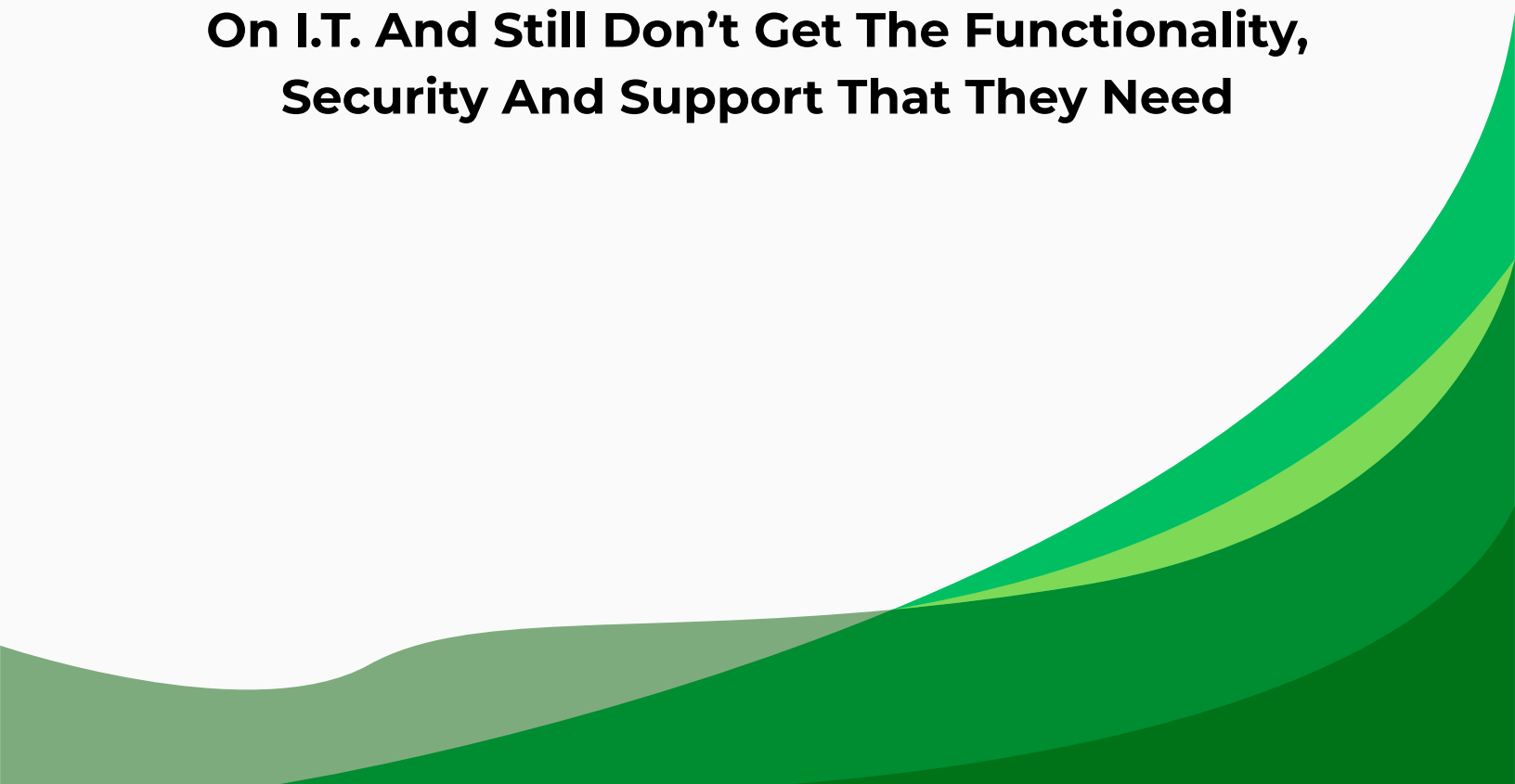




THE I.T. MONEY PIT

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





Securely Wired to the Cloud

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 Western-Ohio and Eastern-Indiana, 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: Tomorrow's Technology Today

Author: Lisa Niekamp-Urwin

www.TomTechToday.com

(419) 678-2083



About The Author



With over 25 years of technology and business experience, Lisa Niekamp-Urwin is President - CEO of Tomorrow's Technology Today in St. Henry Ohio. Founded in 2002, Tomorrow's Technology Today (TTechT) is a technology service provider in Northwest Ohio. Lisa attended the University of Dayton in Computer Science and then University of Findlay in Business Management. She also holds a Project Management Professional from the Project Management Institute, along with a Master's from George Washington University in Project Management. Lisa founded TTechT on the passion and love of technology and in the excitement to bring enterprise technology to the small and medium size businesses in the area.

Lisa has developed a unique cyber security service business which started in the grassroot of Ohio and has expanded to several states and for a couple international companies. Cyber security means layers of protection and implementing an enterprise level solutions that is industry standards without breaking the bank account. This includes EDR, MDR, cloud firewalls, backup with disaster recovery ability, real patch management, email with enterprise level protection services, data loss and information protection and most importantly employee education.

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 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 at least \$1,000 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 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:

- Systems and devices that may be overlapping or underutilized.
- Software subscriptions that aren’t delivering full value—or are duplicating functionality.
- Technology that may be outdated, unsupported, or posing unnecessary risk.
- Infrastructure that could be streamlined or modernized for better performance and collaboration.
- Backup and recovery solutions that may not be meeting today’s reliability standards.
- Connectivity and communication services that may be misaligned with current pricing.
- Collaboration tools and platforms that may be creating inefficiencies or confusion.
- Voice and communication systems that may be missing modern features or flexibility.

At Tomorrow's Technology Today, our managed service plans include an annual IT budget review and planning session to eliminate ad-hoc purchases and surprise costs. Together, we:

- ***Inventory and rationalize software, licenses, and services to cut duplicate and unused tools***
- ***Build a 12-month roadmap with timelines, costs, and owners so upgrades are planned—not rushed***
- ***Set standards to curb “shadow IT” and control spending***
- ***Plan hardware lifecycles to avoid emergency replacements and overtime bills***
- ***Prioritize cybersecurity and compliance investments where they matter most***

This turns IT from a random expense into a predictable, strategic investment.

#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.

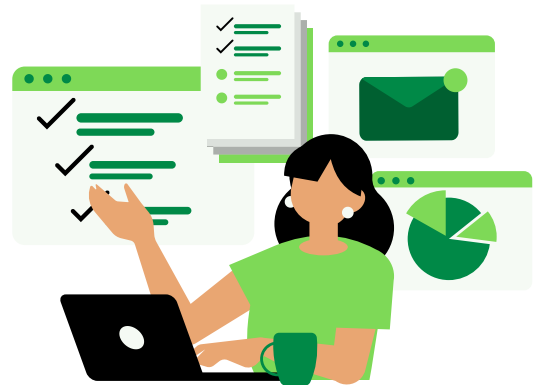
Employees often purchase tools independently and outside of the I.T. budget (also known as “shadow I.T.”) to get their job done. Because these subscriptions are in small amounts, and because most companies don't routinely audit these purchases, most companies are unnecessarily spending thousands of dollars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

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 an annual audit of all subscriptions and hardware 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 through 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 typically help our clients save \$100 to \$800 just in consolidation of their SaaS applications while giving them visibility into what's being spent.

Our managed service plans bake SaaS control into everyday operations. During Annual Planning and Quarterly Business Reviews, we map a 12-month application and license budget. Asset Management inventories every subscription, owner, and renewal date so nothing auto-renews unnoticed. Microsoft 365 administration and our password vault streamline provisioning, while clean offboarding cancels or reassigns seats. Permission Control Access curbs shadow IT and keeps your stack standardized. We consolidate overlapping tools, right-size license tiers, and document an approved app list. As your vendor liaison, we can help negotiate renewals and ensure you're on the most cost-effective plans. Technology alignment sessions verify security, backup, and compliance so data lives in approved systems. Result: fewer duplicate apps, reclaimed licenses, predictable renewals, and a defensible, well-managed IT budget.



#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 worst 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 95% of the 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 Tomorrow's Technology Today, we have an entire team dedicated to solving this for our clients so they have complete peace of mind that they are truly protected!

#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. We have discovered **employees can waste 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 that companies are paying their I.T. company by the minute to handle all the support tickets being submitted. A DOUBLE WHAMMY of needless costs and profits going down the drain.

Working with Tomorrow's Technology Today, we get this down to **30 minutes per month** – one tenth of the time it would normally take.

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 Tomorrow’s Technology Today, we attack chronic I.T. issues by measuring what matters and fixing root causes—not just closing tickets. Every request is logged in our ticketing system, prioritized by business impact, and worked to defined SLOs, with extended Helpdesk hours (7 a.m.–5 p.m.) and an after-hours emergency path. We report trends and metrics to your leadership, because metrics that are measured and reviewed improve—fast. Monthly Technology Alignment checks and Quarterly Business Reviews drive proactive maintenance, patching, and lifecycle planning so systems don’t fail at the worst time. Clean onboarding/offboarding, M365 administration, and permission controls prevent the misconfigurations that cause repeat outages. Post-ticket surveys trigger follow-ups on anything less than excellent. The outcome: fewer recurring issues, faster resolutions, and a predictable support experience your team can rely on.

#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.

Delaying Necessary Upgrades Until Systems Fail: a real-world lesson
We strongly advocate planning and budgeting for upgrades because the alternative is costly and disruptive. One former client declined our documented recommendation to replace an out-of-warranty, custom-built server with failing, unmonitorable drives. After two disaster recoveries, the server failed again, triggering 37 hours of emergency troubleshooting. Most of that time was billable, per our SOW, because the failure stemmed from ignored recommendations and unsupported hardware—exactly the scenario proactive lifecycle planning is designed to prevent. Today, our clients understand why we track warranties, monitor health, and present hardware roadmaps in Annual Planning and Quarterly Business Reviews. When systems approach end-of-life, we schedule budgeted, phased replacements and validate backups and recovery targets. The result: predictable costs, far less downtime, and no “all-hands” emergencies. And when risk remains unacceptable, we will professionally disengage.

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 Tomorrow's Technology Today, 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 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 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 **2** 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.

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 **(419) 678-2083** 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.TomTechToday.com/Network-Security-Assessment

If you prefer, you can also e-mail us at sales@ttecht.com or call (419) 678-2083.

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:



"Always makes us feel like a priority."

Whether it's a major issue or a minor question, their team always makes us feel like a priority—and never makes us feel foolish for asking. What really stands out is their organization, attention to detail, and professionalism. Everyone we've interacted with has been great, and the quick response time is something we truly appreciate. If you're considering an IT partner, I'd encourage you to reach out and see what TTechT can do for your business.

- **George E. Moore Law Office, Celina, OH**

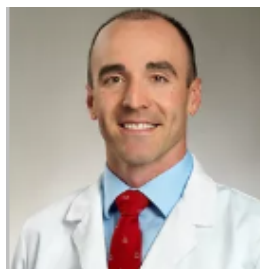


"We work on insurance, TTechT works on IT"

Our remote IT guy retired, making us search for a local IT company. We chose Tomorrow's Technology Today. The single biggest benefit our company experienced is the ability to concentrate on selling and serving insurance rather than dealing with our technology and computer issues.

Tomorrow's Technology Today provides more knowledge than other IT firms, which allows us to use our computers most efficiently. We are extremely satisfied with their service, knowledge, and responsiveness. Give them a call.

- **Block Insurance Agency, Waynesfield & Wapakoneta, OH**



"Peace of mind with TTT"

We are always appreciative of the fast response times from Tomorrow's Technology Today. Our business relies heavily on our computers functioning efficiently so when an issue arises it's nice to know it will be addressed promptly!

Recently we went through a major software update, which included every computer in the office. TTT was great about working with us to get this all done while we were out of the office to be sure the office flow was not interrupted. And on top of that, they were readily available the next business day to be sure everything worked as it should! There is always peace of mind knowing that all of our IT services are handled by a local business who understands the area we live and work.

- **St. Henry Dental, St. Henry, OH**