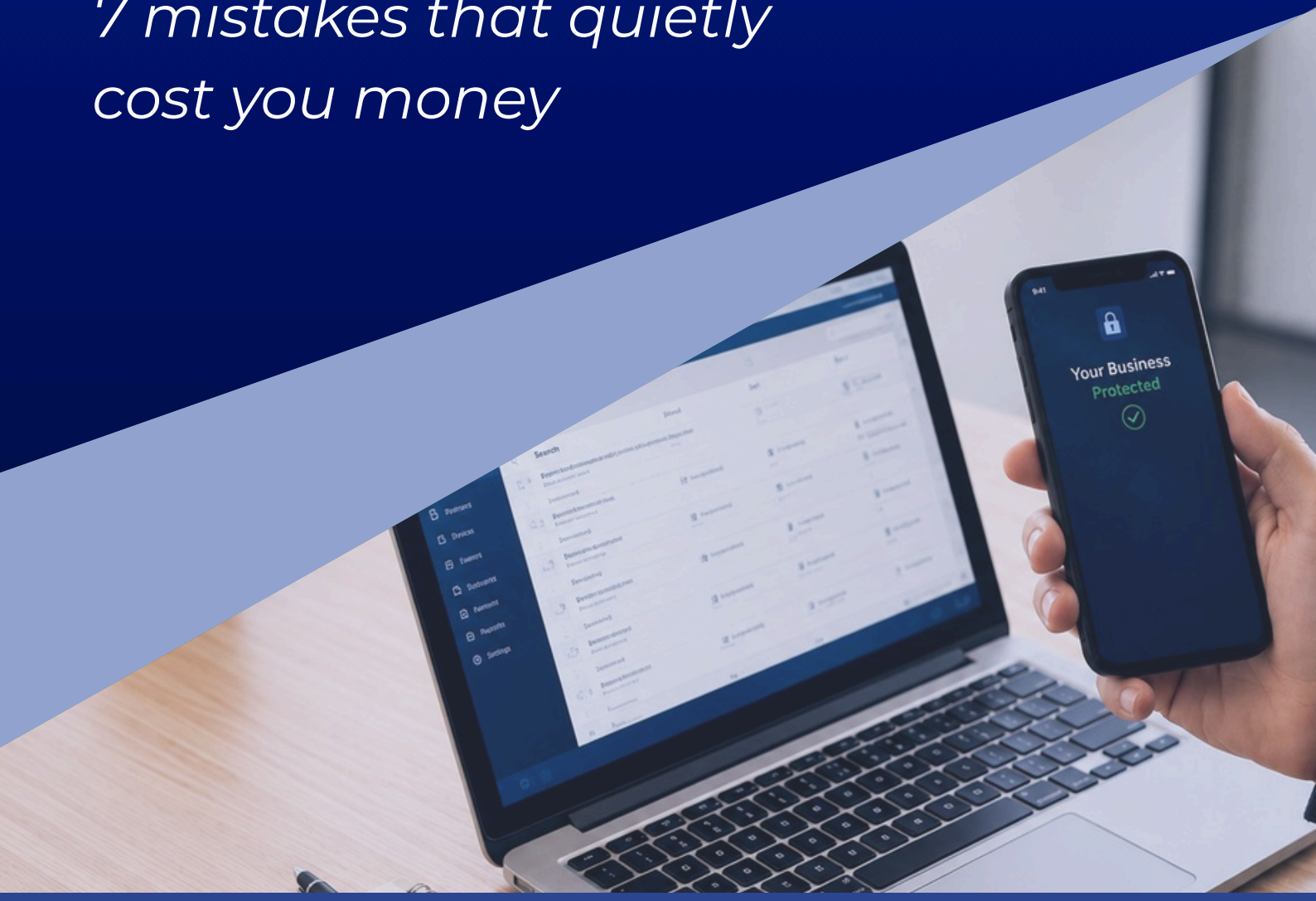
NCI CYBERSECURITY EXPERTS SINCE 1988

The Small Business I.T. Risk Playbook

7 mistakes that quietly cost you money



(615) 270-6081 nashvillecomputer.com sales@nashvillecompuer.com

The Blind Spot

Most IT disasters don't start as disasters. They start small: a backup nobody's checked in a year, a former employee's login that never got shut off, a firewall that's been "good enough" since it was installed. None of these feel urgent on their own. That's exactly why they last so long.

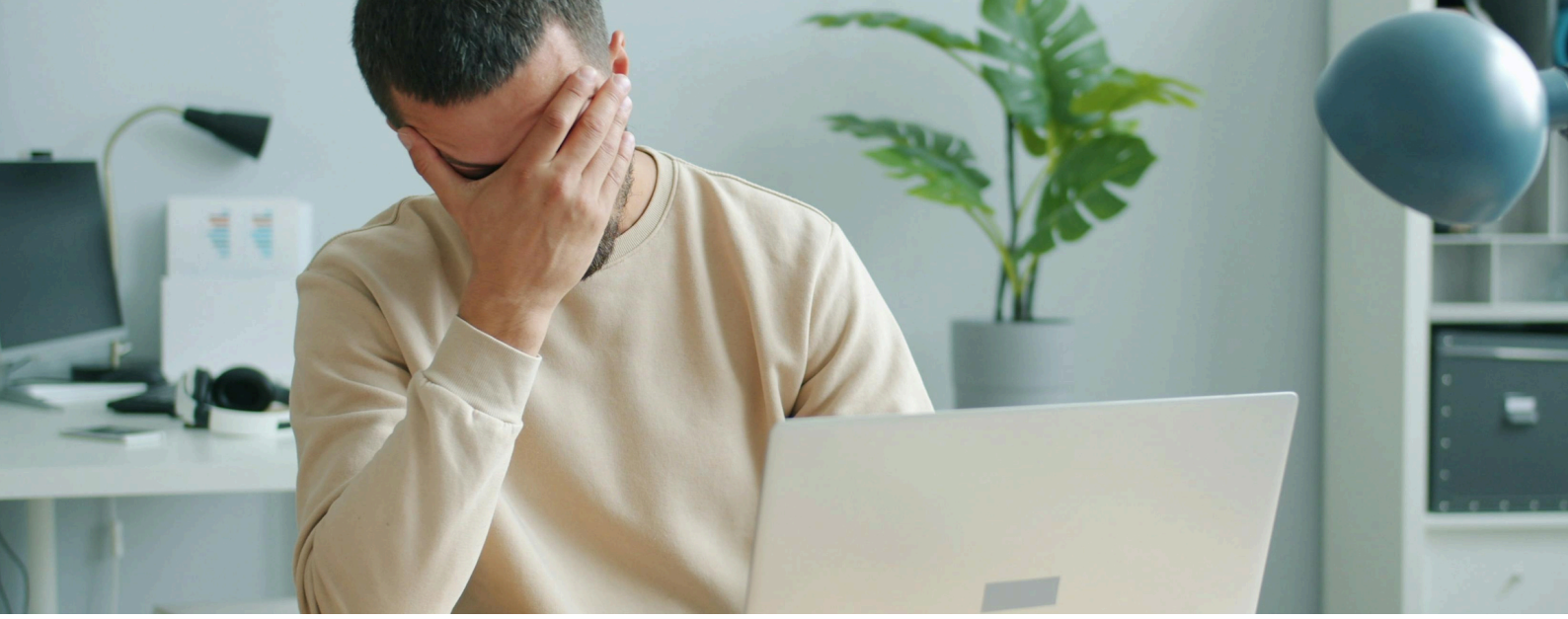
By the time one of these gaps causes real damage — a breach, a lost weekend recovering from a crashed server, a compliance audit that goes sideways — it's not a surprise to anyone who actually looked. It was always there. It just wasn't anyone's job to notice.

This playbook walks through the same 7 mistakes from the checklist, but with the detail that actually matters: what each one looks like in a normal, unremarkable Tuesday; what it's quietly costing you; the signs it's already past "theoretical"; and the difference between patching it and actually fixing it.

You don't need to tackle all seven this week.

You need to know which ones are live.

Charles Henson
Owner, NCI



The 7 Costly IT Mistakes

01 **No One Clearly Owns IT Decisions**

Why ad hoc IT decisions cost more than they should.

02 **Backups Exist, But No One's Tested Them**

Why an untested backup can't be trusted.

03 **Cybersecurity Is A Checkbox, Not A System**

Why having security tools isn't the same as having protection.

04 **Old Employees Still Have Access**

Why lingering access is a bigger risk than it looks.

05 **IT Spending Is 100% Reactive**

Why reactive spending costs more than a plan.

06 **You Don't Actually Know Your IT Provider**

Why inconsistent support costs you time.

07 **No Plan For Growth**

Why IT built for today can't handle tomorrow.

No One Clearly Owns IT Decisions

Ask five people at a typical small business who's actually responsible for IT, and you'll often get five different answers, or a shrug.

Decisions get made by whoever's dealing with the fire in front of them. Software gets purchased twice because nobody knew it was already handled. A security setting gets changed to fix one problem and quietly opens another, and nobody notices for months because tracking the big picture isn't officially anyone's job.

The cost isn't dramatic, it's just constant: wasted spend, drift, and, when something does break badly, precious time lost figuring out who should even be handling it before anyone starts fixing it.

You're probably living this if:

- **You can't immediately name the person, internal or outsourced, who owns your IT roadmap.**
- **IT purchases happen reactively, without being weighed against any larger plan.**
- **Different people have made conflicting technology decisions in the past year.**

The gap between patching it and fixing it:

Naming "whoever's most technical" as the go-to person isn't the same as building real ownership. A real fix means a dedicated point of accountability, internal hire or outsourced account manager, who has actual visibility into your goals and budget, not just your ticket queue.

Backups Exist, But Aren't Tested

Having backups running on a schedule vs. knowing they actually work are two completely different things, and most small businesses only find out the difference the hard way. A backup that's never been restored is a theory, not a safety net.

When it fails, you don't discover the problem until you're mid-ransomware attack or staring at a dead server, reaching for the thing that was supposed to save you. That's the worst possible moment to learn your restore takes three days instead of three hours, or doesn't work at all. The real cost was never the backup itself. It's the operating time you lose scrambling for a plan B that should have already existed.

Ask yourself:

- **Can anyone tell you the last time a dull restore was actually tested?**
- **If a backup job silently failed tonights, would anyone find out before you needed it?**
- **Do you know your actual recovery time, in hours, off the top of your head?**

The gap between patching it and fixing it:

A green checkmark on your backup software tells you a job ran. It doesn't tell you it worked. The real fix is scheduled, documented restore tests (quarterly at minimum, more often for anything critical) with a known recovery time you could quote without checking.

Cybersecurity Is Just A Checkbox

A lot of small businesses have real security tools like a firewall, antivirus, and maybe a password policy, but still have almost no real protection, because none of it is working together. Plus, nothing is watching for the threats that actually get through. Attacks on small businesses are rarely sophisticated. They're phishing emails, stolen credentials, a cloud setting configured wrong three years ago and never revisited.

One click is often all it takes: a locked-down network, a ransom demand, exposed client data. What follows is worse than the incident itself, the trust hit with clients, potential compliance exposure, and a cyber insurance renewal that gets harder and more expensive with an incident on record.

Signs this is you:

- **Multi-factor authentication isn't enforced everywhere it should be.**
- **Employee phishing training was a one-time thing, if it happened at all.**
- **Nobody's actively watching for suspicious activity.**

The gap between patching it and fixing it:

Installing antivirus and calling it done is a checkbox. Real protection is layered with network security, cloud security, MFA, role-based access, tested backups, ongoing employee training. This should work together as one reviewed system, not a pile of separate tools nobody revisits.

Old Employees Still Have Access

Someone leaves the company. Their email gets shut off, usually. Their access to the CRM, the shared drive, the accounting software, the VPN (those often don't, because offboarding isn't a written checklist, it's whatever the departing manager happens to remember to ask for.)

Every account left open is a door nobody's watching, and it doesn't take malicious intent for that to matter. Old credentials sitting in a breach database are exploitable whether or not the former employee ever meant harm. It's also one of the very first things a cyber insurance carrier or compliance auditor checks, and a vague answer here can cost you at renewal or during an audit.

You likely have this problem if:

- **There's no written offboarding checklist and it typically happens from memory.**
- **Nobody periodically reviews old accounts to confirm they're actually closed.**
- **You couldn't produce a clean list of every system a departing employee had access to.**

The gap between patching it and fixing it:

Disabling email on someone's last day feels like enough. It isn't. The real fix is a documented process covering every system, executed the same day, every time... not a mental checklist that depends on who happens to be handling the exit.

IT Spending Is 100% Reactive

If IT only gets money when something breaks (a dead server, a laptop that finally gives out, a compliance requirement that forces your hand) you're running on emergency budgeting, and emergency budgeting is always the most expensive kind. There's no roadmap, no sense of what's coming next quarter, just fires as they arrive.

Rush rates and absorbed downtime cost more than planned upgrades ever would. Worse, reactive spending means your technology never gets ahead of the business; you're permanently patching instead of planning, which quietly becomes its own drag on growth.

This is likely you if:

- **You couldn't describe what your IT budget looks like next year.**
- **Major purchases consistently happen as emergencies, not planned upgrades.**
- **Nobody reviews your technology roadmap against your actual business goals.**

The gap between patching it and fixing it:

Approving spend as emergencies land keeps the lights on. It doesn't build anything. The real fix is an actual budget and roadmap, reviewed on a set cadence, tied to where the business is headed, not just what broke this month.

You Don’t Know Your IT Provider

Every call goes to someone new. A different voice, no context on your setup or your history, no memory of what happened last time you called. You end up re-explaining your business from scratch, every single time.

That costs more than time. Context gets lost and the small details a familiar technician would catch on sight get missed by someone seeing your systems for the first time. A fifteen-minute fix turns into an hour, because "figuring out your setup" is baked into every ticket before the actual work even starts.

You’ll recognize this if:

- **You can’t name your primary technician.**
- **You’ve had to re-explain the same issue to more than one person.**
- **No one checks in on your account outside of active tickets.**

The gap between patching it and fixing it:

Switching providers and hoping the next one's different rarely changes the pattern. The real fix is a provider structure built around continuity (consistent technicians, a dedicated account manager, routine check-ins) instead of a rotating cast of strangers reading off a ticket.

No Plan for Growth

Your current setup works fine, for your current size. But there's no plan for what happens when you add ten people, open a second location, or need to support a hybrid team. Growth becomes something your IT reacts to, instead of something it was built to handle.

That gap turns into the thing slowing growth down instead of supporting it: new hires waiting days for equipment, a new location improvising its own systems from scratch, infrastructure that has to be rebuilt, expensively and urgently, every time the business crosses its next size threshold.

You're probably feeling this if:

- **No one's mapped out what IT needs to look like at your next stage.**
- **New employee onboarding is slow or inconsistent.**
- **A new hire or location would mean scrambling, not following an existing process.**

The gap between patching it and fixing it: growth-related IT needs as they come up feels manageable until it isn't. The real fix is infrastructure, support, and monitoring built with headroom, so growth is something your systems support instead of struggle to keep up with.

A 30-60-90 Day Plan

You don't need to fix all seven mistakes this month.
You need a starting point.

First 30 Days

Identify ownership. Before anything else changes, know who's actually accountable for IT decisions, and get a straight answer on whether your backups have ever really been tested.

Next 60 Days

Close the highest-exposure gaps first. That's usually access control (old accounts still open) and security layering (MFA, active monitoring). These tend to be the fastest to fix and the riskiest to leave alone.

Within 90 days

Build the plan. A documented budget, a roadmap tied to growth, and a provider relationship that isn't starting from zero every time you call.

Stop Reacting To IT Problems

The first step to working with our team is a free discovery call. We'll talk through your goals, take a look at your current setup, and let you know exactly what a plan with NCI would look like — no obligation to move forward.

01

Meeting 1
Set Your Goals

02

Meeting 2
Evaluate Your IT

03

Meeting 3
Review Your Plan

At the end of our discovery process, you will:

- Have a clear understanding of your current IT infrastructure
- Have a detailed price quote with exact costs for stabilization and ongoing work.

Ready to Get Started?

Call today or schedule online to set up your first discovery meeting.

(615) 270-6081 nashvillecomputer.com