



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**



Perform. Protect. Prosper.

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 Virginia, 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: BEL Network Integration & Support

Author: Larry Martin, CEO

3601 W. Hundred Rd., Suite 12

Chester, VA 23831

(804) 796-2631

www.belnis.com



About The Author



Larry Martin is the CEO of BEL Network Integration & Support, a Central Virginia-based I.T. services firm trusted for its reliability, responsiveness, and straight-talk approach to technology. Larry has spent his career helping business owners get control over their I.T. not just by fixing what's broken, but by preventing problems before they start.

What sets Larry and BELNIS apart is a deep understanding of how to support businesses operating in highly regulated, high-pressure environments. Whether it's navigating HIPAA, FINRA, or the cybersecurity threats that keep business leaders up at night, Larry's team is built to deliver peace of mind through proactive service, clear communication, and solutions that actually work.

Before founding BELNIS, Larry spent nearly two decades leading business and technology teams for Fortune 500 companies like Altria, McKesson, and Indivior, where he was entrusted with safeguarding key information assets under the strictest regulatory compliance and budgetary constraints. His real-world experience in business continuity, risk management, and enterprise-scale operations is what gives BELNIS its edge today.

Larry and his wife, Kim, live in Midlothian. Outside the office, he's on the golf course, tennis court, or guitar in hand — always learning, always moving forward.

Clients don't trust BELNIS because they promise perfection... they trust them because they show up, own the problem, and get it done right. This guide is just one more way Larry aims to empower business leaders with the clarity and confidence to make safer, smarter technology decisions

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 under appreciated 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 35+ years we've been providing I.T. support and services that has not produced immediate 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 BELNIS, we avoid this by taking a proactive, structured approach to IT audits and system optimization. We begin every client relationship with a deep dive into your current environment... identifying outdated hardware, duplicate tools, underutilized software, and wasteful licensing. Then we streamline, secure, and simplify.

Take Virginia Controls, for example: they came to us juggling internal IT needs with limited bandwidth. Their network had become a tangle of overlapping tools, legacy gear, and inefficient workflows. We stepped in, conducted a full systems and risk assessment, and **built a leaner IT framework that eliminated waste... all without the cost of hiring additional in-house support. That's not just IT management. That's strategic enablement.**

#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.

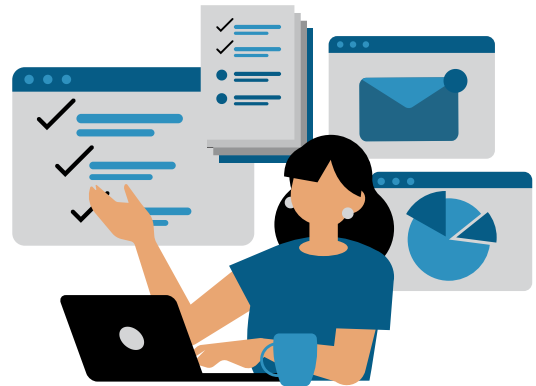
Here are some stats that speak to this point:

- 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.

In fact, one client was unknowingly paying for multiple unused SaaS tools across departments. During our standard IT assessment, we identified several redundant apps and inactive licenses—**cutting thousands in wasted spend almost immediately.** Streamlining these tools not only saved money, but also simplified their team’s workflow and reduced support tickets.



#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 69% of 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 BELNIS, we have an entire team dedicated to solving this for our clients so they have complete **peace of mind** that they are truly protected. In one engagement, **our audit revealed major gaps in endpoint protection and inconsistent backups**, despite the company believing they were fully secure.

We implemented a layered cybersecurity framework, tightened compliance protocols, and helped them meet their cyber insurance requirements. The result? **A fully documented, insurable, and resilient environment that keeps leadership focused on growth... not firefighting breaches.**

#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.**

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 BEL Network Integration & Support we **guarantee** a business hours **response within 12 minutes.** Our current response rate is **less than 3 minutes.**

#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.

In one case, a client delayed replacing an aging server that was out of warranty and hadn't been backed up properly. When it failed unexpectedly, it **resulted in three full days of downtime, emergency data recovery costs, rush hardware replacement, and lost productivity... totaling over \$18,000.** The kicker? The planned upgrade would have cost just \$6,500 and could have been done with zero disruption.

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 BEL Networks Integration & Support, we track and document all of the equipment, software and systems your business owns, giving you visibility into what's actually going on, what truly needs to be upgraded and when, giving you a more control over your budget.

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 current IT spend and plan upcoming upgrades**, so there are no unwelcome surprises or emergency invoices?
- ☐ Have they **reviewed ransomware and cyber-attack protection in the past 3 months**, as part of that same meeting—letting you know exactly what threats you face today?
- ☐ **Do they track and report on how many support tickets your team is submitting?** Is it under 4 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 **looked at software inefficiencies** in your organization and proposed a plan to eliminate unused tools that are costing money?
- ☐ **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 email system to prevent accidental leakage of confidential or protected information?**
- ☐ Have they discussed or offered **dark web / deep web ID monitoring services**, so you're alerted immediately if your credentials show up on illicit cybercrime sites?

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 **804-796-2631** 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.belnis.com/discoverycall

If you prefer, e-mail me at Larry@belnis.com or call me direct at 804-796-2631

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:

Responsive, Reliable, and Keeps Us Focused on Growing Our Business



"Since partnering with BELNIS, we've experienced consistent technical support and **seamless new employee onboarding**. Their quick responsiveness to tickets and escalations set them apart from other IT firms we've worked with. BELNIS takes our growth seriously, consistently seeking feedback and **conducting quarterly business reviews to ensure their services align with our goals**. If you're on the fence about choosing BELNIS, let me reassure you... they will not let you down. Their proactive approach and quarterly business reviews has improved our efficiency and supported us to grow our business."

Tony Goodman
Chief Operating Officer
Adial Pharmaceuticals

BELNIS has Given Us Confidence to Grow with Secure & Reliable IT Systems



"BELNIS has beefed up our IT operations by providing comprehensive expertise that boosts security and streamlines decision-making. Their responsiveness and **reliability, especially during time-sensitive issues**, set them apart from other firms. When it comes to IT, you get what you pay for, and BELNIS delivers the **quality and confidence we need to stay safe and compliant with sensitive data**."

Robbie Sutkay
Chief Executive Officer
Pharmacy Data Solutions

BELNIS Enables Our Team to Focus on Growing Our Business



"BELNIS provides us the capability to have the IT and Project skills needed to expand our business without adding multiple support staff - and it's done in an affordable way. Their staff provides a personal investment "from the top down" and they react with speed and flexibility to our changing needs. They also want to **focus on our future planning geared toward OUR needs, not theirs**. As we were searching for an IT Partner, many came promising, "we can do it all", BELNIS' approach was to listen to us, indicate what we needed & **tailor services** to those needs."

Mike Goodwin
IT Leader
Virginia Controls, LLC.