



Insurable, Not Just Insured

What Your Security Setup Has to Do With Your Coverage

Why this conversation matters right now

Cybersecurity has moved from a background concern to one of the top priorities for small and midsize businesses. Independent research from Vanson Bourne found that 57% of businesses now rank it among their top three concerns over the next two years, up from 43% just a year earlier. Attacks are faster and harder to detect and stop, and some business owners are now realizing this.

Six in ten business owners worry that a serious attack could shut their business down entirely, and that number climbs to nearly three in four among businesses without cyber insurance. Cybersecurity coverage clearly makes people feel safer. Whether it actually delivers when something happens is a different question, and is the reason for this guide.

When you think about Cyber insurance, think of it as the umbrella you buy long before the storm ever shows up. The whole point is that it's there and ready for that one time you actually need it, covering your business financially if a cyber incident hits you unexpectedly.

“An umbrella that doesn't open in the rain isn't protecting anyone, and a cyber insurance policy works in a very similar way. “

Here's the part most business owners aren't aware of. An umbrella that doesn't open in the rain isn't protecting anyone, and a cyber insurance policy works in a very similar way. Having one doesn't automatically mean it opens when the storm actually hits. Whether it does depends on details that a lot of businesses never look into closely until they need to.

A cyber incident without the coverage you thought you had can mean real financial loss, real downtime, and weeks or months of disruption while the business works to recover, on top of what the incident itself costs. Even when a claim gets approved, the payout doesn't always reflect the true cost of getting back to normal. That's exactly why it's worth making sure the coverage you have is coverage you can actually count on.

The two common places to start

Most conversations about cyber insurance start in one of two places.

Shopping for coverage

You're getting a policy for the first time, or coming up on a renewal, and you're not entirely sure whether your business would actually qualify. Insurers have gotten more specific and strict about what they expect to see before they'll issue or renew coverage.

Already have a policy

You already have coverage and feel protected, without realizing there's fine print sitting within the policy. Requirements around security controls, documentation, and the speed at which you report an incident can all affect whether a claim is actually paid.

The thing to keep in mind is that insurance applications are written by underwriters, for underwriters. They were never written to be understood by the business leaders filling them out.

Some common assumptions worth understanding

Assumption #1

"We have multi-factor authentication (MFA), so we're good."

Insurers usually mean MFA is enforced on every account that touches your systems. A business might have MFA fully set up for staff inboxes and still leave it turned off on a VPN connection or an admin account, simply because that part of the rollout never got finished or was forgotten. A small item like this is often enough on its own to have a claim possibly reduced or denied, even if everything else about the response was handled well.



Assumption #2

“Ransomware is always covered.”

Plenty of policies cap how much they'll pay toward a cyber incident, and separate that cap entirely from the cost of everything else that follows, like rebuilding systems, notifying customers, legal fees, and lost revenue while the business is offline. Policies may include something that can exclude the claim outright if the attack exploited a vulnerability the business already knew about but hadn't addressed. Something worth mentioning is that these fine details are most likely in the policy; it's that most people skim past them without realizing what they mean.

Assumption #3

“Our business insurance covers this.”

Standard business insurance was built for things like property damage, liability, and physical theft, not data breaches. Most general policies exclude cyber incidents outright, which means a business can carry solid coverage for years and still have zero protection the day a cyberattack occurs. Cyber coverage is its own separate policy, with its own separate application, list of requirements, and its own renewal to keep up with.

Assumption #4

“We answered honestly, so we're fine.”

A quick 'yes, we have backups' doesn't cut it anymore. Most insurers now want specifics, such as how often backups are tested and where the data actually lives. Answer vaguely, and it'll be treated the same as an incomplete answer. Most of the time, individuals answered based on what they assumed was true rather than what they could actually confirm. That mismatch between assumptions and documentation can be one reason claims are denied or reduced.

**Cyber insurance is worth having, but it
was never meant to carry your
business on its own.**

It works best as one piece of a broader risk management strategy. The requirements insurers want to see are largely the same as those that make an incident less likely in the first place. Enforced access controls. Real-time monitoring. Tested backups. Strengthening your security and strengthening your case for coverage turn out to be the same project. So what are insurers actually asking about?



What most cyber insurers are actually looking for

Throughout various industries, most applications and renewals touch on the same core areas:

- Multi-factor authentication is enforced across every account that can reach your systems.
- Endpoint protection that can detect and respond to a threat in real-time. Having just an antivirus isn't enough.
- Backups are tested on a real schedule, and a set of those backups is stored offline.
- A documented process for patching software before a known vulnerability gets used against you.
- Ongoing security awareness training for your staff, since most breaches start by going after people.
- Email filtering that catches phishing attempts before they reach inboxes.
- Some form of active monitoring so unusual activity gets caught as soon as it is noticed.

Your list will look a little different though

That's the common ground. Your actual questionnaire will ask about it in its own terms, adapted to your specific industry, team size, and the kind of data you handle. For example, a healthcare practice gets asked about patient record access in ways a law firm or a manufacturer never will, even though the underlying concerns (who can get to sensitive data, and how fast you'd notice if something went wrong) are the same.

That's usually where things can get confusing. Business leaders just need to understand that the requirements being asked for are clearly understood and that you have the documentation to back up your answers if or when a cyber incident occurs.

Contact RTC Managed Services to ease your mind

Whether you're trying to understand what it would take for your business to qualify for a policy, or you already have one and want a second set of eyes on your setup, that's exactly the kind of question RTC Managed Services can help you work through. We're not a licensed insurance agent, so we won't tell you whether you qualify. What we can do is look at what's currently in place in your business and help guide you on what insurers commonly expect to see, so you have a clearer picture before you apply. If anything is missing, we can help get it in place quickly. By strengthening your overall risk management, you strengthen your chances of getting the full coverage you're paying for.



<http://rtcmanaged.com>

905-633-3912

Sources

1. ConnectWise, "The State of SMB Cybersecurity in 2025: Racing Against AI-Driven Cyberthreats," 2025 (research conducted by Vanson Bourne, survey of 700 IT and business decision-makers across the US, UK, Canada, and Australia/New Zealand, fielded March 2025).