."

PART 5 OF 5

Week by week, from eight weeks out

Starting later? Keep the order and compress the middle.

01

Eight weeks out — confirm the date, the form and the owner

Confirm the submission date with your broker; it usually falls before the renewal date. Get this year's form and last year's answers, and name one owner for the whole renewal.

02

Seven weeks out — mark what you cannot evidence

Mark every answer you cannot support with a dated document. Do not fix anything yet: that list, not the whole form, is the project.

03

Six weeks out — give the unowned questions an owner

Assign each unsupported answer to a named person. Put requests to providers in writing now; their response time is outside your control.

04

Five weeks out — collect what already exists

Gather the exports, reports and records that exist but were never collected. Date each one and note which question it supports.

05

Four weeks out — decide what can be fixed in time

Split the remaining gaps into what can be true before submission — removing stale administrator accounts, a restore test, a tabletop exercise — and what cannot. Start the first group; give the second an owner, a realistic date and disclosure wording.

06

Three weeks out — draft the answers from the evidence

Write each answer from the evidence, not from memory or last year's form, and check that publicly visible settings such as email authentication records match.

07

Two weeks out — review and sign off

Have the owners of the evidence confirm the answers that rely on their work, and have someone authorised to make representations for the organisation review the whole application.

08

One week out — submit one clean package

Send the application with an index of supporting evidence and a short summary of remediation under way. Keep an exact copy of what was sent, and when.

09

After renewal — turn the second column into the year's plan

Check the terms offered for new conditions, move every "next renewal" target into a plan with owners and dates, and refresh evidence as it ages.

CYBERWAVE SENTINEL

Where Sentinel fits

Sentinel's cyber insurance readiness workspace, included from the Essentials plan, holds the controls underwriters commonly ask about — MFA, endpoint detection, backups and restore testing, email security, patching, incident response, awareness training, vendor risk and encryption — each answered Yes, Partial or No, with its evidence attached. Every evidence item carries an owner, a status and an expiry date, so a lapsed restore test shows as expired in the library rather than surfacing in the week the form is due.

Evidence is attached by the people who own each control. Sentinel does not connect to your systems, collect evidence for you or submit anything to a broker or insurer; the representations in your application remain yours.

See cyber insurance readiness in Sentinel →

Limitations

WHAT THIS CHECKLIST IS NOT

This checklist is general guidance to help you prepare for underwriting questions. It is not legal advice, insurance advice or an interpretation of any policy wording. Applications vary between insurers, products and years, and your broker's current application governs what you are asked. Evidence examples are illustrative, and the systems and dates in the disclosure examples are invented.

CyberWave is not an insurer or an insurance broker, does not bind coverage, and does not guarantee coverage, premium, claim payment or insurer acceptance. Working through this checklist does not mean a submission will be accepted, or accepted on any particular terms. You remain responsible for complete and truthful representations to your insurer or broker.

Related

Cyber insurance readiness →

How the evidence library works →

Risk management and action tracking →

Plans and pricing →

All checklists and templates →