THE I.T. MONEY PIT

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

TECHSPERT
data services LLC

The I.T. Money Pit

5 Ways Businesses 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 enterprises in Northeast Ohio, 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: Techspert Data Services, LLC
Author: Adam Sieminenski
3046 Brecksville Rd Ste. E1 • Richfield OH 44286
https://techspert-data.com
Call us: (216) 800-7800

About The Author

Techspert Data Services was founded by Adam Siemienski, whose passion for computers and networking began in grade school during the early years of the personal computer era. After high school, when formal degree programs in computer networking were not available, Adam pursued a Bachelor of Science in Mechanical Engineering from the University of Akron, working multiple jobs to fund his education.

Adam began his professional career as a junior mechanical engineer at a steam-generating plant in Cleveland, where he frequently volunteered to assist with the company's data network. His commitment to technology led him to roles as a Microsoft Certified Trainer, a partner with a local construction accounting software developer, and a network engineer for the largest technology consulting company in Northeast Ohio at the time.

While managing the helpdesk for a 450-user health insurance company in Akron, Adam continued to support small business networks during evenings and weekends, building strong relationships with clients. Over the past 23 years, Techspert Data Services has grown to specialize in cybersecurity, disaster recovery, business continuity, Ai, and fully managed IT support for construction, manufacturing, and engineering companies ranging from10 to several hundred users.

Adam's approach has always been to minimize downtime, maintain productivity, and provide exceptional value. The team at Techspert is carefully selected for both technical skill and the ability to communicate clearly with business leaders about technology risks and how to mitigate them. This focus ensures that clients are protected against modern threats such as ransomware and are fully prepared to meet the requirements of today's cyber insurance standards.

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 millions of dollars 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 23 years we’ve been providing I.T. support and services that has not produced significant 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.

At Techspert Data Services, we prevent this problem by reviewing our clients' software subscriptions on a regular basis. We identify tools that are no longer being used, licenses that can be downgraded, and apps that duplicate the work of others. This not only saves money but also closes security gaps left open by unused accounts.

One client, a growing manufacturing company, came to us with more than one hundred different software tools in use. Many had been signed up for by individual employees over time. After we completed our review, we cut the list to less than half, adjusted plans to better fit their needs, and closed out unused accounts. This saved them more than $26,000 a year and gave them a clear picture of exactly what they were paying for.

#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.

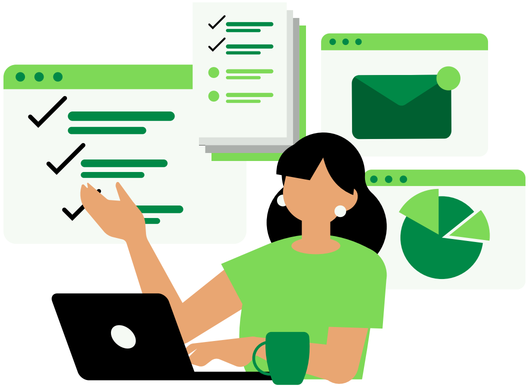
Employees often purchase tools independently and outside of the I.T. budget (also known as "shadow I.T.") to get their job done. Because these subscriptions are in small amounts, and because most companies don't routinely audit these purchases, most companies are unnecessarily spending thousands of dollars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

Part of our service for clients is to conduct a quarterly audit of all SaaS subscriptions so they can be reviewed to determine if they are still needed or can be consolidated, downgraded or simply eliminated, which saves thousands of dollars and closes another door a hacker can crawl though to gain access to your network.

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

In fact, one client, a regional distribution company, came to us with more than one hundred software tools in use, many of them purchased over time by individual employees. During our review, we found they were paying for three different project management tools, two video conferencing platforms, and multiple CRM systems. We worked with their team to select the best option in each category, moved all users to those platforms, and cancelled the rest. The changes saved them over $26,000 a year and made day-to-day operations far simpler for their staff.

#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 9-10 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?

For example, one of our clients in the manufacturing industry thought their existing security setup was strong. During our assessment, we uncovered outdated firewall settings, missing patches on key servers, and unsecured cloud file-sharing links. Within 30 days, we implemented a complete security refresh, closed all known vulnerabilities, and trained their employees on safe practices. Six months later, they narrowly avoided a phishing-based ransomware attack that could have shut down production for weeks.

#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.

Just one hour of this a day adds up when multiplied over an entire year and your entire workforce. As an example, one client we audited discovered each employee was wasting an average of 3 hours per month dealing with tech support issues – a STAGGERING amount of time wasted, not only in lower productivity, but also in the help-desk costs they were paying their I.T. company to handle all the support tickets being submitted. A DOUBLE WHAMMY of needless costs and profits going down the drain.

After coming onboard, we got that down to 30 minutes per month – one tenth of the time.

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.

One client, a professional services firm, was averaging over 40 hours a month in lost productivity due to recurring tech issues. After taking over their IT support, we reduced that to fewer than 5 hours a month by upgrading outdated systems, fixing long-standing network bottlenecks, and putting in a faster help desk process. This not only improved morale but also freed their staff to focus on clients instead of troubleshooting their own computers.

#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 not only become slower and less effective, but they also require more maintenance and support, increasing service fees. Old systems can also fail without notice, forcing you to upgrade without proper planning, incurring emergency support costs, data recovery fees and unplanned downtime.

In many cases, data loss can occur if systems fail unexpectedly – and upgrading old legacy systems may require expensive specialists who can migrate the data and functions to a newer system. Then there's the increased risk of a cyber-attack since older systems tend to be less secure and may no longer be supported by the vendor.

One client, a logistics company, had been putting off replacing their aging file server. When it finally failed, they spent three times the cost of a planned upgrade on emergency recovery and rush installation. Since then, with our tracking system in place, they have been able to schedule every major upgrade well in advance and have not experienced an unplanned outage in over four years.

Done right, upgrades could have been done in smaller, budgeted increments over time, making it easier on the company from a budgetary perspective and in disruption of productivity.

This is why, at Techspert Data Services, we track and document all the equipment, software, and systems a business owns. We give clients a clear, easy-to-understand report that shows what needs upgrading, when it should be done, and what the budget will be. That way, nothing comes as a surprise, and upgrades can be planned in smaller, manageable steps.

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 5 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?

□ **Do you know if your IT support is outsourced to a third party?** Many firms outsource to specialists, but it's critical to know exactly who has access to your systems and sensitive project or client data. If outsourced, have they clearly shown you the security protocols that prevent unauthorized remote access, especially from technicians outside your region?

□ **Are strong password policies enforced across all employees and contractors?** In industries with multiple on-site workers and contractors, weak password habits are a common vulnerability. Is there a mandatory password management system in place? When staff or contractors leave the project, is there a verified process to change all access credentials immediately?

□ **Is there ongoing training to ensure your teams are efficiently using existing software and systems?** Avoid costly duplication of software licenses or tools by empowering your staff to fully utilize current platforms—especially project management and CAD software critical to your workflows.

□ **Has your IT provider recommended or performed a comprehensive IT risk assessment every year?** Regulatory bodies and safety standards increasingly require documented risk assessments. Your IT partner should proactively identify vulnerabilities unique to your operations, from on-site device security to cloud data protection.

□ **Do they employ web-filtering technologies to block access to risky or non-work-related sites?** On construction sites and factory floors, preventing malware infections through unsafe browsing protects both onsite equipment and back-office systems.

□ **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?**

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 216-800-7800 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://techspert-data.com/cyber-security-assessment/

If you prefer, you can also e-mail me at ajsiemienski@techspert-data.com or call me direct at : 330-441-4426 x104

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:

“Trustworthy Experts Who Care”

I’m confident that Techspert is continually pro-active against threat actors. We have yearly discussions at minimum to provide updates and upgrades to our system to keep our company as safe as possible. We have trusted, and have worked with Techspert so long, there is not much of a comparison to make. Their response time is almost always immediate, and there is always someone on their team to help solve our problems. I would gladly share their expertise with anyone. I have recommended Techspert to others and will continue to do so.

-Ben Yost, Yost Food- Brunswick, OH

“They Talk With Me, Not Over Me”

Worrying about data breaches and ransomware are a thing of the past as I think our network is adequately locked down. Many emailed links do not work because our Cybersecurity defenses see it as potentially malicious but I have yet to run in to an issue where one of you was not on top of the problem almost immediately! When choosing a Technology Services company, I would say that the top 2 criteria are knowledge and customer service. Knowing how to talk with people makes rough situations much easier to handle, especially when it comes to a client that is losing their mind over what they feel is or could be a major dilemma. All your staff that I have dealt with directly have been very professional but at the same time brought themselves to my level or the level of the person they are currently assisting at our department to make the conversation comfortable and easy to understand.

-Michael Day, Gates Mills Police Department -Gates Mills

“Invaluable Asset to Our Business”

With Techspert’s expertise and experience, we feel very secure. Techspert is the only IT firm I’ve worked with and I don’t care to ever find out about any others. I’d recommend Techspert to anyone I know. It’s invaluable to be able to go to an IT firm with problems big or small and have them fixed as quickly as possible.

-Jonathan Collins, Diamond Steel Construction Co. - North Lima