

CYBERSECURITY BLIND SPOTS:

THE RISKS YOU DON'T SEE BUT HACKERS DO

Every business leader understands the importance of cybersecurity. Yet the biggest threats often aren't headline-grabbing breaches. They're the overlooked gaps hiding in plain sight. These blind spots may seem minor: a missed software update, an inactive account or an untested backup. But for hackers, they're open doors. Here are the most common gaps and how to close them before they become costly mistakes:

1. Unpatched systems

Every missed update is an invitation to attackers. Hackers track patch cycles and exploit known vulnerabilities.

Fix: Automate patch management and set alerts for lagging systems.

2. Shadow IT and rogue devices

Employees downloading unauthorized apps or connecting personal devices to your network can introduce malware that stays dormant until it's too late.

Fix: Enforce strict app and device policies. Regularly scan for unknown endpoints.

3. Over-permissive access

Too much access is dangerous. Hackers love accounts with excessive permissions.

Fix: Apply least privilege principles, mandate MFA and review permissions regularly.

4. Outdated security tools

Cyberthreats evolve daily. Old antivirus or intrusion detection tools can't keep up.

Fix: Audit your security stack and replace outdated tools before they fail you.

5. Orphaned accounts

Former employees' credentials often remain active, making them prime targets for attackers.

Fix: Automate offboarding to disable accounts immediately.

6. Misconfigured firewalls

A firewall is only as strong as its settings. Old or temporary rules create vulnerabilities.

Fix: Audit configurations, document changes and remove unnecessary permissions.

7. Untested backups

Backups aren't a safety net unless they work. Many businesses discover too late that theirs are corrupt or incomplete.



Fix: Test backups quarterly and store them securely in immutable storage.

8. Missing security monitoring

You can't protect what you can't see. Without centralized visibility, threats slip through unnoticed.

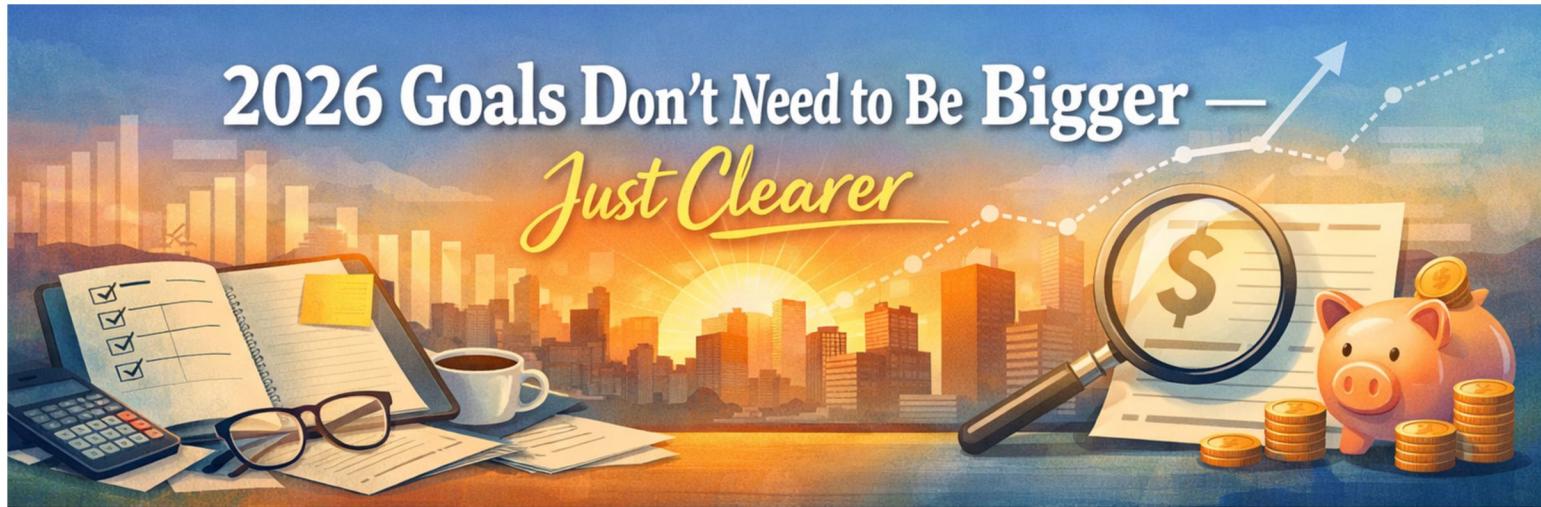
Fix: Invest in continuous monitoring or partner with an experienced IT provider.

9. Compliance gaps

Frameworks like GDPR or HIPAA aren't just paperwork. They're essential for strong security.

Fix: Conduct regular compliance reviews and maintain documentation.

Bottom line: Identifying blind spots is only the beginning. The real value lies in fixing them quickly. Start with these fixes and you'll strengthen your defenses where it matters most.



Every year around this time, the same thing happens. We start talking about goals. Growth. Efficiency. "Doing more with less." And then, somewhere around Q2, reality kicks in, usually in the form of expenses nobody saw coming.

A renewal hits a credit card.

A subscription everyone forgot about quietly auto-renews.

Something shows up on a statement and no one's quite sure who approved it.

Here's the thought we keep coming back to as we look ahead to 2026: It's hard to set good goals if you don't actually know where your money is going. Not in a spreadsheet-from-last-year kind of way. In a real, current, "what are we paying for right now?" way.

Most businesses don't overspend because of one bad decision. They overspend because of lots of small, reasonable decisions made over time.

- A tool added during a busy stretch
- Software that seemed inexpensive at the time
- Licenses still active for people who left
- Renewals that happen before anyone remembers they exist

None of these are huge on their own. But together, they create noise, and noise makes planning harder than it needs to be.

Visualize and Optimize Costs
Manage, track, and access all your IT contracts in one place. Never miss a renewal or key update again.

A Different Way to Think About "Cutting Costs"

When people hear "cutting costs," it usually sounds negative. Like something you do when things are going wrong. But that's not really what this is about. For 2026, the goal doesn't have to be cutting. It can just be clarity.

When you know what you're paying for, when it renews, and whether it's still being used, decisions get easier. There's less scrambling and fewer surprises. Planning feels calmer. Most business owners we talk to aren't trying to squeeze every dollar. They just want to feel like they're in control.

Why This Matters More Than It Seems. Uncertainty is tiring. Even small, unexpected expenses add mental load, and that mental load leaks into everything else: budgeting, hiring, investing, and long-term planning.

When expenses are visible and organized, that pressure eases up. Goals feel more realistic. Conversations are simpler. You spend less time reacting and more time deciding.

Something We're Offering as We Head Into 2026

As we head into the new year, we're opening up something new to a small group of clients. We're offering our expense-tracking service free to the first five clients who want to use it. No catch, just a way to help a few businesses start 2026 with clearer visibility and fewer surprises.

After that, the service will be available throughout 2026 for \$59 per month. No pressure. No rush. If it sounds helpful, let us know. And if not, we hope this way of thinking helps you approach your 2026 goals with a little more clarity and a little less noise.

Sign up: [TIGERHAWKTECH.COM/BETTER-TRACKER](https://tigerhawktech.com/better-tracker)

TECH TRENDS

YOUR BUSINESS SHOULD ACTUALLY PAY ATTENTION TO



Every year, tech publications release bold predictions about revolutionary trends that will “change everything.” Before long, you’re buried in buzzwords such as AI, blockchain and the metaverse, with little clarity on what truly drives revenue growth.

Here’s the truth: Most tech trends are hype designed to sell expensive consulting services, but buried in the noise are a few genuine shifts that will impact how you work. Let’s focus on what really matters. Here are three trends worth your attention and two you can safely ignore.

Trends worth your attention

1. AI built into tools you already use

AI is no longer a separate tool you have to learn. It’s being embedded directly into the software you already use every day. Your email program will draft responses. Your CRM will write follow-up messages. Your accounting software will automatically categorize expenses and flag any anomalies.

Why it matters: You’re not learning new tools; you’re just getting smarter versions of what you already use. Instead of asking “Should we adopt AI?” the question becomes “Should we turn on these features we’re already paying for?”

What to do: When your software offers AI features, try them for two weeks before deciding if they help. Many will be gimmicky, but some will save hours.

Time investment: Minimal. You’re already using these tools.

2. Automation without the headache

Building custom automations used to require hiring a developer or learning complex software. Now, new tools let you create workflows just by describing what you want in plain English.

Example: “When someone fills out my contact form, add them to my spreadsheet, send a welcome email and remind me to follow up in three days.” The AI figures out how to make it happen.

Why it matters: Automation moves from “We should do this but don’t have time” to “We can set this up in 20 minutes.”

What to do: Identify one repetitive task your team does weekly. Describe it to an automation tool and see if AI can build it for you.

Time investment: 20 to 30 minutes to set up your first automation.

3. Security regulations get real

Cybersecurity is shifting from best practice to legal requirement. States are passing data privacy laws. Insurance companies are requiring specific security measures. Enforcement is getting serious.

Why it matters: Not having basic protections

is becoming like not having business insurance. It’s a liability you can’t afford.

What to do: Cover three basics: multi-factor authentication on all accounts, regular data backups you can restore and written cybersecurity policies you follow.

Time investment: Two to three hours to set up properly.

Trends you can safely ignore

1. The metaverse for business

Virtual reality meetings have been “the next big thing” for a decade. Headsets are still expensive and uncomfortable. Unless you’re in architecture or design, skip it.

What to do: Nothing. If VR becomes useful for mainstream business, you’ll know because competitors will use it successfully.

2. Accepting crypto payments

Crypto sounds cutting edge, but it adds tax complexity, volatility and higher fees. Unless customers actively request it, stick to cards and ACH transfers.

What to do: If someone asks, politely say no. Reconsider only if multiple customers request it organically.

Focus on trends that save time, reduce risk and improve efficiency. Ignore the hype and invest where it truly benefits your business.

THE HIDDEN COST OF IGNORING TECH HEALTH

Your business runs on technology, but when was the last time you checked its health?

IT maintenance often gets ignored until something breaks. The reality is that neglecting your tech environment doesn't just invite risk. It can quietly drain resources, reduce efficiency and erode trust over time. Regular IT health checks are as important as financial audits or employee reviews. They ensure your systems perform at their best and help you stay ready for the unexpected.

The high price of inaction

Neglecting the health of your technology ecosystem isn't a small oversight; it's a risk multiplier. When systems are left unchecked, small technical issues can grow into major disruptions. The longer these problems go unnoticed, the more expensive and complex they become to fix. Here are some of the hidden costs your organization could face when IT issues go unaddressed:

Financial costs

Downtime and lost revenue: Unidentified vulnerabilities or outdated infrastructure can lead to system outages, costing thousands per hour in lost productivity and sales. For businesses that rely on real-time transactions or customer-facing platforms, even a short outage can have a major impact. In competitive markets, downtime doesn't just halt work. It can also drive customers toward faster, more reliable competitors.



Ransomware and breach costs: Blind spots in your IT environment often become entry points for cyberattacks. The average cost of a data breach is now in the millions, and ransomware demands can cripple operations for days or even weeks. Beyond the immediate financial hit, there's the long-term cost of rebuilding systems, restoring data and regaining trust.

Compliance penalties: Missing controls, outdated policies or incomplete documentation can result in fines for noncompliance with HIPAA, GDPR or other regulations. These penalties can be severe and often come with a loss of credibility that affects partnerships and customer relationships.

Recovery and remediation expenses: Emergency fixes, forensic investigations and public relations damage control are far more expensive than proactive maintenance. A single breach can lead to legal fees, customer notifications, compensation claims and costly settlements. The more reactive your approach, the greater the long-term financial strain.

Security risks

Data loss or theft: Unsecured endpoints, outdated software or misconfigured access controls can expose sensitive data. Once data is compromised, recovery is difficult and customer confidence can take years to rebuild.

Unauthorized access: Orphaned accounts or unmonitored devices are often exploited by

SHINY NEW GADGET OF THE MONTH

OIKKEI AI Wireless Mouse

Meet the ultimate multitasker: a wireless mouse that doubles as an AI-powered audio recorder. Perfect for remote meetings, this device captures conversations accurately while you navigate your screen—no extra gadgets needed.

Streamline note-taking, improve collaboration and keep your workflow efficient. If you're looking for a simple way to save time and stay organized, this innovative tool is a game-changer for busy business leaders.



Tech of the Month Keep the votes coming



Natalie Thompson
IT Specialist

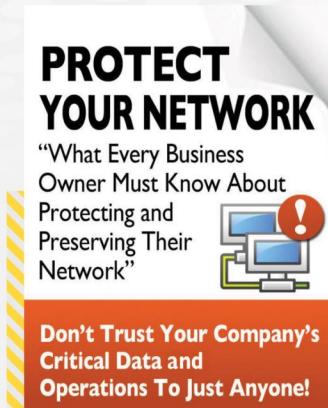
Natalie is Tech of the Month once again, and it is well deserved. She shows up every day ready to help, solve problems, and make life easier for both our clients and our team. We are incredibly proud of the work she does.

FREE REPORT

What Every Small-Business Owner Must Know About Protecting and Preserving Their Company's Critical Data and Computer Systems

This report will outline in plain, nontechnical language the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills. By the end of the report, you'll have an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at:
www.tigerhawktech.com/protect



CARTOON OF THE MONTH



"The look you get when you say, 'Let's circle back.'"

...continued from page 4

attackers or insider threats. These accounts can remain active for months before being discovered, creating an easy path for exploitation.

Malware propagation: A single unpatched system can become a launchpad for malware spreading across your network. One infected device can compromise your entire environment, interrupting operations and exposing confidential data across departments.

Operational and strategic impact

Reduced performance: Inefficient systems and outdated hardware slow down teams, create workflow bottlenecks and frustrate users. When technology becomes an obstacle rather than an enabler, productivity drops, morale suffers and business momentum stalls.

Missed opportunities: When you don't really know what's going on in your IT setup, planning ahead becomes a guessing game. Without accurate insights, it's difficult to forecast growth, plan digital transformation or

leverage new technologies effectively. Businesses that fail to modernize risk falling behind competitors that are faster, smarter and more agile.

Poor decision-making: When leadership operates without clear data about IT performance, decisions become reactive instead of strategic. This can lead to wasted investments, misaligned priorities and overlooked risks that could have been prevented with better visibility.

Reputational damage

Loss of client trust: A breach or prolonged outage can quickly erode years of goodwill. Clients expect reliability, privacy and accountability. Failing to deliver on those expectations can drive them to competitors who appear more secure and dependable.

Brand impact: Public incidents tied to IT failures can damage your brand's credibility and market position. Negative headlines and social media backlash can linger long after the issue is

resolved, overshadowing your successes and shaking customer confidence.

Ignoring your tech health doesn't just risk downtime. It weakens your entire foundation. Regular IT assessments help identify vulnerabilities before they escalate, optimize performance and ensure compliance. Think of it as preventive care for your business. A little attention today can protect your reputation, save money and keep your organization healthy in the long run.



HOW TIGERHAWK IS IMPROVING EMAIL PROTECTION IN 2026



Email is still where most business communication happens.

It's how invoices are sent, documents are shared, and sensitive information moves quickly between people who trust each other. That familiarity is also what makes email one of the most common places where compliance issues begin, especially for businesses subject to HIPAA or PCI requirements.

Most compliance problems don't come from bad intent. They come from everyday work.

A quick reply.

A document sent in a hurry.

Information shared without realizing it should have been protected.

That's why email, particularly outgoing email, deserves more attention than it usually gets.

A Quieter, More Complete Approach to Email Protection

As part of our 2026 improvements, Tigerhawk is implementing full Inky email protection for every Tigerhawk Complete customer.

This upgrade strengthens protection for emails coming into your inbox, and also adds automated safeguards for emails being sent out, including email encryption when sensitive information is detected.

The goal isn't to slow anyone down or add steps. It's to reduce the risk of accidental exposure while letting people work the way they already do.

What You'll Notice (and What You Won't)

One visible change is that the purple warning banner that appeared at the top of some emails will be gone. That's intentional. Those banners were designed to help, but over time, they added visual noise and were easy to ignore, especially when they appeared on legitimate messages.

Inky takes a more contextual approach. Legitimate emails look normal, and when something needs attention, the guidance is clear and written in plain language.

Less noise. Better awareness.



Why This Matters for Compliance

For businesses that need to meet HIPAA or PCI requirements, protecting sensitive information isn't optional — but it also shouldn't be disruptive.

By automatically identifying risky messages and encrypting outbound email when appropriate, this approach helps:

- Reduce the risk of accidental data exposure
- Support compliance responsibilities
- Take pressure off employees
- Minimize unpleasant surprises

All without changing how email works day to day.

What This Means for You

If you're a Tigerhawk Complete customer, this upgrade is being added automatically. There's nothing to install, manage, or learn.

Our goal is simple: reduce risk without adding friction.

And if you never think about this again, that's exactly how good protection should work.

