TIGERHAWK INSIDER

Insider Tips To Make Your Business Run Faster, Easier and More Profitably

MARCH 2026

WHEN AN IT RELATIONSHIP STARTS TO FEEL LIKE A BAD DATE

Most bad dates don't begin badly. They start with quick replies. Clear plans. A sense that someone is paying attention. You leave thinking things are handled.

Business technology relationships often begin the same way. At first, support is responsive. Systems are set up. Problems get fixed. There's relief in knowing someone is "on it."

Technology fades into the background where it belongs.

Then your business grows. More tools are added. Your team gets busier. Security concerns grow. What once felt simple now feels complicated.

The Honeymoon Phase Ends

Replies take longer. Issues that were supposedly resolved return. You hear phrases like "we'll look into it" more often than you'd like.

Before you know it, you're adapting your business to someone else's bad behavior.

You call. You leave a message. Maybe you send an email. Then you wait for hours. Sometimes days.

Meanwhile, your team is stuck. You're paying employees who can't do their jobs because IT "support" is missing in action.

That's not support. That's a bad date who says, "I'm on my way" and never shows up.

Healthy tech relationships don't leave you hanging. Problems get acknowledged, triaged and fixed fast. Better yet, many of them never happen because someone is watching your systems before they melt down.

Why Tech Relationships Go Bad

Most small-business tech relationships fail for the same reason most relationships fail: No one is maintaining the relationship.

Tech often runs on a reactive model: Something breaks, you call, they patch it, everyone ignores it again, repeat. That's like talking to your spouse only during fights.

You're technically communicating, but you're not building anything stable.

Meanwhile, your business keeps growing, so the IT relationship that worked with five people and one shared drive doesn't survive with 15 people with more data and more apps being targeted by smarter criminals.

What a Healthy Tech Relationship Feels Like

A good tech relationship isn't exciting. It doesn't create drama. It feels calm.

A good IT partner doesn't just fix problems. They prevent problems. They monitor, patch and maintain quietly in the background so issues don't sneak up on you during payroll, tax prep or your biggest client deadline of the quarter.

Here's the real sign you're in a good tech relationship: You stop thinking about IT most days because it just works. Not trendy. Not magical. Reliable.

The Big Question

If your IT provider was a person you were dating, would you keep seeing them? Or would your friends say, "Seriously? You're still calling that guy?"

If you've normalized bad tech behavior, you're paying twice: in dollars and in stress. And neither one is necessary.

Healthy tech relationships don't leave you hanging. Problems get acknowledged, triaged and fixed fast. Better yet, many of them never happen because someone is watching your systems before they melt down.

TIGERHAWK Technologies Est. 2005

Pressure Doesn't Create Weakness. It Reveals It.

Every March, teams enter the tournament believing they are ready. They have studied film, adjusted lineups, corrected mistakes, and refined their strategy over the course of the season. On paper, everything looks solid. Then the pressure rises. The lights are brighter, the margin for error narrows, and small mistakes suddenly carry real consequences. A single defensive lapse turns into a scoring run, and one careless turnover shifts the momentum of the entire game. Weaknesses that went unnoticed earlier in the season become impossible to ignore. The tournament does not create those weaknesses; it simply reveals what was already there.

Business operates the same way. Most days feel manageable, and operations move forward without much friction. Systems run, emails flow, and employees log in and complete their work without incident. There is rarely a sense of urgency strong enough to force a close examination of the foundation supporting everything behind the scenes. That is, until something changes.

A cyber incident exposes outdated security measures. An employee leaves and takes undocumented knowledge with them. A server fails and the backups have never been tested. Rapid growth stretches infrastructure that was never designed to scale. In those moments, pressure does not create the problem; it reveals the true strength or fragility of what has been built.

The Quiet Fundamentals That Actually Win

Championship teams do not depend on emotion, hype, or momentum when the stakes are high. They depend on fundamentals. They communicate clearly, understand their roles, and execute the same disciplined habits they have practiced all season. When pressure increases, they fall back on structure rather than improvisation. As longtime Duke coach Mike Krzyzewski often reminded his players, "Pressure is a privilege."

The moment feels heavy because it matters, and it only matters because preparation has brought you there.
In business, the same principle applies. Success under pressure is rarely the result of last-minute heroics. It is the result of steady, intentional preparation carried out long before the spotlight appears. The organizations that operate calmly during disruption are not lucky; they are structured. Their systems are documented, their responsibilities are clear, and their fundamentals are strong enough to hold when the moment tests them.

Structure Is Built Before the Spotlight

What separates strong teams from fragile ones is not talent. It is preparation that most people never see.
Film study happens in empty gyms.
Conditioning happens early in the morning.
Corrections are made long before the crowd is watching. By the time the tournament begins, the real work has already been done.

Business systems are no different.
The time to test backups is not after a server fails. The time to review access permissions is not after an employee leaves. The time to upgrade aging infrastructure is not when growth has already outpaced capacity. Strong organizations build structure before it is urgently required.
Preparation feels quiet. Sometimes it even feels unnecessary. But it is precisely that quiet discipline that allows teams and businesses to operate confidently when conditions become intense.

When Systems Are Intentional

Organizations with intentional systems respond differently when disruption hits. They are not scrambling to remember who has access to critical files. They are not guessing whether backups will restore. They are not calling vendors in a panic because something stopped working at the worst possible time.
Instead, they execute.

They follow documented procedures. They rely on tested safeguards. They move forward because the groundwork was already laid. Pressure does not feel pleasant, but it does feel manageable.

And that difference matters.
Because in both sports and business, the moment of pressure does not determine success. It reveals whether success was prepared for long before the moment arrived.

AI TOOLS ARE EVERYWHERE

HERE'S HOW TO USE THEM WITHOUT MAKING A MESS

You log back into work after a well-deserved break and your inbox is already full. Meetings are stacking up. The to-do list is longer than you remember. You're back to doing too much with too little time.

And now, on top of everything else, AI is everywhere.

Every app is pushing the same message: "Add AI." "Automate with AI." "Use AI or fall behind." Meanwhile, you're wondering where this actually helps your business and how to keep it from blowing up in your face.

Right now, AI is the new intern everyone hired without training. While interns can be amazing, they can also make big mistakes if nobody sets rules.

3 Time-Saving Ways to Use AI in Your Business

Here are three easy ways AI tools can save you time.

1. Inbox triage and first-draft replies

If your inbox feels overwhelming, AI can help reduce the noise. It can scan long email threads, surface what matters, draft solid first responses and flag messages that need attention. What it cannot do is understand customer nuance or decide what the actual reply should be. That workflow should remain simple: AI drafts. Humans approve.

2. Meeting notes that turn into action lists

Meetings are a tax on productivity. The bigger problem isn't the meeting itself, it's what happens after it ends.

AI note tools can summarize conversations, highlight decisions, capture action items, assign owners and generate clean recaps. This reduces "wait, what did we decide?" moments and helps prevent tasks from slipping through the cracks.

3. Simple reporting and forecasting

Most business owners don't lack data, they lack the time to interpret it.

AI can summarize trends, flag anomalies, surface patterns in support tickets, and churn and turn raw numbers into plain English. Think of it as a sorting machine, not a crystal ball.

The Guardrails: How to Use AI Without Doing Something Dumb

This is where most businesses get burned. They treat AI like a search engine and accidentally feed it something sensitive.

Rule 1: *Never paste sensitive data into public AI tools*

Customer information, payroll or HR data, passwords, and internal financials do not belong in AI prompts. If you wouldn't want it to be public, DON'T share it with the AI tool.

Rule 2: *Control who can use what*

Shadow AI is exploding in small businesses. Employees sign up for random tools with corporate accounts because they want to be efficient. You need an approved tools list, clear guidance on acceptable data use and tighter permissions for sensitive roles.

Rule 3: *AI drafts. Humans decide.*

We said it before, but it's so important we can't emphasize it enough. Anything created by AI that goes out under your brand should be reviewed and approved by a human. No exceptions.

Rule 4: *Assume everything you type is being stored*

Public AI tools live on someone else's servers. Even if data is not being used today, it is still stored somewhere. Like the internet, assume data sent to an AI tool lives forever and act accordingly.

Rule 5: *When in doubt, don't paste*

If you're unsure, don't share until you ask. Make it so others feel comfortable asking.

What AI Done Right Actually Looks Like

Real businesses don't start with massive AI transformations. They pick one or two time-wasting processes, add AI with guardrails, measure the impact and expand slowly.

The businesses pulling ahead aren't chasing hype. They're experimenting safely.

Because the real question isn't whether or not your team is using AI, it's whether they're using it safely.

GUARDING AGAINST ACH FRAUD

GUARDING AGAINST ACH FRAUD

Why Vendor Payment Change Requests Deserve Extra Scrutiny? It usually starts with a simple email.

A vendor you recognize says their banking information has changed. The message looks professional. The logo is correct. The invoice feels routine.

All they need is for you to update the ACH details before the next payment goes out.

And that's where businesses get into trouble.

Over the past year, fraudulent ACH change requests have become one of the most successful financial attack methods targeting small and mid-sized organizations. They are not flashy. They do not require malware. They rely on one thing:

Trust.

How the Scam Unfolds

Fraudsters rarely act randomly. In many cases, they spend time quietly observing how a business communicates before ever sending a fraudulent request. They pay attention to vendor relationships, invoice timing, and who within the organization is responsible for processing payments. Once they understand the normal rhythm of operations, they send a payment change request that looks completely routine.

The email may appear to come from a familiar contact, and the branding or formatting often matches past communication. Sometimes the sender's email address is altered slightly in a way that is easy to overlook. In other situations, a real vendor's email account may have been compromised. The message might feel ordinary, or perhaps just slightly different in tone, but not unusual enough to immediately raise concern.

The objective is straightforward: redirect a legitimate payment into an account controlled by the attacker. By the time the real vendor follows up about a missed payment, the money has typically already been transferred, and recovering those funds can be extremely difficult.

Why This Attack Works So Well

ACH payment fraud is effective because it takes advantage of routine business processes. Accounting teams handle payments regularly, and legitimate updates to vendor banking information do occur. Urgent requests are also common in day-to-day operations, which makes it easier for a fraudulent message to blend in.

Attackers rely on familiarity and speed. They assume that most organizations trust email communication and that busy teams may update payment details without independently confirming the request. In many cases, there is no formal policy requiring verification before changes are made, which creates an opening for fraud to succeed.

When payment updates are treated as routine administrative tasks instead of potential risk events, it becomes much easier for a fraudulent request to slip through unnoticed.

The Control That Stops It

There is one simple rule that dramatically reduces the risk of ACH fraud: never change payment instructions based solely on an email request. If a vendor asks to update their banking information, the safest approach is to call them using a phone number you already have on file and confirm the change directly.

Once confirmed, document who verified the request and when, and require internal approval before updating your records. This process may add an extra step, but it is the kind of safeguard that protects your business. Fraud depends on speed and assumption, while protection depends on verification and consistency.

Make It Policy Not Preference

Strong security should not depend on whether someone feels that an email seems suspicious. It should rely on a clearly defined process that everyone follows every time. When payment change verification becomes standard procedure rather than a judgment call, attackers lose their advantage.

They may be able to send convincing messages, but they cannot pass a direct phone call to a known and trusted contact. That one consistent step helps protect your revenue, your vendor relationships, and your organization's stability. In financial matters, trust is valuable, but verification is essential, and when it comes to ACH payment changes, it is always better to pause first and proceed carefully.

THE HIDDEN BOTTLENECK KILLING YOUR PRODUCTIVITY

(IT'S NOT YOUR PEOPLE)

If you're a business owner, you've had this exact thought: "Why does everything take longer than it should?"

It's not because your people are bad or because they don't care. It's because most processes have extra steps baked in that nobody asked for.

Those steps usually come from tech friction: tools that don't connect, networks that drag and access chaos that makes everyone wait.

Over time, that friction is the difference between "we're moving" and "we're stuck." Let's expose three hidden bottlenecks slowing businesses like yours down and how to fix them without a massive overhaul.

Bottleneck #1: Your Apps Don't Talk To Each Other

Translation: You're running a copy-paste business.

Sales enters a customer in your CRM. Operations re-enters the same information into a project tool. Billing re-enters it again into accounting. Someone emails a spreadsheet "just to be safe."

Nobody wants to do this. They do it because the tools they're using don't share data, so humans become the integration layer.

That creates duplicated work, dropped details, inconsistencies and delays that feel like people are working slowly but are really systems being inefficient.

The hidden cost adds up fast. If 10 people spend just a few minutes a day retyping or reconciling data, that's more than 26 hours a month lost to busy work. Multiply that by payroll, and you're burning money to keep tools from speaking to each other.

Bottleneck #2: Slow Or Unstable Networks

Translation: Death by a thousand loading screens.

This one is sneaky because it feels normal. Files take longer to open. Cloud apps lag. Calls glitch. People restart tools without thinking about it. Nobody complains about a few seconds here and there, but your business bleeds time in small cuts.

It also drains morale. Nothing kills momentum like staring at a loading bar while a customer waits. Network drag turns motivated employees into tired employees, even when they're trying hard.

Bottleneck #3: Approval and Access Chaos

Translation: Everyone is waiting on the one person with the password.

This is where productivity quietly dies.

- "Who has access to that folder?"
- "Can someone approve this?"
- "I need the login for this tool."
- "Only Steve can do that."
- "Steve is out today."

...continued on page 4

SHINY NEW GADGET OF THE MONTH

Solos AirGo A5 AI Smart Glasses

The Solos AirGo A5 AI Smart Glasses bring hands-free AI into your line of sight. With these smart glasses you can translate text on the fly and access contextual information while staying focused on the task in front of you. For busy business leaders, this means fewer interruptions and faster decisions. Instead of stopping to search, information comes to you in real time. It's a small shift that adds up to time savings over a busy week.

Tech of the Month Keep the votes coming

Natalie Thompson IT Specialist

We're proud to recognize Natalie as this month's Tech of the Month. Natalie consistently brings professionalism, patience, and attention to detail to every client interaction. She has a strong ability to solve problems clearly and efficiently while making sure the people she supports feel confident and taken care of.
Her reliability and positive attitude make a real difference for both our clients and our team. Congratulations, Natalie!

FREE DOWNLOAD

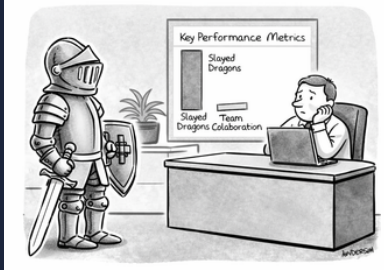
If You Are Considering Cloud Computing for Your Company, Read This First

If you are considering cloud computing or Microsoft 365 to save money and simplify IT, it is extremely important that you get and read this special report: **"5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud."**

This report discusses in simple, nontechnical terms the pros and cons of cloud computing, data security and how to choose a cloud provider. Learn three little-known facts that most IT consultants don't know or won't tell you about cloud computing that could end up causing you MORE problems and costing you more money than you anticipated. **Even if you aren't ready to move to the cloud**, this report will give you the right information and questions to ask when the time comes.

Get your FREE copy today: www.URLHERE.com/cloudreport

CARTOON OF THE MONTH



"Your results are impressive, but we're concerned you're not working with others enough."

...continued from page 3

Businesses normalize this because it just feels like how things work. In reality, it's a permissions system designed by accident.

When access is messy, work stalls and people create risky workarounds while the business becomes dependent on single points of failure.

The 10-Minute Bottleneck Diagnostic

To find your biggest friction points, ask your team three questions:

- "What is one thing you do every day that feels like a waste of time?"
- "Where do you get stuck waiting for something or someone?"
- "What tool or system makes your job harder than it needs to be?"

Don't prompt them. Just listen. You'll hear the same answers repeated by different people.

Finding the bottlenecks is easy, but fixing them is where most businesses stall.

Fixing the Bottlenecks

Once you see the friction, you can remove it. Apps that don't connect can usually be integrated, sometimes natively and sometimes through automation. When data flows automatically, manual work disappears.

Slow networks and Wi-Fi need to be audited and optimized. Sometimes the issue is outdated equipment. Sometimes it's configuration. Sometimes it's simply too many devices on too little bandwidth.

Access chaos requires structure. Document who has access to what. Set up onboarding so people have what they need on day one. Use a password manager instead of sharing credentials.

None of this is glamorous, it's infrastructure. Fix one bottleneck and the whole team moves faster.

How an IT Service Provider Removes the Drag

Most business owners know something is slowing them down. They just don't have time to diagnose it, research solutions and implement fixes while running the business.

A good IT service provider helps by integrating tools, stabilizing networks, setting clean access rules, automating handoffs and building systems that match how your business actually operates.

In short, productivity improves not because people changed but because the environment stopped working against them. If your team is busy but results are lagging, the bottleneck is rarely the people. It's the systems around them.