Your First Renewal Moves

Cyber Insurance Readiness Assessment

Sylvan Assurance, LLC

Version 1.0 · Updated 2026-10-05

Contents

The ninety days before your cyber insurance renewal, in plain English 1
The shape of the ninety days 1
What the form will ask 2
The big four, in the order to take them 2
File the proof as you go 3

About This Guide **4**

The ninety days before your cyber insurance renewal, in plain English

Who this is for: the owner or manager who has a cyber insurance renewal coming and wants to walk into it prepared rather than surprised. This is not the whole discipline. It is the short version: what the form will ask, the order to take the big four controls in, and the proof worth filing as you go.

One rule before anything else. The renewal form is a list of yes/no questions about your security controls, and one tie-breaker settles every argument before it starts: *if you cannot say where the proof would come from, it is not a yes.* An honest no with a dated plan behaves better, at renewal and at claim time, than a hopeful yes the file cannot back.

The shape of the ninety days

Behind the renewal date on your policy sits the underwriter's real deadline, often weeks earlier. Your broker knows it, so the countdown starts with a phone call, and every later mark counts back from that real deadline, not from the date on the policy's face.

90 days out. Call the broker. Ask three things: when the underwriter actually needs the completed application; what proof the carrier expects alongside the attestation this year; and how an honest no with a dated remediation plan is treated. Put the remaining marks on the calendar with real dates while you are still on the call.

60 days out. Sit with the form. Ninety minutes, the application, three highlighters: green for a confident yes, amber for probably-but-no-proof, red for no (or for any ques-

tion you cannot parse). Apply the tie-breaker honestly: nobody signs the highlighters, so this is the cheap place to be wrong. Copy the ambers and reds onto one page. That page is your work plan for the next month.

30 days out. Refresh the proof. Fresh, dated exports for the big four (the next section says exactly which), plus the second-ring records. File them where you can find them on a bad day.

14 days out. Read it aloud. Every answer, against its artefact: for each yes, name the dated proof behind it and where it is filed. Any yes that is still a hope becomes an honest no with a remediation date.

Day 0. Sign, file a copy, deliver it to the broker. Early files get shopped around for better terms; late files just get placed.

Starting inside ninety days? Make the broker call this week and keep the remaining marks in order on your own clock. A mark you reach late, in order, still works; a mark you skip does not.

What the form will ask

Carriers write their own forms, but the forms rhyme. Nearly all of them ask about nine controls:

The big four. On effectively every application: multi-factor authentication (MFA), endpoint detection and response (EDR), tested backups, and a written incident response plan.

The second ring: patching, security-awareness training, offboarding (removing access when people leave), and email authentication.

The payment rule: a call-back verification step before any change to payment details or any large transfer, the control that guards how money moves.

Each question is really asking one thing underneath its wording: *would this control actually hold, and could you prove it?*

The big four, in the order to take them

The order below is about calendar time, not importance. Start the slow ones early and bank the fast win first.

1. MFA. Close it this week. MFA asks for a second proof of identity beyond the password, and the form's version of the question is strict: enforced as a platform rule for *every* account, every person, the shared mailboxes, and above all the administrator account your Information Technology (IT) provider uses. For most firms on Microsoft 365 or Google Workspace, enforcement is a weekend's work. *Proof to file:* the dated enforcement-policy export and the user-coverage list with the count visible.

2. EDR. Open the conversation the same week. EDR is software on every workstation and server that notices break-in behaviour and lets someone act on it. It has the longest lead time of the four: choosing a product or asking your managed service provider (MSP, the outside company that runs your computers) to deploy theirs, then rolling it out, so the conversation starts now even though it finishes last. *Proof to file:*

the coverage export, reconciled against your device list, and the written answer on who monitors it.

3. Tested backups. Schedule the restore test. The form does not ask whether you take backups; it asks whether you have *restored* from them. A restore test needs a quiet afternoon and a calendar entry, which is why it slips. Put a date on it at the 60-day mark and write one page about what you restored, when, and how long it took. *Proof to file:* that dated restore-test note.

4. The written incident response plan. One page, written last. Who declares an incident, who calls the insurer's hotline, who talks to customers, and where the contact numbers live. It is the shortest artefact of the four and it is written last on purpose: it references the other three. Review it once a year and date the review. *Proof to file:* the plan page with its current review date visible.

File the proof as you go

Every move above ends the same way: a dated artefact goes into a folder. That is deliberate. The evidence pack is the renewal's real output: a place where the MFA export, the EDR coverage list, the restore-test note, and the plan page sit together, dated, so that renewal morning is retrieval rather than archaeology, and so a claim, if one ever comes, starts from your records rather than your recollections. One folder, six months from now, will repay this ninety days many times over.

Where to go from here. The free Cyber Insurance Readiness Assessment at sylvanassurance.com walks the same nine controls in about five minutes and reads each one green, amber, or red the way the form will. The companion book, *Cyber Insurance in Plain English*, carries the full version of everything here: the form decoder, the evidence-pack checklist, and the countdown as a dated wall page.

About This Guide

This guide is produced by **Sylvan Assurance, LLC** and reflects professional experience translated into plain-language guidance for small business owners.

It provides **general guidance and recommended practices**. It is **not** insurance, legal, or brokerage advice, and Sylvan Assurance is not an insurance carrier, broker, or law firm. Every recommendation is **optional** - a widely accepted way to reduce a common risk. **Your policy wording controls - confirm specifics with your broker or carrier.** Responsibility for your business remains with you.

For full terms, see the Terms of Use provided with the Cyber Insurance Readiness Assessment.

Copyright 2026 Sylvan Assurance, LLC. Not for resale.

Free to share unchanged with credit. Terms: sylvanassurance.com/licence/free/

Where to go from here

Scan for the full toolkit that builds on this guide.
sylvanassurance.com/go/toolkit-cyber-insurance-readiness

Scan for the companion book - the full story, in plain English.
sylvanassurance.com/go/cyber-insurance-plain-english