THE I.T. M$NEY PIT

5 Ways Eye Care Practices Waste Thousands Of Dollars On I.T. And Still Don't Get The Functionality, Security And Support That They Need

IT4EYES
AN STS COMPANY

The I.T. Money Pit

5 Ways Eye Care Practices Waste Thousands Of Dollars On I.T. And Still Don't Get The Functionality, Security And Support That They Need

After conducting hundreds of I.T. assessments for small to midsize practices, we've uncovered 5 areas where companies routinely spend hundreds of thousands of dollars on I.T. yet still struggle with recurring problems, downtime, ineffective systems and security risks.

This report will show you exactly where money is leaking out of your organization and being wasted on I.T. systems and software that are old, unnecessary and putting you at risk, and what to do about it now.

Provided By: IT4Eyes
Author: John Siggard
291 E 1400 S #8 St. George Ut.84790
www.it4eyes.com 435-313-8132

About The Author

John Siggard is the founder of Superior Technical Solutions (STS) and IT4Eyes, two Managed Service Provider (MSP) companies based in Washington, Utah. Since launching STS in 2009, he has specialized in cybersecurity, network analysis, security risk assessments, and IT support. With over 25 years of IT experience, John has built a team renowned for its exceptional service, earning STS the 2024 Soteria Award as one of North America's most trusted MSPs. He is also the co-author of Cybersecurity: The Silent Battlefield, a #1 best-selling book on Amazon, further establishing his expertise in the industry.

John's passion for technology began early when he secretly upgraded the family computer. His dad was supportive, introducing him to a friend with a computer business—laying the foundation for his future in IT. As a teenager, he worked unpaid for an IT professional and, at 17, was hired by Salt Lake City's Primary Children's Medical Center as a network engineer. There, he gained invaluable corporate IT experience and learned that in critical areas like the NICU, quick response times are vital.

In 2002, John took a two-year leave to serve in Mozambique, an experience that exposed him to global inequalities and deepened his appreciation for service. Despite limited technology, he found fulfillment helping locals maximize their resources, shaping his leadership and values.

Returning to IT, he became frustrated with slow industry response times. This led him to build STS around responsiveness, integrity, and communication. His team meets regularly to ensure client needs are met with comprehensive IT solutions. He is part of a top 100 MSP group that meets quarterly to discuss security concerns, IT trends, and proactive threat management.

John's special needs child has profoundly shaped his empathy and advocacy skills, strengthening both his personal and professional life. In his free time, he enjoys strategy games, mountain biking, and family time.

The I.T. Money Pit:
5 Ways Businesses Waste Money On I.T.

Even in the best of times, no business wants to have money secretly "leaking" out of their organization due to waste, poor management and a lack of planning.

But when it comes to I.T., most CEOs don't even know what they're spending money on, much less if they're making smart investments to minimize cost and waste. It's the proverbial "money pit," a "black hole" of cost that they are unable to accurately assess.

Like a malnourished obese person, they are consuming FAR more calories than necessary, but still not getting the micronutrients they need. Businesses are often in the same situation with I.T. – **they are spending thousands of dollars, but are still not getting the speed, performance, security and productivity they need.**

As Andy Grove, former CEO of Intel, said, "Only the paranoid survive." In our experience, most CEOs are **not paranoid enough when it comes to loss prevention and I.T. waste.** That's why we wrote this report.

My team and I have found thousands in dysfunctional I.T., SaaS bloat, unnecessary software, productivity-killing systems and underappreciated cyber risk – even in generally well-run companies led by respected executives.

In fact, there has yet to be a client we've helped in the 16 years we've been providing I.T. support and services that has not produced savings. Not one.

As you read this report, know that this IS very likely going on in your organization. As you go through this, know that what follows are only five of the most common areas where we see waste occurring. When we do a deeper analysis, we often find several other areas that need attention. Please take a look at everything below and know there IS a different path you can take – and one you should look into sooner rather than later.

#1: "Maverick" Spending, No Strategy And Undisciplined Planning

Many companies we've audited have a mishmash of patchwork technology pieced together like an old Frankenstein monster lumbering along. Nothing makes sense, nothing works as efficiently as it should, and the entire I.T. system is awash in inefficiencies, duplicate and redundant resources and outdated technologies – _all adding up to thousands of dollars wasted, unnecessarily, that could be put to better use in the business OR simply added to bottom-line profitability._

Do you have a veritable technology "junk drawer" full of equipment, wires and software that nobody can identify or explain and that does nothing but suck up space and precious resources?

In our audits of I.T. environments, we almost always uncover multiple servers, switches and other devices – all of which they are paying to support and back up – that could easily be consolidated and upgraded to deliver faster performance, more reliability and more security.

Over time, different cooks in the kitchen have added pieces and patched problems with Band-Aid after Band-Aid instead of strategically designing the whole to maximize productivity and lower the total cost of ownership by using more up-to-date (and lower-cost) cloud technologies.

In fact, most of the C-suite executives we've interviewed do not know what they even have and are paying for. I.T. is a giant black hole of spend that nobody can justify.

That's why the first step in understanding how to lower your overall I.T. costs and get a far better ROI is to conduct a deep audit of your entire environment to look for:

- Redundant machines, servers and devices.
- Duplicate SaaS applications your company is paying for (see "SaaS Bloat").
- Out-of-date software that's putting your organization at risk for a cyber-attack.
- Old servers that could be consolidated and moved to the cloud for greater speed and availability, easier access and team collaboration and productivity.
- Backup systems you're paying for that are unreliable and inconsistent.
- XXXXXX
- XXXXXXXX
- XXXXXXXXX

At Superior Technical Solutions, we prevent these problems through strategic planning meetings. We take the time to understand your business, how you use technology, and what you truly need to run efficiently.

For example, in one client assessment we discovered seven servers—but no one could at the practice could say what they did. After some research we found that Six were storing legacy data from obsolete systems the company no longer used, yet they'd been paying for them for years. We also found 13 unused computers still listed (and billed) under their service plan. By identifying what they actually needed and eliminating the excess, and showed them that they could redirect those wasted IT dollars into other areas that would grow the business.

#2: SaaS Bloat

In the era of cloud- and subscription-based everything, it's easy for small and midsize businesses to accumulate software-as-a-service (SaaS) subscriptions without a clear inventory or strategy.

Employees often purchase tools independently and outside of the I.T. budget (also known as "shadow I.T.") to get their job done. Because these subscriptions are in small amounts, and because most companies don't routinely audit these purchases, most companies are unnecessarily spending thousands of dollars in duplicate and unnecessary SaaS applications.

Here are some stats that speak to this point:

- A 2023 Productiv SaaS Trends report found that the average midsize company uses 254 SaaS apps, **yet only 45% of those licenses are actively used.**
- According to Gartner, organizations overspend on SaaS by at least 30% due to poor management of licenses and subscriptions.
- Flexera's 2023 State Of ITAM Report states that 49% of companies identify "identifying unused or underused software" as a top cost-optimization priority.

Let's say your business uses 100 SaaS apps at an average of $25/month per user, and only half are actively used. That's $1,250/month ($15,000/year) in waste for a 10-person team – and that's being conservative.

We also routinely find:

- Businesses are paying for full-feature enterprise plans when a basic tier would suffice.
- Companies fail to revoke and/or cancel licenses after employees leave or when the licenses are no longer needed.
- Employees have multiple software tools that do the same thing (e.g., three project management platforms, two virtual meeting and communication tools, multiple CRM systems, etc.).
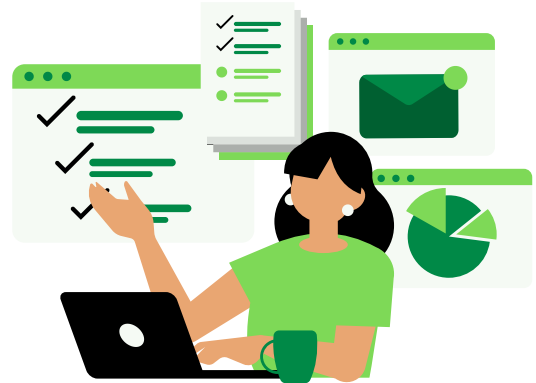
Left unchecked, SaaS bloat silently drains your I.T. budget and wastes money that could be going directly to your bottom line. Trimming even 10% to 20% of this waste can free up thousands for higher-payoff investments.

We typically help our clients save money just in consolidation of their SaaS applications while giving them visibility into what's being spent.

#3: Grossly Inadequate Data Compliance And Cybersecurity Protections

While you might not think of spending money on cybersecurity as a "cost savings," you would do a complete 180 if you ever experienced the massive expenses associated with a ransomware attack or breach.

When A Cyber-Attack Happens, The Losses Stack Up And Multiply While Sales Tank.

Right away, there's an instant loss of productivity. At best, you're crippled. In the worse cases, you're completely shut down, unable to transact, unable to deliver the promised products and services to clients and unable to operate. In other cases, thousands if not millions of dollars are drained directly from your accounts without any chance of recovery.

Then you have the loss of critical data, reputational damage, potential lawsuits and government fines. **The epicenter of this disaster lands DIRECTLY on YOUR desk for YOU to deal with** – a problem that WILL significantly undo your best-laid plans for growth and progress.

Yet, despite this, we have found that 92% companies we've audited are GROSSLY unprepared and unprotected from a ransomware attack or other major cybersecurity event EVEN THOUGH they have invested heavily in I.T. staff and resources. Before we showed them irrefutable evidence of these inadequacies, the CEO was convinced that "I.T. has it handled." A ticking time bomb they didn't know was "live" under their seat.

Let me also point out that many insurance companies now require you to have a robust cybersecurity plan and protocols in place in order for you to be insurable. And with new data-protection laws being introduced and implemented on both a federal and state level, you may have clients coming to you to demand you show proof of adequate cyberprotections or they will be unable to do business with you. Do you really want to wait until you have the proverbial "gun to the head" need to get this enacted?

At Superior Technical Solutions, we have an entire team dedicated to solving this for our clients so they have complete peace of mind that they are truly protected and compliant. For example, we recently worked with a rapidly growing medical practice. HIPAA compliance was always "on the list," but as they expanded to three locations and 40 employees so quickly, IT was overlooked. They were unknowingly operating with zero real cybersecurity measures in place—a disaster waiting to happen.

We moved quickly to design and implement a comprehensive compliance and security plan, giving them peace of mind that patient data was protected, regulatory requirements were met, and their business reputation was safeguarded. In their industry, trust is everything—one breach could have halted their growth overnight, cost millions in fines, and potentially put them out of business.

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

As the saying goes, "Overhead walks on two legs." Any leader knows that unproductive, distracted workers not only kill profitability but increase the chances of mistakes, missed deadlines, sloppy work and low morale. A frustrated team is not a productive one.

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 our audit, many CEOs are shocked to discover their employees are dealing with chronic I.T. problems that are constantly getting in the way of serving clients, closing sales and doing their job, forcing them to stop what they are doing, redoing the work they just spent hours doing or possibly NOT doing what they are supposed to do.

And it all adds up. Just one lost hour per employee per day—multiplied across an entire workforce—can cost a company hundreds of hours (and tens of thousands of dollars) each year. In one audit, we discovered one business's employees were spending hours every day trying to fix their own IT problems because their provider's response times were painfully slow. Worse, even when tickets were answered, issues weren't fully resolved, and poor communication meant more delays. The office administrator, for example, was burning a significant portion of her week chasing down tech fixes instead of doing her actual job.
This constant firefighting was costing them in two ways:

- Lost productivity – hours of valuable work time wasted.
- Inflated support costs – paying their IT company to handle endless tickets that should have been prevented in the first place.

In fact, we've found that employees spend an average of up to 3 hours per month dealing directly with tech support issues—a staggering waste when you factor in the hidden costs of missed opportunities and reduced output.

After we stepped in, that same client saw immediate improvement: problems were resolved quickly and correctly, communication was clear, and employees could get back to work without long interruptions. The result? More productivity, higher morale, and far better profitability.

In the majority of the situations where this is happening, I.T. is being outsourced to an organization that is not as responsive as they should be and has not been strategic or proactive in upgrading systems to avoid these costs.

To make matters worse, many support tickets are submitted by employees into a "black hole" without a guarantee of resolution or response time – so they're left waiting for HOURS, unable to work, simply because their outsourced I.T. company is not getting back to them quickly.

Problems occur again and again, and frustrated employees end up finding a work-around or attempt to fix it themselves because it's less frustrating than sitting on their hands waiting for a tech to call them back and fix the problem.

All the while, the company is paying their outsourced I.T. company to resolve all of this – but they're only compounding the problem.

> At Superior Technical Solutions, our average response time to problems is 10 mins or less.

#5: Delaying Necessary Upgrades Until Systems Fail

With inflation and costs on the rise, it's no surprise CEOs and CFOs try to stretch I.T. systems upgrades until they are absolutely necessary – but there is a false economy in waiting too long.

Older systems don't just slow down productivity; they require more maintenance, more support, and higher service fees. When they fail—often without warning—you can find yourself scrambling with:

- Emergency support costs
- Data recovery fees
- Unplanned downtime
- Expensive specialists needed to migrate legacy systems
- Lost productivity for your entire team
- Higher risk of cyberattacks due to outdated, unsupported technology

We've seen firsthand how devastating this can be. One client had an aging server that hosted all of their business data, running a custom legacy program that was absolutely critical to their daily operations. The problem? Only one person(not even an employee) knew how to use it.

The company didn't know how outdated and fragile this system was—and their IT provider had never taken the time to do an assessment of all their systems. When that one key person unexpectedly passed away, they were suddenly left with no one who understood how to operate the system. The business ground to a halt.

They came to us in crisis. We had to locate a rare specialist who understood the coding, forensically extract the data, and rebuild the application in a modern, accessible format for the entire team. The result? They lost a month of productivity, spent over $100,000, and endured weeks of stress and frustration.

Here's the kicker—if they had upgraded proactively, the cost would have been around $1,000 and could have been handled in a planned, low-disruption way.

When done right, upgrades can be budgeted and scheduled in manageable phases, minimizing downtime and spreading costs over time.

At Superior Technical Solutions, we prevent situations like this by tracking and documenting every piece of equipment, software, and system you own. This gives you clear visibility into what you have, when it needs to be replaced, and how to budget for it—so you're never blindsided by an avoidable disaster.

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 on how many support tickets your team is submitting?** Is it under <<X>> per month per employee? If it's higher than that, what are they proposing to eliminate recurring problems your employees are constantly having to deal with?

☐ 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.

Note: The above is merely a starter list of ideas. You MUST review and modify to fit your situation, clients and professional advice. Do NOT use "as is" without consideration.

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 **435-313-8132** 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:

www.stsutah.com

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:

Before we had IT4Eyes doing our IT we were attempting to do it ourselves between the dr.s and staff but, we got to the point with the amount of technology we have at our office that we needed some help. Since we have hired Them, life has been so much easier! Whenever we have an issue, they are very easy to get a hold of and then they handle the problem very promptly and efficiently so that we can get back to our jobs of serving our patients. We highly recommend.

-Dr. Eric Drake, Southwest Vision

We've been working with IT4Eyes for our IT needs, and I can't express enough how beneficial their services have been for us. The single biggest benefit has been their dedication to quick response times. IT issues can be critical, and knowing that they will be resolved promptly provides us with immense peace of mind.

What sets IT4Eyes apart is their exceptional service. Although I haven't worked with other IT firms before, I can confidently say that the personable and accessible nature of their team is outstanding. Their commitment to service is what truly makes them a cut above the rest. For anyone on the fence about choosing IT4Eyes as their IT firm, I would suggest comparing the services and benefits of all options. While it may seem expensive, the superior service and the peace of mind that comes with it are worth every penny. The level of support and the personal touch they offer are invaluable and always win in my book.

-Stone Canyon Eye Care