THE I.T. M$NEY PIT

5 Ways NC Municipalities and Local Businesses Waste Thousands On IT Without Getting Security, Support, Or Results

The I.T. Money Pit

5 Ways NC Municipalities, CPA Firms, Construction Companies, and Manufacturers Waste Thousands On IT Without Getting Security, Support, Or Results

After working with municipalities and businesses across North Carolina for more than 10 years, I've seen firsthand how IT can quietly drain budgets while still leaving organizations exposed to downtime, cyberattacks, and poor performance.

This report will show you the five biggest money pits where NC organizations waste thousands on IT every year, and more importantly, what you can do right now to stop the waste, tighten security, and get the reliable support your team deserves.

Provided By: CW IT Support
Author: Brian Satz, President
5500 Market Street, Unit 100B
Wilmington NC 28405
www.cwitsupport.com
910-726-1595

About The Author

Brian Satz, President of CW IT Support

I've spent more than 15 years in IT, and in that time I've seen just about everything—from towns running on a single aging server in a back closet, to CPA firms storing client data without any real protection, to manufacturers losing entire days of production because their systems went down.

That's why I built CW IT Support: to give North Carolina municipalities and businesses the kind of IT partner they can count on. No excuses, no jargon, just real solutions that keep systems running and keep data safe.

Our team is trusted by town managers, city clerks, finance officers, CPAs, contractors, and business owners across North Carolina. Under my leadership, CW IT Support was named a finalist in the 2024 MSP Titans of the Industry Awards in the Local Government category, a recognition that reflects our dedication to protecting and serving the public sector with integrity and innovation.

But what matters most to me is that the organizations we serve can sleep at night knowing they are protected. I believe IT should make your life easier, not harder. That's the standard we hold ourselves to every single day at CW IT Support.

The I.T. Money Pit:
5 Ways North Carolina Organizations Waste Money On IT

For most organizations, IT is like a hidden money pit. Leaders are spending thousands of dollars every year, but they're still not getting the speed, security, and reliability they need. Systems crash, employees waste hours fighting with technology, and executives are left wondering where all the money went.

As Andy Grove, the former CEO of Intel, once said, "Only the paranoid survive." In my experience, most leaders aren't paranoid enough when it comes to IT waste and loss prevention. They don't know what they don't know, and that blind spot can cost hundreds of thousands of dollars in wasted spend, downtime, and cyber risk.

At CW IT Support, we've uncovered millions of dollars in wasted technology spend across North Carolina towns, CPA firms, construction companies, and manufacturers. From outdated systems and duplicate software, to "shadow IT" purchases that no one is tracking, the waste adds up fast.

The good news is that it doesn't have to be this way. Every single organization we've assessed has uncovered fast savings and stronger protection once we pulled back the curtain. Not one exception.

In this report, I'll walk you through the **five most common ways North Carolina organizations waste money on IT.** As you read, I want you to ask yourself a simple question: *How much is this costing us right now?*

#1: “Maverick” Spending, No Strategy And Undisciplined Planning

Too many North Carolina organizations treat IT like a junk drawer. Over the years, different “fixes” get slapped on without a plan—old servers left running in closets, overlapping software subscriptions nobody remembers buying, and a mix of hardware that doesn’t talk to each other.

When we come in to audit a new client, we often find:

- Multiple servers and devices that could be consolidated or moved to the cloud.
- Duplicate software systems doing the same job, each draining the budget.
- Outdated applications still in use, creating serious cybersecurity gaps.
- Backup systems that cost money but can’t be trusted in an emergency.

The result? Thousands of dollars wasted, frustrated employees, and leaders in the dark about what they’re actually paying for.

This lack of strategy is especially costly for municipalities and CPA firms, where compliance and transparency matter. For manufacturers and construction companies, it often means projects slow down and productivity takes a hit.

The first step to solving this problem is simple: conduct a full IT audit. When you know what you have, you can eliminate redundancies, consolidate systems, and finally see where your money is going.

At CW IT Support, we’ve never done an audit that didn’t uncover immediate savings. If your IT feels like a black hole, chances are you’re paying for far more than you need—and still not getting the results you should.

At CW IT Support, we avoid this by conducting quarterly SaaS audits for our clients. *We review every subscription in use, identify duplicates or unused licenses, and consolidate tools where possible. This not only saves money, but also reduces the number of entry points hackers can exploit.*

For example, one electrical contracting company we worked with ordered multiple versions of M365 licensing for each employee because they thought they needed E-mail licensing in addition to the apps, and double-purchased licensing for nearly 150 employees! Once we corrected this, it saved them close to $10,000 annually on M365 subscriptions alone.

#2: SaaS Bloat

Cloud software is supposed to make life easier, but for many North Carolina organizations it's just another money pit. With every department swiping a credit card for the latest app, it's easy to lose track of what's being used and what's not. This "shadow IT" drains budgets, creates duplication, and opens the door to security risks.

The reality is harsh:

- The average midsize business runs more than 250 SaaS apps, but less than half of those licenses are actually used.
- Most organizations overspend on SaaS by 30 percent or more because no one is managing subscriptions.
- Nearly half of companies admit unused or underused software is one of their top cost problems.

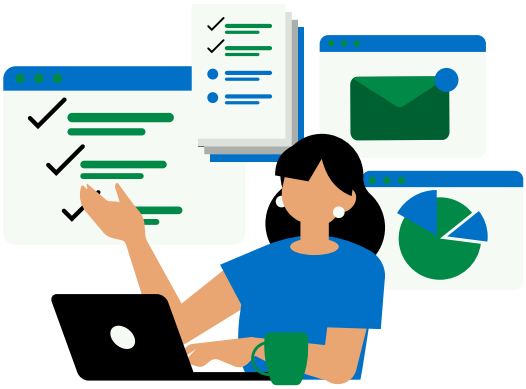
Here's what that looks like in real numbers: if a 10-person team is paying for 100 SaaS apps at an average of $25 per user, but only half are being used, that's $1,250 every month—or $15,000 every year—gone with nothing to show for it.

We see this all the time in NC municipalities, CPA firms, and construction companies: three different project management tools, multiple video meeting platforms, or old accounts still active long after an employee has left. The costs pile up silently, month after month.

At CW IT Support, we eliminate SaaS bloat by auditing every subscription, consolidating tools, and making sure you only pay for what you actually need. This not only saves thousands of dollars a year, it also closes security gaps created by unused accounts and redundant systems.

We also routinely find:

- Businesses paying for full enterprise plans when a basic tier would do just fine.
- Licenses still active for employees who left months ago.
- Multiple apps doing the same job—three project management tools, two video meeting platforms, and several CRMs—all bleeding money every month.



At CW IT Support, part of our service is to conduct a quarterly SaaS audit. We review every subscription, cut out what's no longer needed, consolidate where possible, and downgrade bloated plans. This not only saves thousands of dollars, it also shuts down another door hackers can use to get into your systems.

Left unchecked, SaaS bloat silently drains your IT budget and wastes money that should go directly to your bottom line. Even trimming 10 to 20 percent of unused apps can free up thousands of dollars for higher-payoff investments.

On average, our clients save $5,000 to $15,000 per year just by consolidating SaaS applications and getting visibility into where the money is really going.

***In fact, one North Carolina CPA firm we worked with** discovered they were paying for three separate cloud storage platforms and two different video conferencing tools. We consolidated them into one secure system, cut over $12,000 in annual waste, and reduced their cyber risk by eliminating five unnecessary entry points.*

#3: Weak Cybersecurity and Compliance Protections

You might not think of spending money on cybersecurity as a "cost saver," but you'd see it differently if you ever experienced the massive fallout of a ransomware attack or data breach.

When A Cyber-Attack Happens, The Damage Stack Up And Multiply While Business Grinds to a Halt.

The first thing you lose is productivity. At best, your team is crippled and scrambling. At worst, you're completely shut down—unable to process payments, serve citizens, close the books, or deliver on contracts. In many cases, thousands or even millions of dollars are drained from accounts with no chance of recovery.

Then come the lawsuits, compliance penalties, reputational damage, and government fines. The epicenter of this disaster lands squarely on your desk—a problem that can derail growth, stall projects, and put your organization in the headlines for all the wrong reasons.

Yet in our audits across North Carolina, we've found that nearly every municipality, CPA firm, construction company, and manufacturer we review is dangerously unprepared. This is true even when leaders believe they've already "got it handled." Before we present them with hard evidence, most executives are convinced their IT team has protections in place. What they really have is a live time bomb under their seat—one incident away from disaster.

Many insurance providers now require proof of strong cybersecurity protections before they'll even write or renew a policy. On top of that, new state and federal data-protection laws are being rolled out, and clients are increasingly demanding evidence of compliance before signing contracts. If you can't show proof, you could lose coverage—or worse, lose business. The question is simple: do you want to wait until you're under the gun to fix it, or get ahead of it now?

> ***At CW IT Support, we have an entire team dedicated to cybersecurity and compliance.*** *Our job is to give clients complete peace of mind that they're not only protected, but also covered when an insurer, regulator, or auditor asks for documentation. For example, a North Carolina CPA firm we recently onboarded discovered their backups weren't compliant with their cyber insurance requirements. We rebuilt their system, documented the protections, and gave them the paperwork they needed to stay covered. That's the level of detail every business needs today.*

#4: Chronic I.T. Problems, System Failures And Slow Response To Problems

There's an old saying: "Overhead walks on two legs." Frustrated, unproductive employees cost more than dollars. They make more mistakes, miss deadlines, and lower morale. But what most leaders don't realize is just how often their employees are slowed down or completely blocked by recurring IT failures. It's hidden from them until someone finally blows up about it.

Yet We Find That Most CEOs Don't Realize Just How Often Their Employees Are Being Interrupted And Distracted Due To Recurring I.T. Failures Because It's "Hidden" From Them.

After one of our audits, many CEOs are shocked to learn just how much time their teams are wasting dealing with nagging IT issues. Hours are lost redoing work, waiting on help desk tickets, or finding workarounds. Employees don't always complain because they'd rather just "make it work"—but the productivity drain adds up quickly.

In one recent case, we found that employees at a local manufacturer were losing an average of three hours per month each waiting on IT support. Across the entire staff, that wasted time was costing the company thousands in payroll plus additional fees to their IT provider for handling the endless tickets. That's a double hit: higher costs and lower output.

In most cases where we see this happening, IT is outsourced to a provider that isn't as responsive as they should be and isn't proactive about preventing problems before they start. Employees submit tickets into a black hole and wait for hours—sometimes days—because there's no guaranteed response time. Productivity stalls while the meter keeps running.

When issues keep coming back, frustrated employees give up and try to fix things themselves, often creating even bigger problems. Meanwhile, leadership is paying their IT company to "manage" the situation, but instead of solving root causes, that vendor is compounding the cost.

At CW IT Support, our average response time is under 15 minutes, and we guarantee resolution times that keep your employees working instead of waiting. For one North Carolina client, we cut wasted downtime from three hours per employee per month down to just 30 minutes. That's the difference between IT being a roadblock and IT being invisible.

#5: Delaying Necessary Upgrades Until Systems Fail

With costs on the rise, it's no surprise many leaders delay upgrades as long as possible. But waiting too long creates a false economy. What feels like savings today often leads to higher expenses tomorrow.

Older systems don't just run slower. They require more maintenance, more support calls, and higher service fees. And when they fail without warning, you're forced into emergency upgrades, expensive data recovery, and costly downtime that could have been avoided with a plan.

Done right, upgrades should be budgeted, phased, and scheduled before failure forces your hand. Stretching systems past their lifespan only increases risk—and the price tag that comes with it.

In many cases, when old systems fail unexpectedly, the damage is bigger than just downtime. Critical data can be lost, and recovering it requires expensive specialists. Migrating functions from an outdated system to a newer one under emergency conditions always costs more than planning the upgrade in advance. To make matters worse, older systems are often no longer supported by the vendor, which leaves them vulnerable to cyber-attacks and compliance failures.

> ***One NC Municipality we supported delayed replacing aging network switches for years,*** *living on borrowed time. Eventually they suffered a massive failure across multiple sites, and introducing new switches on the fly created more issues before it was fully resolved. This project ended up costing them twice as much as it would have if it were planned, plus created a couple of days of downtime and wasted payroll for their team.*

The truth is, upgrades don't have to be disruptive or financially overwhelming. Done correctly, they can be phased in over time with clear budgets, giving leadership visibility and control. That's how you avoid surprises and spread the investment in a way that makes sense.

At CW IT Support, we track and document every piece of equipment, software, and system your organization owns. We map out when each one actually needs to be upgraded and provide budget forecasts so you can plan ahead. This way, you avoid emergencies, reduce downtime, and keep costs predictable.

Is Your Current I.T. Company Allowing You To Waste Money, Break The Law And Incur Risk?

Take This Quiz To Find Out

If your current I.T. company does not score a "Yes" on every point, they are NOT adequately protecting and serving you. Don't let them "convince" you otherwise and DO NOT give them a free pass on any one of these critical points. Remember, it's YOUR business, income and reputation on the line.

- ☐ **Do they meet with you quarterly to review your current I.T. spend and map out future upgrades so you can appropriately budget for I.T. spend?** Or do they wait until an upgrade is on fire and then send you a big, expensive quote for a critical upgrade you didn't budget or plan for?

- ☐ **Have they met with you recently – in the last 3 months – to specifically review and discuss what they are doing NOW to protect you from ransomware and the latest cyber-attacks?** This should be a routine report provided with the quarterly strategy meeting mentioned above.

- ☐ **Do they track and report how many support tickets your team submits each month?** If the number is high, have they shown you a plan to eliminate recurring problems instead of just patching them?

- ☐ Have they proposed ways to **consolidate and eliminate SaaS bloat** in your organization?

- ☐ **Have they ever asked to see your cyber liability insurance policy?** Have they verified they are doing everything your policy REQUIRES to avoid having a claim denied in the event of a cyber-attack?

- ☐ **Do THEY have adequate insurance to cover YOU if they make a mistake and your practice is compromised?** Do you have a copy of THEIR CURRENT policy? Does it specifically cover YOU for losses and damages?

- ☐ **Have you been fully and frankly briefed on what to do IF you get compromised?** Have they provided you with a response plan? If not, WHY?

- [ ] Have they told you if they are outsourcing your support to a third-party organization? **DO YOU KNOW WHO HAS ACCESS TO YOUR I.T. SYSTEMS AND THE DATA IT HOLDS?** If they are outsourcing, have they shown you what security controls they have in place to ensure that a rogue technician, living in another country, would be prevented from using their free and full access to your network to do harm?

- [ ] **Do they have controls in place to force your employees to use strong passwords?** Do they require a PASSWORD management system to prevent employees from using weak passwords? If an employee is fired or quits, do they have a process in place to make sure ALL passwords are changed? Can you see it?

- [ ] **Do they provide employee training so your staff knows how to utilize the tools they have instead of buying additional software and tools you don't need?**

- [ ] **Have they recommended or conducted a comprehensive risk assessment every single year?** By law, you're required to do this, and your I.T. company should be handling the I.T. part of that for you.

- [ ] **Have they implemented web-filtering technology to prevent your employees from going to infected websites or websites you DON'T want them accessing at work?** I know no one in YOUR office would do this, but why risk it?

- [ ] **Have they given you and your employees ANY kind of cybersecurity awareness training?** This is now required by law for many industries and by insurance companies as a condition of receiving coverage.

- [ ] **Have they properly configured your e-mail system to prevent the sending/receiving of confidential or protected data?**

- [ ] **Do they offer, or have they at least talked to you about, dark web/deep web ID monitoring?** There are new tools available that monitor cybercrime websites and data for YOUR specific credentials being sold or traded. Once a leak is detected, this tool notifies you immediately so you can change your password and be on high alert.

Ready For Efficient I.T. Services That Don't Waste Your Money And Put You At Undo Risk?

Because you're a prospective client, I'd like to offer you a **FREE I.T. Systems And Security Assessment** to demonstrate how we could put the ideas in this report to work for you and dramatically improve the value you are getting for your I.T. spend, eliminate waste and reduce your exposure and risk to a devastating cyber-attack.

The next step is simple: Call my office at **910-726-1595** and reference this report to schedule a brief 10- to 15-minute initial consultation.

On this call we can discuss your unique situation and any concerns you have and, of course, answer any questions you have about us. If you feel comfortable moving ahead, we'll schedule a convenient time to conduct our proprietary (and FREE) **I.T. Systems And Security Assessment.**

This Assessment can be conducted with or without your current I.T. company or department knowing (we can give you the full details on our initial call).

At the end of the Assessment, you'll know:

- Where you are overpaying (or getting underserved) for the I.T. services, tools and support you are paying your current I.T. company to deliver.
- Whether or not your company is truly protected from hackers and ransomware, and where you are partially or totally exposed to a devastating, extremely expensive cyber event.
- If your data is actually being backed up in a manner that would allow you to recover it quickly in the event of an emergency or ransomware attack. (Hint: Most backups are NOT.)
- How you could lower the overall costs of I.T. while improving communication, security and performance, as well as the productivity of your employees.

Fresh eyes see things that others cannot – so, at a minimum, our free Assessment is a completely cost- and risk-free way to get a credible third-party validation of the security, stability and efficiency of your I.T. systems.

Sign Up For Your FREE Assessment At Our Website:

https://www.cwitsupport.com/cyber-security-assessment/
or scan this QR code :

If you prefer, you can also e-mail me at brian@cwitsupport.com or call me direct at 910-726-1246.

Please don't be "too busy" and set this aside to deal with it later. If you have even a sneaking suspicion that money is being wasted and you are at risk for a cyber-attack, every minute counts.

Here's What Our Clients Have To Say:

"I called Brian, and he came out here himself at 6:30 in the morning. He and I started up the server that same morning, and I just wanted to hug him. It was very difficult for us, but CW IT Support helped us get through it. Since then, if there's ever an issue, which is rare, I call Brian's cell phone and he gets it worked out."

-Mike Gawinski, CEO, Rulmeca Corportaion

"So for anyone skeptical of outsourcing their IT like I was, I would say don't overlook CW IT Support and don't let the fact that they're not physically on-site interfere with getting the best services at the best price. I mean, I could hire an internal IT employee, but I would have to pay them benefits, and what happens if they get sick or go on vacation? With CW IT Support, the cost is comparable, but I get access to the expertise of an entire firm, and that will always be worth it in my eyes."

-Doug Shipley, Town Manager, Topsail Beach

"At John Starz Electric, we understand the importance of seamless operations in today's fast-paced business world. Down time is lost time. That's why partnering with CW IT Support has been an absolute game changer for us.Their commitment to operating quickly and efficiently is clear ensuring that downtime is minimized, and our productivity is maximized. Their highly trained staff is easy to work with and always there to handle our IT needs in a professional and courteous manner when we need them most! With IT Support, you are not just getting an IT team, you are getting Peace of Mind."

-John Starzynski, President, John Starz Electric

"They don't just wait for problems. They tell us when upgrades are due, when new software can make things more efficient. It's like having a tech partner who's always thinking three steps ahead." That includes expansion planning. "We're still growing, and CW is already helping us think ahead about network structure, user load, and avoiding issues like the IP address shortage we just experienced. That level of foresight is huge."

-Kristen Yow, HR Administrator, Odyssey Mechanical LLC