A SECURITY SPENDING GUIDE FOR SOUTHWEST FLORIDA BUSINESSES

OVERPAID AND UNDERPROTECTED

What your security stack should actually cost a business your size, and how to tell if yours does.

Secured. Insured. Compliant. Which tier your business belongs in, what belongs in each one, and the two places businesses consistently overspend.

four winds it
Business-Minded Technology™

fourwindsit.com
(941) 315-2380

The most expensive mistake in security is not the one you think

Most business owners assume the worst security mistake is not spending enough. It isn't.

The most expensive mistake we see is a business paying for a security stack built for a company four times its size, while missing two or three basic controls that would have actually mattered. They are spending real money every month and they are still going to have a problem at renewal.

This happens because of how security gets sold. The incentive in our industry runs one direction: more products, bigger bundle, higher monthly. Nobody makes money telling you that the platform your provider quoted is designed for a hospital system and you run an eleven-person practice.

> **Security should be sized to the size and scope of your business, and it should grow as you grow. Not before.**

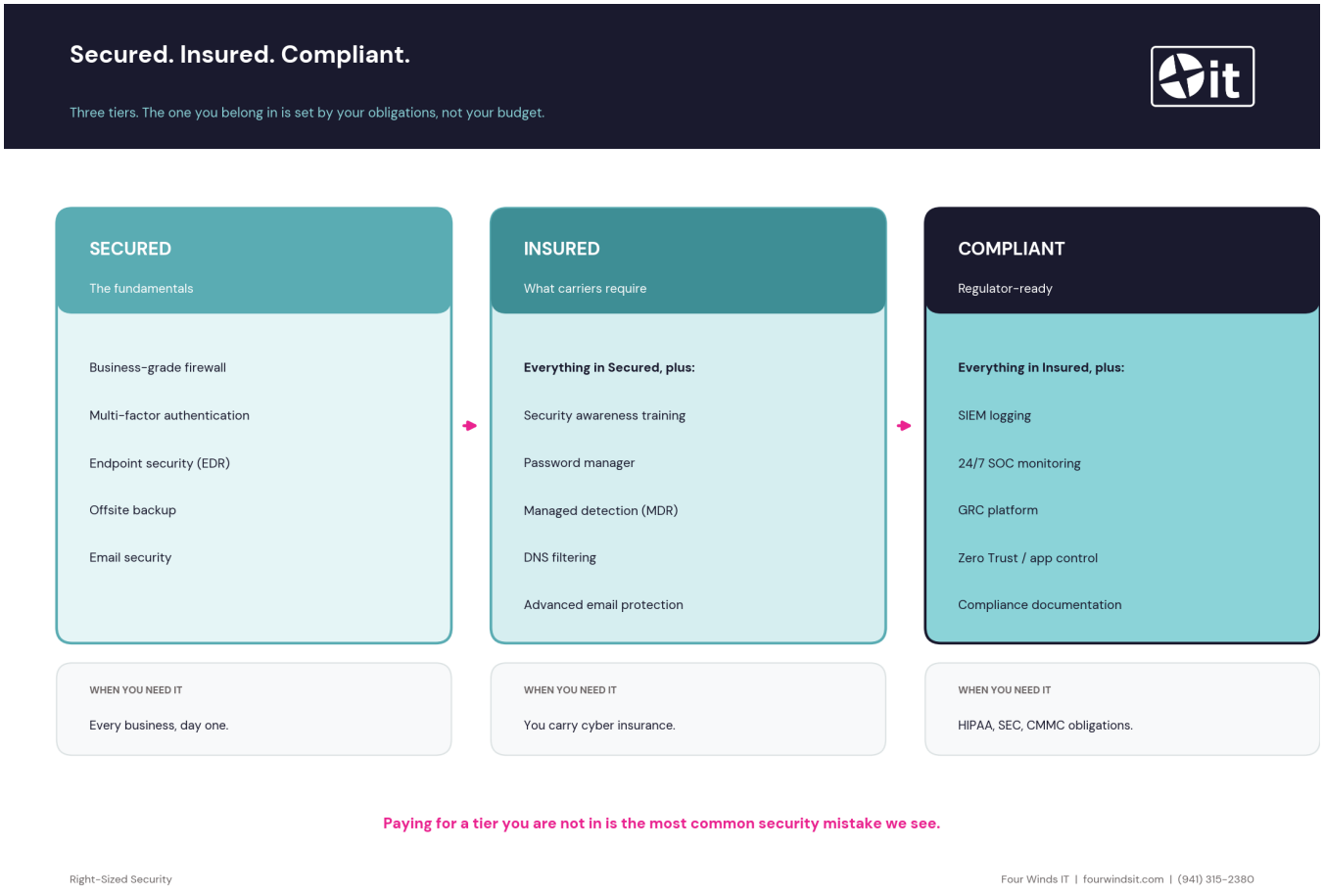
That is not us telling you to skimp. We can take a company from a one-person shop all the way through HIPAA, NIST, CIS, and SOC 2. We do it regularly. If you want to run enterprise-grade security at fifteen people, you are welcome to, and we will build it. It is just going to be expensive per person, and you will carry the policy and procedure overhead that comes with it.

What we will not do is scare you into it.

This guide gives you the framework we use internally to decide what a business actually needs. Read it, figure out which tier you are in, then go look at what you are paying for. Most people find at least one surprise.

The three tiers

We organize security into three tiers. Not because it is a clever marketing structure, but because after more than ten years of doing this, businesses fall into three groups, and the difference between them is not how much they care about security. It is what obligations they carry.



Secured is the floor

If you are a business in 2026 with employees and a bank account, you need all five. There is no size small enough to skip these. A three-person office gets hit by the same automated phishing campaigns as a three-hundred-person office, because the attacks are not targeted, they are sprayed.

Insured is what carriers created

Look at any cyber renewal application from the last two years and you are looking at a checklist of these controls. Carriers figured out that most claims trace back to a missing basic control, so they stopped asking whether you take security seriously and started asking whether MFA is enforced.

Compliant is for when someone can compel proof

The distinguishing feature is not that the controls are better. It is that somebody outside your company can demand evidence, and you have to produce it on their timeline. If nobody can compel you, you probably do not belong here yet.

How to tell which tier you are in

Three questions. Answer honestly.

- **1. Does anyone outside your company have the right to inspect your security?** A regulator, an auditor, or a large client with contractual audit rights. If yes, you are Compliant.
- **2. Do you carry cyber insurance, or does a client or carrier require specific controls?** If yes, you are Insured, and your floor is set by the application you signed, not by your own judgment.
- **3. Do you have employees, email, and data you cannot afford to lose?** Then you are Secured, and that is a legitimate place to be. Plenty of well-run businesses operate here correctly.

What actually moves you up

Tiers change because the business changes. These are the real triggers, and none of them are a salesperson's phone call.

TRIGGER	WHERE IT MOVES YOU
You buy a cyber insurance policy	Secured to Insured
A client sends a security questionnaire as a condition of the contract	Secured to Insured
You start handling protected health information	Insured to Compliant
You take on a government or defense contract	Insured to Compliant
You cross roughly 50 employees	Insured, with Compliant on the horizon
You acquire a business or open a second location	Re-evaluate everything

> **Notice what is not on that list: the calendar. Nobody should move you up a tier because it is renewal season and the provider needs a bigger number.**

The part nobody wants to talk about

Here is a question worth asking before you buy another security product.

Can you name what you are currently paying for?

Not the total. The line items. Which products, what each one does, what each one costs.

Most people cannot, and that is by design. When security is bundled into a single line on your invoice, three things become invisible.

- **You cannot tell which tier you are paying for.** You might be paying Compliant-tier prices for a Secured-tier stack, or the reverse, which is worse.
- **You cannot see overlap.** We regularly find businesses paying for two products that do the same job, because one was added years ago and never removed when the newer one came in.
- **You cannot make a decision.** If you do not know what DNS filtering costs per user per month, you cannot decide whether it is worth it. You are just approving a number.

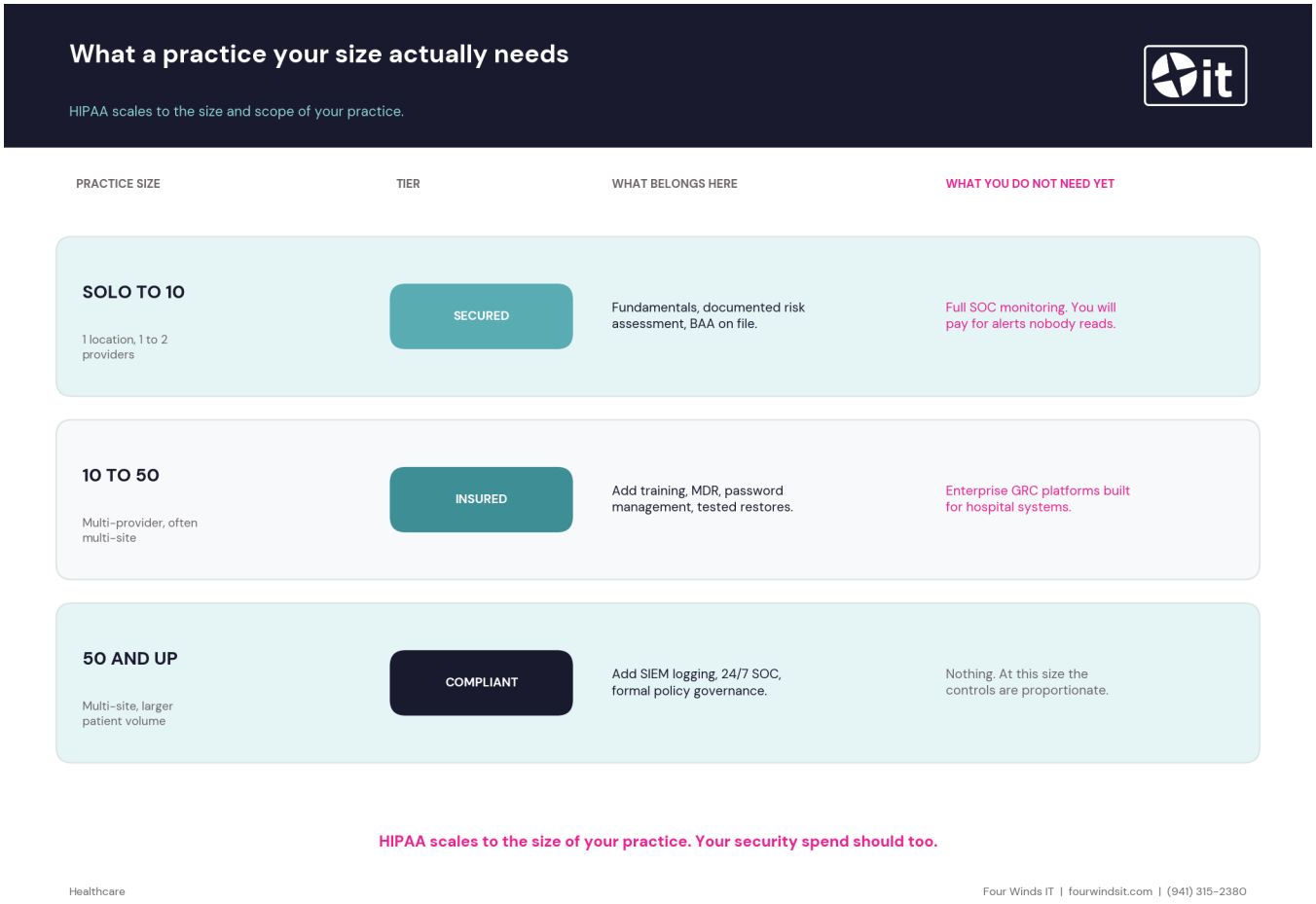
We bill every security component as its own line item, with a monthly report behind it. Not because it is generous. Because a client who can see what they are buying makes better decisions, and clients who make better decisions stay clients.

> **If your provider cannot produce a line-item breakdown of your security stack within a day, that is the finding. You do not need to know anything about firewalls to know that is a problem.**

If you run a medical practice

HIPAA is the most misunderstood regulation we deal with, and the misunderstanding costs practices real money in both directions.

What HIPAA actually says is that your safeguards should be appropriate to the size, complexity, and capabilities of your organization. That language is in the rule. It is not a loophole. A five-provider practice is not held to the same implementation as a regional hospital system.



The three things that actually get practices in trouble

- **No current security risk assessment.** The first document requested in almost any inquiry, and most practices either never did one or did one years ago and filed it.
- **No Business Associate Agreement with the IT provider.** If your technology company touches systems with patient data and there is no BAA, that gap is on your side. Ask today.
- **Controls that exist but cannot be proven.** In an audit, probably reads the same as no.

Proof is the product

Where practices overspend

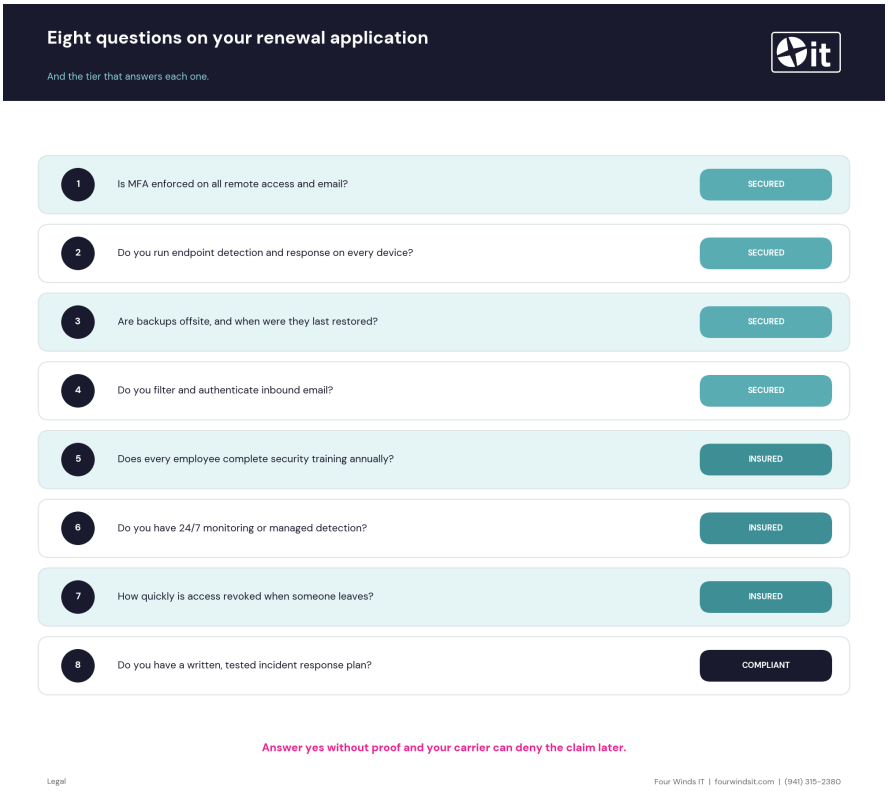
Twenty-four-hour SOC monitoring at a scale where nobody is positioned to act on the alerts, and enterprise governance platforms built for organizations with a compliance department. Both are real products. Both are usually premature under fifty people.

Where practices underspend

Documentation and restore testing. Neither is exciting. Both are what you are actually judged on.

If you run a law firm

Your obligation is not primarily regulatory. It is ethical and contractual, and that changes what matters. Three parties are evaluating your security right now, whether or not you have noticed: your cyber carrier, your malpractice carrier, and your clients.

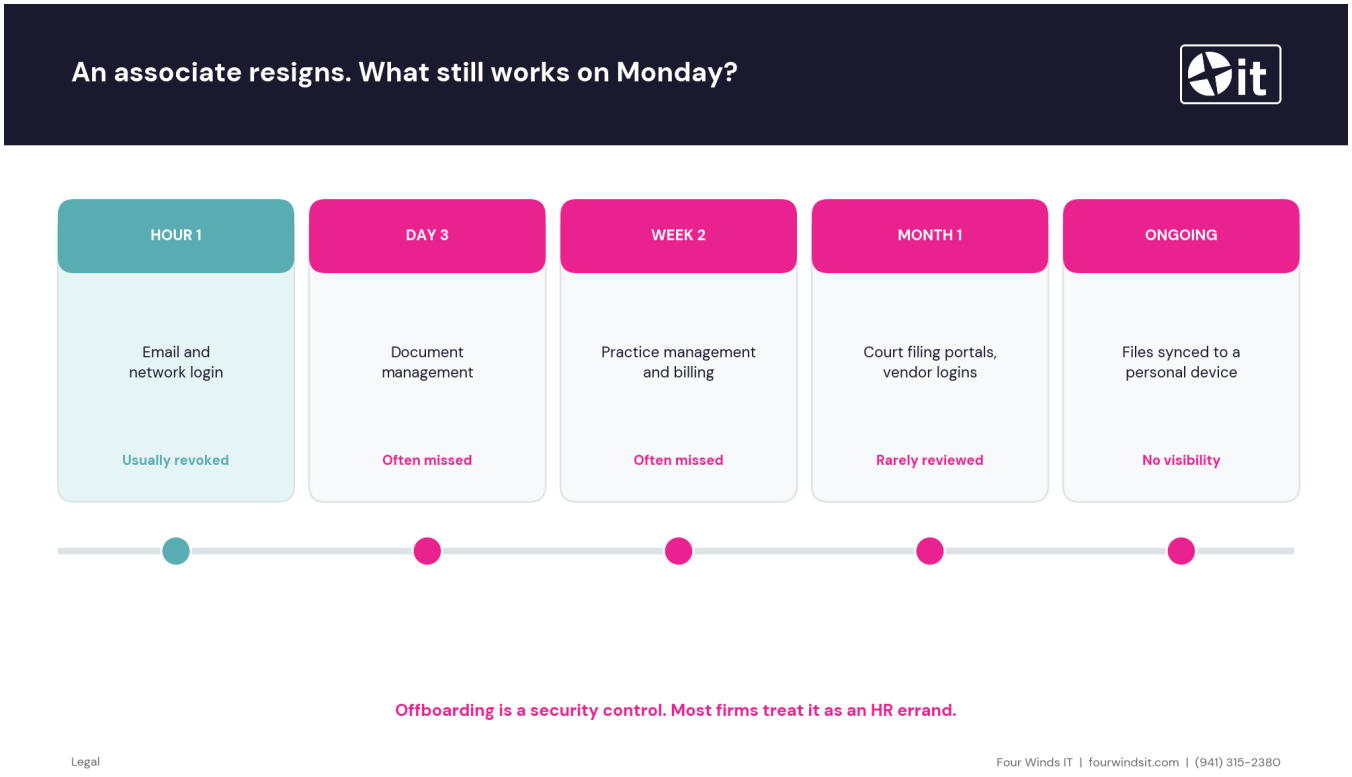


The control most firms fail, and it is not a product

Offboarding. When an associate or a paralegal leaves, email and network access usually die within the hour. Document management often does not. Practice management and billing frequently does not. Court filing portals and vendor logins almost never get reviewed, because nobody owns the list.

That is not a technology gap. It is a process gap, and it is the single most common finding in the reviews we run for firms.

What departure actually looks like



Where firms overspend

Buying a security platform to solve a problem that is really a permissions problem. Role-based access inside the systems you already own is cheaper and more effective than another layer on top of a document management system where everyone can see everything.

Where firms underspend

Email authentication and business email compromise protection. The realistic threat to a firm holding client funds is not an intrusion. It is a convincing email about wire instructions.

If you run a financial services firm

This includes RIAs, CPA practices, and insurance agencies. Different regulators, same structural problem: your obligation is written down somewhere, and it is probably not being met on paper. Most small firms have the controls and not the document. The document is the part that gets examined.

The three things examiners and custodians actually ask for

- **A written information security program.** Not a folder of invoices from your IT provider. A document that says what you protect, how, and who is responsible.
- **Vendor due diligence records.** You are accountable for the security of the firms you hand client data to. Most firms have never documented a single review.
- **An incident response plan.** Written, and ideally tested once. Almost everyone answers this one honestly, because almost nobody has one.

Where financial firms overspend: enterprise governance platforms and centralized log monitoring at a headcount where nobody can act on either. Where they underspend: wire verification procedure and email authentication. The realistic loss event is a client instruction that was not what it appeared to be.

If you run a manufacturing operation

Your risk is not primarily about data. It is about hours of production. This is how it actually happens, and it is not the way it gets pitched to you.

The three things that matter most here

- **Separation between the office network and the plant floor.** If a compromise on the business side can reach production, the blast radius is your output, not your paperwork.
- **A tested restore of the ERP specifically.** Not backups in general. The system that schedules production, restored, with a date on the test.
- **Contractor and temp offboarding.** Manufacturing has more short-term access than almost any industry we work in, and less process around removing it.

The obligation you may not have noticed is your customers. Larger buyers now send vendor security questionnaires as a condition of the contract, and defense-adjacent work brings CMMC requirements with real deadlines. That is what moves a manufacturer to Compliant, and it usually arrives as a purchase order attachment rather than a regulation.

Find out which tier you are actually in

You can do a version of this yourself in about an hour. Pull your last invoice, list every security line item, and check it against the tier tables in this guide. If your provider cannot give you the line items, you have learned something already.

There is also a ninety-second version at fourwindsit.com/resources/security-tier-check. Three questions, no email required to see the result.

IF YOU WOULD RATHER WE DID IT

The Security Stack Review

Send us your cyber policy or your most recent renewal application, whichever you have handy. A client security questionnaire works too.

We come back with which of those controls you can actually prove today, which ones you cannot, and which tier your business is genuinely operating at.

No charge. No meeting required. Five business days.

If you want the fuller picture, send your IT invoice along with it and we will check whether your spend matches your tier. Optional. Plenty of people skip it.

If your renewal is coming up in the next sixty days, this is the useful window. Finding a gap now is a very different conversation than finding it on the application.

If the answer is that you are in good shape, we will tell you that. We have done it plenty of times, and it is a much better outcome for everybody than selling you something you did not need.

dmborden@fourwindsit.com | (941) 315-2380 | fourwindsit.com

Four Winds IT is a technology company serving 300+ businesses across Southwest Florida, headquartered right here in Sarasota. Strategy, cybersecurity, cloud, and AI. Itemized billing, no seat minimums, no hardware markup, and a 100% US-based team that answers the phone.