INTERMIXIT

FREE REPORT

No fluff. No tech-speak. Just facts every CPA should know.

EXPOSED: The 7 Most Dangerous IT Mistakes We Uncover in Accounting Firms

What Your IT Provider Isn't Telling You—And How Hidden Gaps Could Put Your Firm, Clients, and Compliance at Risk!

A Special Report by IntermixIT – Experts in IT & Cybersecurity for Accounting Firms

Exposed: The 7 Most Dangerous IT Mistakes We Uncover in Accounting Firms

Let's Be Honest—You're Probably Not as Protected as You Think

If you run an accounting firm, you're sitting on a vault of sensitive financial data. Tax returns. Payroll files. Bank account details. Social security numbers. It's the kind of information your clients trust you to protect—and the kind cybercriminals actively pursue.

Unfortunately, most firms are far more vulnerable than they realize.

They've got antivirus installed. Someone set up a backup system. There's an IT company they can call when something breaks. On paper, it looks like they're covered. But as we've seen over and over again, surface-level protection creates a false sense of security.

When we sit down with managing partners or operations leaders and start asking questions, the confidence starts to fade.

- Are your backups tested and verified regularly?
- Is your IT setup aligned with your cyber insurance policy? (This is HUGE)
- Is multi-factor authentication enabled on all critical systems?
- Could your firm pass an FTC Safeguards audit if it happened tomorrow?

That's usually when things get quiet.

What's most concerning is that these aren't rare issues. **They're everywhere.** Most firms we assess—whether they're local two-partner practices or multi-office teams with millions under management—have one or more of these weaknesses hiding in plain sight. And in many cases, the IT provider hasn't raised a single red flag.

We're not here to create fear. **We're here to create clarity.**

This report outlines the seven most common and dangerous IT mistakes we uncover in accounting firms. You'll learn why they happen, how they quietly put firms at risk, and what your provider should already be doing to prevent them. If any of this sound familiar, it might be time to take a second look at the systems and people you're trusting with your most valuable asset—your data.

What You'll Learn in This Report

This isn't a technical checklist or a generic compliance article. It's a practical, inside look at what's really going on behind the scenes in accounting firms across our region.

Here's what you'll walk away with:

- The seven most common IT security failures we find when assessing CPA firms
- How to identify whether your current IT provider is protecting your firm or just billing you
- A clear explanation of what the FTC Safeguards Rule requires—and what most firms are missing
- The biggest reason cyber insurance claims get denied after a breach
- What a secure, compliant, and truly supported IT environment should look like

If even one of these red flags shows up in your environment, your firm could be more vulnerable than you think.

Let's help you find out…

1. Your Backups Exist. But No One's Watching Them.

Let's be real—almost <u>every</u> accounting firm we talk to says the same thing:

"We have backups."

That's great. But here's the question nobody's asking: **Are they working?**

See, having a backup system is one thing. Knowing it's been tested, verified, and can actually recover your data in a crisis? That's something else entirely.

We see this all the time. The firm thinks they're covered. But when we look closer, we find backups that haven't run in weeks. No off-site copies. No alerts if the system fails. And in some cases, the backup is sitting on the same server as the live files. One crash or ransomware attack, and *everything's gone.*

If you're an accountant, you already know the stakes. Losing client tax files or payroll records during busy season isn't just a nuisance—it's a full-blown nightmare. And it's your reputation on the line.

Here's how to know if this is a problem:

- When was the last time someone tested your backups to make sure they actually work?
- Is someone actively monitoring them daily, or are you just hoping they're running?
- Could you recover your client files today if your server crashed or got encrypted by ransomware?

If you're not sure about any of those, that's your answer.

Backups should be like fire extinguishers. Always in place, regularly checked, and ready when you need them—not a dusty afterthought.

2. There's No Multi-Factor Authentication on Critical Systems

Most breaches don't start with hackers cracking complex code. They start with someone logging into your email.

One password. One careless click. One reused login from a compromised website—and suddenly someone else is inside your system.

Multi-factor authentication (MFA) is one of the simplest and most effective ways to stop that from happening. It requires a second layer of verification—usually a code from your phone or app—to log in.

And yet, we walk into accounting firms every month where no one is using MFA for Microsoft 365, cloud accounting software, or remote desktops. That's a huge red flag.

If a hacker gets into your email, they can reset passwords, impersonate your firm, and access client files. MFA prevents that. It's basic, and it's expected.

Even cyber insurance carriers now require MFA before they'll even consider paying a claim.

If your provider hasn't enforced MFA across your systems, **they're not protecting you.** They're leaving the front door wide open.

3. Your IT Provider Hasn't Mentioned the FTC Safeguards Rule

If you're an accounting firm, you are subject to the FTC Safeguards Rule. It requires firms to implement a written information security plan, conduct regular risk assessments, provide staff training, and monitor for threats.

We're not talking about optional best practices. These are federal requirements.

Yet, most firms we assess have never even heard of the rule—because their IT provider hasn't mentioned it.

That's unacceptable.

If your provider doesn't know the rule exists, **you're already at risk.** If they've heard of it but haven't walked you through where you stand, they're not doing their job.

The FTC doesn't care if you "thought you were covered." You either are or you aren't—and you need documentation to prove it.

4. There's No Written Incident Response Plan

If a breach happens—and let's be honest, it might—what's the first step?

Who do you call? Who talks to clients? What systems get shut down? When do you notify regulators?

If the answer is "we'd figure it out," you're not prepared.

A proper incident response plan outlines exactly what to do, when to do it, and who's responsible. It reduces panic, controls damage, and keeps you in compliance.

We ask every firm we assess: "Do you have a written response plan?" The answer is almost always no.

And here's the catch: the FTC Safeguards Rule **requires** one. So does your cyber insurance policy.

If you don't have it documented, you're not ready—and regulators know it.

5. You're Relying on Antivirus and Calling It "Security"

There was a time when antivirus software was enough. That time is long gone.

Today, threats are faster, smarter, and more targeted than ever. And your protection needs to go far beyond a single application.

We still see firms using only antivirus, with no active threat monitoring, no firewall logging, no vulnerability scans, and no phishing simulations.

That's not security. That's luck.

Real cybersecurity includes:

- Managed detection and response
- Multi-layered endpoint protection
- User awareness training
- Patch management
- Encrypted backups
- Real-time alerting when something goes wrong

If your provider isn't giving you these, you're exposed, and you won't know it until it's too late.

6. Your Staff Isn't Being Trained to Spot Cyber Threats

It only takes one click on the wrong email to bring your firm to a halt.

Phishing attacks don't care if you're a solo practice or a 40-person firm. If your staff isn't trained to spot fake logins, bad links, or spoofed emails, you're vulnerable.

Training doesn't need to be complex. But it does need to be consistent.

You should be running phishing simulations, providing short training videos, and reinforcing best practices throughout the year. If your provider isn't offering this—or hasn't brought it up—they're skipping a critical piece of your defense.

Human error is still the number one cause of data breaches. You can't afford to leave your people unprepared.

7. Your "Flat-Rate" IT Plan Doesn't Cover What You Actually Need

This one might sting…

A lot of firms think they're on an all-inclusive IT plan. But when we dig into the details, we find that certain cybersecurity tools, compliance support, monitoring, and even routine maintenance are all considered "extras." Many times the "routine maintenance" isn't even getting done.

That's not flat-rate. That's **bait-and-switch**.

We've seen firms paying monthly fees only to get hit with surprise invoices for services they assumed were included. Or worse, they only find out something isn't covered **after** an incident.

Ask your provider to show you exactly what’s included—in writing. If it’s vague or full of exceptions, that’s a sign they’re protecting themselves—not you.

Your IT agreement should be simple, straightforward, and built around what your firm actually needs to stay secure, compliant, and supported.

You’ve Seen the Gaps—Now What?

If you’ve made it this far, it’s probably because something resonated. Maybe you recognized a few of the mistakes. Maybe more than a few. Or maybe this confirmed what you’ve suspected for a while: your current IT setup might not be as solid as it looks.

Good Firms Get Burned All the Time

Here’s the problem: most firms don’t realize there’s an issue until something breaks. A ransomware attack. A failed backup. A compliance fine. That’s when panic sets in—and the finger-pointing starts.

But by then, it’s too late to prevent it.

The good news is that you don’t have to wait for the disaster. **You can get ahead of it.**

Confidence Starts with Clarity

This guide wasn’t about selling fear. It was about showing you what’s really happening inside firms like yours. And once you know where the risks are, you can do something about them.

The firms that win in this space aren’t the ones who get lucky. They’re the ones who ask the hard questions, challenge the status quo, and partner with experts who treat IT like a mission-critical part of the business.

They’re not reactive. They’re ready.

So What’s the Next Step?

It’s not overhauling everything overnight. It’s not switching providers tomorrow. It’s getting a clear view of where your firm stands—and what’s putting it at risk.

We’ve made that first step simple….

INTERMIXIT

How to Get Started with IntermixIT

1. **Book Your 15-Minute Introduction Call – www.intermixit.com/15minutes**
   This isn't a sales pitch—it's a focused conversation to understand your firm's current setup, your challenges, and what's keeping you up at night. We'll walk you through our no-cost cybersecurity assessment and help you identify any immediate vulnerabilities or compliance gaps.

2. **Receive Your Cybersecurity Assessment**
   Once we connect, our team will perform a comprehensive review of your IT environment. We'll evaluate your systems with a focus on security, productivity, and budget impact. You'll walk away with clear, actionable insights—not vague tech talk.

3. **Discuss Customized IT Solutions**
   We'll go over the assessment together, answer your questions, and show you how IntermixIT can support your firm with all-inclusive, fully managed IT services. No surprise fees. No confusing contracts. Just real support that works the way it should.

Get Started with IntermixIT – A 15-Minute Call to Secure Your Assessment
Schedule Here - *www.intermixit.com/15minutes*

Interested in Seeing How Another Accounting Firm Got Their IT Right?

Gift CPAs is a fast-growing firm with five offices across Pennsylvania. Before working with IntermixIT, they struggled with slow systems, weak cybersecurity, and reactive IT support. Now, they're faster, more secure, and fully supported—especially during tax season.

Scan the Code - Read the Case Study!

https://intermixit.com/success-story-gift-cpa/

Take a look inside this success story to see how IntermixIT can provide the secure, reliable IT support your firm needs.