The IT Money Pit

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

After conducting hundreds of IT assessments for small to midsize enterprises in Central Florida, we've uncovered 5 areas where companies routinely spend hundreds of thousands of dollars on IT 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 IT systems and software that are old, unnecessary and putting you at risk, and what to do about it now.

Provided By: CMIT Solutions of Central Orlando
Author: Mike Sabitov
390 N Orange Ave Orlando, FL 32801
www.cmito.com | 407-768-1001 | sales@cmito.com

Notice: This publication is intended to provide accurate and authoritative information in regard to the subject matter covered. However, no warranties are made. It is provided with the understanding that the author and the publisher are NOT engaged in rendering legal, accounting or related professional services or advice and that this publication contains opinions of its author. This publication is NOT intended as a substitute for specific legal or accounting advice for any particular institution or individual. The publisher accepts NO responsibility or liability for any individual's decisions or actions made as a result of information or opinion contained herein.

The IT Money Pit:
5 Ways Businesses Waste Money In IT

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 IT, **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 IT – **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 IT waste**. That's why we wrote this report.

My team and I have found millions of dollars in dysfunctional IT, 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 X years we've been providing IT support and services that has not produced at least $100,000 in fast 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 IT 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 IT 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. IT is a giant black hole of spend that nobody can justify.

That's why the first step in understanding how to lower your overall IT 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 cyberattack.
- 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.

#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 IT budget (also known as "shadow IT") 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 IT 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 $500 to $5,000 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 cyberattack 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 1 out of 3 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 IT staff and resources. Before we showed them *irrefutable* evidence of these inadequacies, the CEO was convinced that "IT 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?

#4: Chronic IT 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 IT failures because it's "hidden" from them.

After our audit, many CEOs are shocked to discover their employees are dealing with chronic IT 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 IT 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, IT 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 IT 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 IT company to resolve all of this – but they're only compounding the problem.

#5: Delaying Necessary Upgrades Until Systems Fail

With inflation and costs on the rise, it's no surprise CEOs and CFOs try to stretch IT 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 cyberattack since older systems tend to be less secure and may no longer be supported by the vendor.

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.

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

Take This Quiz To Find Out

If your current IT 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 IT spend and map out future upgrades so you can appropriately budget for IT 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 cyberattacks?** 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 10 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 cyberattack?

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

- ☐ **<u>Have you been fully and frankly briefed on what to do IF you get compromised</u>?** 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 IT 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 IT company should be handling the IT 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 IT 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 IT 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 IT spend, eliminate waste and reduce your exposure and risk to a devastating cyberattack.

The next step is simple: Call my office at **407-768-1001** 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) **IT Systems And Security Assessment**.

This Assessment can be conducted with or without your current IT 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 IT services, tools and support you are paying your current IT 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:* The majority are NOT.)
- How you could lower the overall costs of IT 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 IT systems.

Sign Up For Your FREE Assessment At Our Website:

www.cmito.com/discoverycall

If you prefer, you can also e-mail me at msabitov@cmito.com or call me direct at 407-608-5705.

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 cyberattack, every minute counts.