Cyber Insurance in Plain English

A Small-Business Field Guide to Getting Covered, Staying Covered, and Being Ready When You Claim

Sylvan Press

Sylvan Press

Field-tested, plain-English references for the people who do the work and stand behind their call.

Cyber Insurance in Plain English

A Small-Business Field Guide to Getting Covered, Staying Covered, and Being Ready When You Claim

Published by Sylvan Press, the security imprint of Sylvan Assurance, LLC, Vermont, USA.

ISBN (paperback): 9798951893697
ISBN (hardcover): 9798951893703
ISBN (ebook): 9798951893710

First edition, 2026.

Disclaimer. This book provides general guidance and recommended practices, not legal, financial, insurance, brokerage, or other professional advice, and it does not create any advisory, brokerage, or consulting relationship between the author, the publisher, and the reader. Every recommendation is optional (a widely accepted way to reduce a common risk), and the reader decides which to adopt, adapt, or decline. Following this guidance does not guarantee any particular outcome, coverage decision, or premium, and does not prevent any particular breach, incident, or loss. Insurance policies differ by carrier, state, year, and endorsement: **your policy wording controls**, and questions about your specific coverage belong with your broker, your carrier, or your attorney. Where this book refers to laws, standards, or commercial products, it does so for general awareness only; product references are illustrative examples, not endorsements, and the carriers, brokers, firms, and claim accounts in these pages are fictional or composite. Cost figures are typical ranges as of mid-2026; confirm current quotes before purchasing.

Sylvan Press, sylvanassurance.com

Contents

Cyber Insurance in Plain English

A Small-Business Field Guide to Getting Covered, Staying Covered, and Being Ready When You Claim

The promise

This year's renewal asked for proof. Multi-factor authentication on every account. Detection software on every computer, monitored. Backups you have actually restored from. An incident plan with names on it. Certified, in writing, by an officer of the company, which is to say, by you.

This book walks the form with you. What each question means in plain English. What "counts" for each control, and what it should cost. How to answer honestly without hurting yourself. What the policy's own fine print asks of you in return. And, the part the worst week of some future year will thank you for, what evidence to keep, dated and filed, so that what you certified stays provable long after the screenshots would otherwise be gone.

You will not need to become technical. Every term in this book is explained in words that mean something, at the moment you need it, and

again in the glossary at the back. Three small firms walk every page with you (a twelve-person accounting group, a solo bookkeeper, and a forty-one-person title agency) so that you see every control worked through at three sizes before you fill in your own.

Who this book is for

The owner who is also the insurance contact. The office manager the supplemental was forwarded to. The person at a small firm who pays an IT company's invoice without a reliable way to judge the work, and who has just discovered that the cyber policy now comes with homework attached. If your company has somewhere between one and fifty people and nobody whose job title contains the word "security," this book was written at your desk.

If your renewal is soon

Renewals do not wait for page order. If your supplemental is due inside ninety days, Chapter 1 closes with the sprint router, the reading path that matches your clock: triage the form this week with Chapter 3, make the broker and IT calls with Chapter 13's scripts, close the big four controls with Chapters 4 through 7, read Chapters 10 and 11 before you sign anything, and lock in the proof with Chapter 12 while the screenshots are one click away. Appendix D's renewal countdown keeps the whole sequence on one page.

A note on what this book is not

It is not legal, insurance, or brokerage advice, and it does not replace reading your own policy: **your policy wording controls**, and questions about your specific coverage belong with your broker, your carrier, or your attorney. Product names appear only as examples, never as recommendations; the carriers, brokers, and firms in these pages are fictional, and the claim stories are composites. Cost figures are typical ranges as of mid-2026: confirm current quotes when you buy.

Purchase of this book includes free updates while it remains in our catalog.

Sylvan Press: plain-language security and compliance for the people who do the work and stand behind their call.

1 The Renewal That Asked for Proof

The email from the broker arrived on a Tuesday, between a payroll question and a client reschedule. Corinne Fairweather almost filed it for the weekend. The subject line was the same as every year, *Fairweather Accounting Group: cyber policy renewal*, and for six years, the renewal had been a formality. Sign where the tabs said sign. Pay the premium. Forget about it until next June.

Then she opened the attachment.

The renewal packet had grown. Behind the usual declarations page sat a document she had not seen before: a *supplemental application*, four pages of questions about the firm's computers. Not friendly questions. Specific ones. Was multi-factor authentication enforced for all users on email, remote access, and administrative accounts? Did every workstation and server run endpoint detection and response software, and was it monitored? When had the firm last performed a verified restore from backup; and was a copy kept offline? Did a written incident response plan exist, and when was it last reviewed?

Then the sentence that moved the email out of the weekend pile: *Responses must be certified by an officer of the company. Coverage terms for the upcoming period will be based on the controls attested below.*

Corinne read the four pages twice. She is the owner of a twelve-

person accounting group in Ohio. She is also, in the way of twelve-person firms, its human resources department, its facilities manager, and, she was discovering, its insurance contact. She could answer perhaps a third of the questions from memory. Multi-factor authentication: probably, on some things? The firm used Microsoft 365, and she remembered approving something about phone codes two years ago. Endpoint detection and response: she did not know what that was. The words did not attach to anything. Backups: the firm paid Cobalt IT, its outside computer support company, a monthly fee that included the word "backup" on the invoice. Whether anyone had ever *restored* from one: no idea. A written incident response plan: no.

She did what most owners do: forwarded the supplemental to Danny Reyes, her account manager at Cobalt IT, with a one-line message. *Can you handle this?*

Danny called back the next morning and said three things. First, some of it, yes, Cobalt could pull backup reports and could have multi-factor authentication fully enforced within weeks. Second, endpoint detection meant new software on every computer, not in the current contract; he would quote it. Third, and he said this carefully, the certification itself was not something Cobalt could do. The form asked an officer of the company to attest. That was Corinne. Whatever went on those four pages, she would be the one signing it.

Corinne is not a technologist, but she has signed enough documents to respect the word *certify*. She had certified payrolls, tax filings, engagement letters: statements she could stand behind because she knew them to be true. What unsettled her about this form was not the technology. It was being asked to attest to a state of things she could not currently see. She could not, that Tuesday, have told you whether the firm's backups had ever been restored, or what was watching the office computers, or who Dee, her office manager, would call first if the worst happened on a Friday afternoon. The form wanted her signature on facts she did not yet possess. That gap, between the signature required and the knowledge to back it, is the exact distance this book is written to close.

That is the moment this book is written for. Not the breach. Not the ransom note. The Tuesday when the renewal arrives asking for proof,

and the owner discovers that the policy she has been quietly paying for now comes with homework; and that the homework has her name on it.

What changed

For a long time, cyber insurance worked like this: the application asked broad questions, the answers were taken more or less on faith, the premium was modest, and the policy sat in a drawer. Carriers were competing for market share in a new line of business, and underwriting was light.

Then the losses arrived. Ransomware turned from a nuisance into an industry. Business email compromise, the quiet fraud where an attacker talks a bookkeeper into wiring money to the wrong account, became one of the most expensive crimes in America by dollar volume, according to the FBI's annual Internet Crime Report. Carriers paid out, repriced, and paid out again. And somewhere in that cycle, the industry reached a conclusion it has not walked back: the difference between a small claim and a catastrophic one usually came down to a handful of basic controls on the customer's side. Whether stolen passwords worked without a second step. Whether anything was watching the computers. Whether the backups survived and had ever been tested. Whether anyone knew who to call in the first hour.

So the questions got specific, and the answers grew consequences. Premiums now move based on what you attest. Some controls have become effectively mandatory, not because a law says so, but because the market does: without them, carriers decline the risk, or attach exclusions, or price the policy like the gamble it is. And the attestation itself has teeth. The answers you certify become part of the insurance contract. If a claim arrives and the investigation finds that a control you certified was not actually in place, you have handed the carrier a reason to fight.

To see why the industry moved, picture the kind of week it learned to price. A bookkeeper at a firm the size of Fairweather opens what looks like a routine supplier message; a fake login page quietly captures her password; for six unremarkable weeks a stranger reads the firm's mail and learns exactly how it pays people. Then, at month-end,

a real supplier's banking details arrive changed, in an email convincing enough that no one questions it, and a legitimate-looking payment lands in a criminal's account. No alarm sounds, because nothing was "hacked" in the movie sense: someone signed in as an employee and waited. What follows is lawyers, forensics, notifications, and a hole in the operating account. Multiply that quiet week by a few thousand firms a year and you have the losses that rewrote the application. Every question on Corinne's supplemental is the industry pointing at one moment in that story and asking: at your firm, could this have been stopped, or at least seen, before month-end?

None of this is a scandal. It is insurance doing what insurance does with every risk it learns to measure: the same road fire coverage travelled when inspectors started asking about sprinklers. But it does mean the renewal is no longer a formality, and the person it lands on, you, needs to understand what the form is actually asking.

Here is the reframe this book is built on, and it is genuinely good news: *everything the carrier is asking for is something you would want anyway.* The form is not an obstacle between you and coverage. It is a checklist of the things that make the bad Tuesday survivable: written by an industry that pays for bad Tuesdays professionally and has strong opinions about what makes them cheaper. You are not doing homework for the insurance company. You are doing it for the version of you that may someday have a very bad week, with the insurance company footing part of the bill for the supervision.

Whose book this is

This book is written for the owner who is also the insurance contact. The person the supplemental lands on. You might run an accounting group, a dental practice, a design studio, a title agency, a nonprofit, a machine shop. You have somewhere between one and fifty people, no security team, probably no full-time IT person, and possibly an outside computer support company (a *managed service provider*, or MSP, in the industry's language) whose invoice you pay and whose work you have limited ability to judge.

You do not need to become technical to use this book. That is a promise, and it comes with a discipline this book holds throughout:

every technical term gets explained in words that mean something, at the moment you need it, and again in the glossary at the back. Not expanded: *explained*. Knowing that EDR stands for "endpoint detection and response" tells you nothing. Knowing that it means *software that watches each computer for break-in behaviour and can cut a compromised machine off from the network* (*a step beyond antivirus, which matches known bad files*) that tells you what you are buying, why the carrier cares, and what to ask your IT provider. That is the standard every explanation in this book is held to.

Three organisations walk through every chapter with you, so that nothing stays theoretical:

Fairweather Accounting Group: Corinne's firm. Twelve people, client financial data, Microsoft 365, an MSP contract with Cobalt IT whose account manager, Danny Reyes, answers the phone. Inside the office, Dee runs the front desk and the filing, and, as it turns out, will end up the quiet keeper of the evidence pack in Chapter 12. Fairweather is the book's home base, because a firm of that shape is who the renewal squeeze lands on hardest: big enough that carriers expect real controls, small enough that nobody owns them. Every worked example in this book shows Fairweather's version first.

Vega Bookkeeping: Marisol Vega, working solo with one part-timer. Marisol's examples show the smallest version of each control that is still real, for readers whose entire company fits in one room. If that is you, look for Marisol's variant after each Fairweather example, it is usually shorter, cheaper, and faster to put in place.

Dunmore Title & Escrow: forty-one people, an in-house IT manager named Theo Brandt, and wire-transfer exposure that makes its carrier ask harder questions. Dunmore shows what the same controls look like with a real IT person in the building, useful for reading what your MSP *should* be doing, and for readers whose firms are on the larger end of small.

Two more members of the cast deserve an introduction. **Sam Herrera**, of Herrera & Park Insurance, is the independent broker who handles Fairweather's policy, placed with its carrier, **Ledgestone Mutual**. A broker sells you the policy and, in the good cases, advocates for you with the carrier; a carrier is the company whose money actually

pays a claim. Neither is a security advisor, and neither fills out your supplemental, that officer's signature is yours. Understanding whose side each player is on (carrier, broker, MSP) is Chapter 2's job, and it is shorter than you fear. (Ledgestone Mutual, Herrera & Park, and Cobalt IT are inventions, as is every carrier, broker, and IT firm in this book. The names are fictional; the patterns they show are drawn from the real ones.)

What this book will do

By the last page, you will be able to do five things you may not be able to do today.

Read the form. The supplemental application stops being four pages of intimidation and becomes a map. Chapter 3 walks the common core (the questions that appear, in some wording, on nearly every carrier's application) and explains what each is actually asking and what a defensible yes looks like.

Close the gaps that matter. Chapters 4 through 8 take the controls one at a time: multi-factor authentication, endpoint detection and response, backups, the incident plan, and the second ring of patching, training, offboarding, and email settings. Each chapter answers the same four questions in the same order: what is this, what counts as having it, what should it cost, and what evidence proves it. Much of it is cheaper than you expect. Some of it you already own and merely need to switch on.

Answer honestly without hurting yourself. Chapter 9 is about the form itself: why the inflated yes is the most expensive word in this book, how to give an honest no with a remediation date attached, and how to handle the question you genuinely cannot answer yet.

Understand what you are buying. Chapters 10 and 11 cover the policy side: what moves the premium, what the deductible and sublimits actually mean for a firm your size, and where the fine print narrows coverage. Read those two before you sign anything.

Keep the proof. Chapter 12 is the heart of the book: the evidence pack. A thin, boring, dated file of screenshots and logs (assembled in about an evening, maintained in about an hour a quarter) that answers the question every claim eventually asks: *can you show that the controls you*

certified were real, and running, at the time it mattered? When something does go wrong, Chapters 14 and 15 walk the first calls and the claim itself, and the evidence pack is where that work either gets easy or gets hard.

The remaining chapters round out the system: Chapter 13 gives you the scripts for managing the people you pay, what to ask your MSP, how to judge the quote, and what to ask your broker, including the questions Corinne wished she had asked on that first Tuesday. Chapter 16 turns the whole thing into an annual rhythm, so next year's renewal can be an afternoon instead of a season.

What this book will not do

It will not make you a security professional, and it will not try. The controls in this book are the insurance core: the short list carriers have converged on because it moves losses. A broader security program for a small business is a bigger subject, and it has its own book in this series, *The Small Business Security Playbook*. The two overlap the way a driving test overlaps with being a good driver.

It will not sell you anything. This book names product categories, not products. Where a category is easier to grasp with examples, you will see names, "such as Microsoft Defender for Business or CrowdStrike", and every such mention means *example*, never *recommendation*. The same neutrality applies to carriers and brokers: the ones in this book are fictional, the claim stories are composites drawn from public patterns, and nothing here endorses anyone. You will also see cost figures, "EDR typically runs five to ten dollars per computer per month", which are honest mid-2026 ranges meant to protect you from wild quotes, not prices anyone owes you. Confirm current numbers when you buy.

And it will not tell you what your policy covers. That sounds strange in a book about insurance, so here is the plain version, which this book will repeat at every point where it matters: *your policy wording controls.* Policies differ by carrier, by state, by year, and by endorsement. This book teaches you what the questions mean, what the standard machinery looks like, and what to ask; it does not replace reading your own policy, and it does not replace your broker, your attorney, or your car-

rier on questions about your specific coverage. Where this book says "typically" or "most policies," it means exactly that, and the exceptions are why the professionals exist.

If your renewal is soon: the sprint router

Books are written in a sensible order. Renewals do not arrive in one. If your supplemental is due in sixty or ninety days, here is the path through this book that matches your clock. (If you have the luxury of time, ignore this and read straight through: the chapters build.) The printable version of this schedule (a renewal countdown you can pin to the wall, with the milestones below dated against your actual deadline) is Appendix D, next to the first-calls page. Tear it out now, and the rest of this section becomes a plan you are working rather than a passage you are reading.

This week: know what you are looking at. Read the rest of this chapter, then Chapter 3, with your own supplemental open beside it. Mark each question green (confident yes), amber (probably, but no proof), or red (no, or no idea). When Corinne did this at her kitchen table on the Thursday, the four intimidating pages resolved into three short lists: a handful of greens she could actually defend, a cluster of ambers that all meant the same thing (*we probably do this, but I could not prove it today*) and four honest reds. The firm's whole cyber posture, which had felt like an undifferentiated fog, turned out to be about a dozen real questions with knowable answers. That is what the sitting does: it converts dread into a list, and a list is a thing you can finish. If you want the same triage interactively, the free Renewal Readiness Check at this book's companion site walks the identical questions, on your screen, nothing uploaded, nothing tracked.

Weeks one and two: the calls. Read Chapter 13 *before* you talk to anyone, then make two calls with its scripts in hand. Your broker: confirm the actual deadline, ask what form of proof the carrier expects with the attestation, and ask how an honest no with a dated remediation plan is treated; the answer will lower your blood pressure. Your MSP or IT person: hand over the amber-and-red list and ask the three questions from Chapter 5's pattern: what do we have today, what would closing this cost, and what will you give me as evidence.

Weeks two through six: close the big four. Chapters 4 through 7, in that order: multi-factor authentication (often a weekend, often free), endpoint detection and response (a quote and a rollout), backups with a verified restore (one honest test), and the one-page incident plan (an evening, and Appendix D gives you the skeleton). Chapter 8's second ring follows as time allows, much of it is settings, not spending.

Before you sign: the policy side. Chapter 9 for the form itself, then Chapters 10 and 11 so you know what the premium is buying and where the coverage narrows. If you read nothing else twice, read the "failure to maintain" passage in Chapter 11, it is the clause the evidence pack exists to answer.

The week it is all done: lock in the proof. Chapter 12. Build the evidence pack while the screenshots are one click away. An evening now; an argument you never have to have, later.

Chapters 14 and 15, the incident and the claim, are not sprint reading. Skim them once so you know what is there, note where Appendix D's first-calls page goes (near the phone, genuinely), and come back when the renewal is signed.

The premise, stated plainly

Corinne's story ends well, and not because anything dramatic happened. It ends well because the supplemental turned out to be finite. Four pages. Perhaps a dozen real questions. Behind them, five controls and a filing habit: most of them cheaper than the premium increase she was bracing for, one of them free, all of them things a twelve-person firm could stand up in a season without anyone becoming a technologist.

That is the premise of this book: the form is finite, the controls are learnable, the evidence is boring, and the owner who understands all three walks into renewal (and, if it ever comes to it, into a claim) from strength. Insurance is the one corner of security where someone else has already decided exactly what "good enough" means and written it down. This book is the translation.

Turn the page, and we will start with the thing you are actually buying.

Recap: The cyber-insurance renewal has changed: carriers now ask for specific controls, attach premiums to the answers, and require an officer's certification, which makes the owner the accountable party. Everything the form asks for is protective for the business itself, not paperwork for its own sake. This book walks the form in plain English: the common core of controls (Chapters 3–8), answering honestly (Chapter 9), the policy side to read before signing (Chapters 10–11), the evidence pack that makes attestations provable (Chapter 12), the vendor and broker scripts (Chapter 13), and the incident, claim, and renewal system (Chapters 14–16). Three organisations, Fairweather (12 staff), Vega (solo), and Dunmore (41 staff), carry every worked example. If your renewal is inside ninety days, the sprint router in this chapter maps your path.

Next: Chapter 2, What Cyber Insurance Actually Covers (And What It Never Did). The policy in plain English: first-party and third-party coverage, what a policy is and is not, and the players, carrier, broker, MSP; and whose side each one is on.

You've just read Chapter 1 of

Cyber Insurance in Plain English

The full book runs 336 pages across 16 chapters,
with a complete back-of-book index.

Published by Sylvan Press, the book imprint of Sylvan Assurance:
field-tested, plain-English references for the people who do the work.

Scan to see the full book - and where to buy it.
sylvanassurance.com/go/cyber-insurance-plain-english

Not ready for the full book? See where you stand first - free, a few minutes:

sylvanassurance.com/go/free-cyber-insurance-readiness