

TIGERHAWK INS

Insider Tips To Make Your Business Run Faster, Easier And

TIGERHAWK NAMED
TOP 10
IN HEALTHCARE IT



MSP
TITANS
OF THE INDUSTRY Awards

2025 FINALIST in Healthcare IT

Tigerhawk Named a Top 10 MSP in North America for Healthcare IT

I'm incredibly proud to share that Tigerhawk Technologies has been named one of the Top 10 Finalists in the 2025 MSP Titans of the Industry Awards for Healthcare IT in North America. This is a huge honor not just for our team, but for our entire Tri-State community. It's not every day that a national recognition like this comes to an IT company right here in the Quincy/Hannibal area.

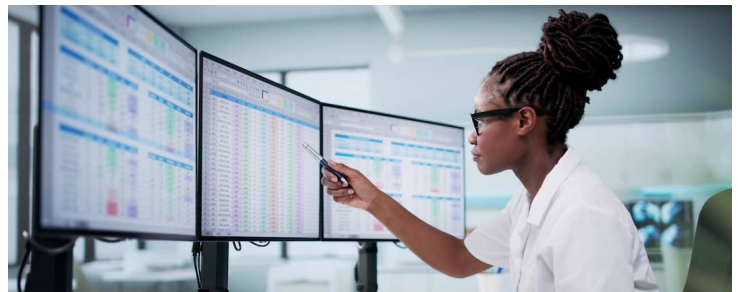
For the past 20 years, we've focused on delivering secure, reliable technology solutions to healthcare providers who care for our communities. Being recognized at this level validates all the long nights, tough calls, and forward-thinking work our team has poured into helping healthcare organizations stay compliant, protected, and productive. We're honored to stand shoulder to shoulder with some of the best providers in the country, and even more honored to serve the people and businesses here at home.



SECURITY IS NO LONGER OPTIONAL

In today's world, cybersecurity isn't just about keeping hackers out. It's about meeting the growing requirements of insurance companies, regulators, and industry standards. That's why, starting **October 1st**, we're upgrading **all Tigerhawk Complete service packages** to include **24/7 Security Operations Center (SOC) and Managed Detection & Response (MDR) services**.

What does that mean for you? It means real people are actively watching over your computers, servers, tablets, and even cloud services like Microsoft 365 every minute of every day. If something suspicious happens, they investigate and respond, typically within **15 minutes**. This level of protection is already standard for our medical clients, and it's becoming a must-have for every business, especially with new requirements from liability and cyber insurance providers. Consider this upgrade one more way we're helping you stay secure, compliant, and ready for whatever comes next.



TIGERHAWK
Technologies Est. 2005

continued on page 2...

TIGERHAWK INSIDER

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

THE TRUTH ABOUT CYBERSECURITY

EVERY BUSINESS LEADER SHOULD KNOW



There are many common myths when it comes to cybersecurity, and, unlike harmless stories, these myths can leave you with gaping holes in your company's cybersecurity defenses. Here are five common myths and the truth behind them.

Myth #1: It Won't Happen To Us.

There's a common belief among small and medium-sized businesses that they are too small to be a target for attackers. But this isn't the case; in fact, some cybercriminals target SMBs specifically, with the knowledge that SMBs are less likely to have the resources for reliable cybersecurity.

Cyberattacks happen to organizations of all sizes, in all verticals and geographies,

and hit 80% of businesses. The global financial toll? A projected \$9.5 trillion. And while large corporations can take the hit and recover, a single ransomware attack has the potential to put an SMB out of business.

So, regardless of what type of business or organization you have, you must protect yourself from cyberattacks and reduce your exposure. Always assume you are a target – because you are one.

Myth #2: If It Worked Then, It'll Work Now.

It's very common for decision-makers to reason that since they've never been breached in the past, they won't be breached in the future either. However, that belief doesn't account for the rapid

pace at which technology – and cybercrime – are evolving.

The threat landscape is constantly changing and there is a very real game of cat-and-mouse at play. If you're not moving forward, you're moving backward. Effective security is a cycle of anticipation, adaptation and action.

Myth #3: Once Secure, Always Secure.

Unfortunately, technology is fluid – just like your business. Every time you bring on a new member of staff and add new devices, your technology's configuration shifts. As it does, it creates new avenues of attack from cybercriminals.

That's why continuous monitoring

and management are necessary to maintain security integrity. The attack surface stretches beyond common focus areas. Because of this, strong cybersecurity demands a holistic, proactive, continuous approach.

Myth #4: Business Optimization Is Incompatible With Security.

Many organizations still assume that security initiatives create operational friction – delaying releases, adding red tape and increasing costs. This outdated thinking frames security and business optimization as mutually exclusive, as if improving one compromises the other.

While these perceptions may have roots in the past, they don't reflect modern practices. Today, security enables optimization. That means minimizing both waste and risk – including security risk.



In the end, secure systems are more resilient, predictable and cost-effective. This makes security a driver of business performance, not a barrier.

Myth 5: A Strong Password Is All I Need.

Creating a strong password (at least 16 characters long and a blend of letters, numbers and special characters) for each account is important, but it's not the only step needed to keep your data secure. For one, every account and device needs a unique password. If you reuse passwords, it

means that if one of your accounts is hacked, all of your other accounts are at risk. To store all your unique passwords, we recommend a password manager!

Enabling MFA for every account will double your protection. The few seconds required to enter a code sent to your phone is well worth the extra security. That said, there are plenty of other vulnerabilities that savvy hackers can exploit to attack your business's data. That's why working with an MSP is a critical component of maintaining your company's cybersecurity.

FREE Cybersecurity Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cybersecurity audit to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.



To Get Started And Claim Your FREE Assessment Now, Call Our Office At (217) 617-4159

CARTOON OF THE MONTH



DR. PHIL

PUSHES BUSINESS OWNERS TO "OWN IT"—IN LIFE AND IN BUSINESS



In a recent interview, Dr. Phil McGraw, celebrity psychologist and talk show host, gave frank advice on what it really means to be in business—and how business owners stay true to themselves while doing it.

Staying True To Passion And Standing Out

"I don't do anything that I'm not a hundred percent passionate about. And I never wanted to be a member of the herd. I didn't want to be a face in the crowd," McGraw said. "I wanted to market my education in a way that set me apart from the rest of the industry. I think you have to do that [in business]."

Define And Articulate Your Differentiator

"You have to know what separates you from everybody else that thinks they do what you do. What do you bring to the table that nobody else does? What do you do that's different than everybody else? If you don't know what your differentiator is, if you can't articulate it and don't market it in an easily perceptible way, then you aren't really in business yet."

You Are Your Own CEO

"I think every one of us is a company of one," said McGraw. "I don't care if you work for the United States post office. Every one of us is a company of one—and you are your own CEO. Then the question becomes: how are you doing in managing your career? How are you doing in managing your stock?

How are you advancing your game? What is the world willing to compensate you for? If you can't articulate that with clarity and precision, then you're not really in business yet. You haven't gotten the courage."

Define, Commit And Own Your Brand

"No one is going to confuse me with anyone else, just like you're not going to confuse McDonald's with a great steakhouse. That's important to me," he said. "Define your brand, decide what it is, make a commitment to it and ride that horse to the finish line. You've got to decide what it is that you're selling and own it. Be who you are on purpose. Don't just get up and react to the world. Decide who you are and do that on purpose. Don't apologize for it. Own it."

Authenticity Is Key To Facing Criticism

"In the pursuit of that, you will face criticism. Not everyone will like you and your brand. But that's exactly why you have to believe in what you're doing passionately," says McGraw. "You can't just put it on. You have to believe it. A lot of people don't like some of the things I do. And I get that. But how boring would this world be, if we were all the same? We have a divisive world, in terms of ideas. But you have to believe what you believe. Then when somebody disagrees with you, if you're authentic in your position, you won't have a problem standing with it."

SHINY NEW GADGET OF THE MONTH

BenQ ScreenBar Halo Monitor Light



The BenQ ScreenBar Halo is a sleek USB-powered LED monitor light designed with an asymmetric optical system that directs soft, glare-free illumination onto your desk while avoiding screen reflection. With adjustable brightness and color temperature, you can dial in the perfect lighting using the wireless controller. It even has a backlight to reduce contrast with your surroundings. Plus, the auto-dimming feature adapts to your room's lighting, so it's always just right. No messy cords or mounts – just clean, functional lighting that protects your eyes and keeps your setup looking sharp.

Tech of the Month Keep the votes coming



Steven Goldhaber Quincy IT Team Lead

Congrats to Steven Goldhaber, our Tech of the Month! Steven is a lifelong learner with a passion for crypto, AI, and quantum computing. Known for his efficiency, empathy, and patience, he strives for excellence in everything he does. His proactive mindset aligns with his favorite quote: "Never put off till tomorrow what you can do today."

5 SIGNS

YOU'RE DUE FOR A TECH UPGRADE



At first, hanging on to old technology for as long as possible seems like a great way to stretch your IT budget. However, the cost of doing so is much higher than simply replacing the tech.

Continuing to use old hardware and outdated software can cost your business in productivity, budget and security.

The Real Cost

There are a few ways that outdated technology is costing your business. First, old systems move slower, causing your team to move slower and impacting productivity. These systems can also fail completely, causing unexpected downtime and putting a major dent in your deliverables.

There's also the risk factor to consider.

Outdated software and hardware are more vulnerable to cyberattacks, because they are no longer being patched to protect against known vulnerabilities.

Hackers are able to exploit these vulnerabilities and access your business's data. Because of this latent risk, your business also runs the risk of failing compliance audits. That's why it's so important to update to the latest software or hardware to stay secure.

Here are a few signs it's time to upgrade your technology:

1 Your Systems Are Still Running On Windows 10 Or Older

Windows 10 is rapidly approaching end of life; Microsoft will end support for it in October 2025. This means any new vulnerabilities will no longer be patched by security updates. Continuing to use Windows 10 past its end-of-life date is a major cybersecurity and compliance risk. To keep your business protected, start planning your upgrade path now and make the switch to Windows 11.

2 You Frequently Call IT For The Same Tech Problems

Frequent crashes and lagging systems aren't just annoyances, they're also indicators that your technology is failing. Slow systems, crashes, frustrated team members and constant tech support add up – and mean a significant impact on your productivity.

3 Your Existing Software Isn't Compatible With New Tools

If you're still using legacy software, it may not integrate with mobile apps or cloud platforms. This limits your ability to adopt new technologies, serve clients efficiently and scale your business.

4 Your Devices Are Slowing Down Your Team

If your team's computers are taking ages to boot up, or freeze or crash during video calls, they're slowing down your entire workflow. At the end of the day, time is money. Inefficient systems harm both. Devices more than three to five years old should be audited for performance and energy efficiency to ensure they aren't having a negative effect on your productivity and energy consumption.

5 You're Relying On Outdated Security Mechanisms

If your business's firewall or antivirus hasn't been updated in years, you're taking serious risks with your data. Cyberthreats evolve quickly; to keep your business safe, your defenses need to evolve too. Outdated systems are often the first point of entry for ransomware attacks.

If you're worried that upgrading tech will break the bank, we hear you. But hanging on to slow, outdated systems can cost more in lost productivity, security gaps and patchwork fixes. The good news is there are plenty of affordable, strategic upgrade paths to keep your business running smoothly without blowing your budget.

GET A FREE DARK WEB & NETWORK SCAN



OCTOBER IS CYBERSECURITY MONTH

Tigerhawk Complete clients are protected with 24/7 monitoring to detect threats before they become breaches. From stolen credentials circulating online to hidden vulnerabilities in your infrastructure, we provide early warnings and expert insight so you can act fast, stay secure, and protect your business with confidence.

WHY YOU NEED A DARK WEB SCAN

A dark web scan is often the only way to know if your company's sensitive data is already in the wrong hands. Stolen emails, passwords, and credentials can circulate online without your knowledge. By the time a breach is obvious, the damage is done. A scan gives you an early warning so you can act fast and stay ahead of cybercriminals.

WHY YOU NEED A NETWORK SCAN

A network scan is the best way to find and fix security gaps before hackers exploit them. As threats grow more advanced every day, even a single weak spot can put your data, reputation, and business at risk. A scan acts like a health check for your IT infrastructure, revealing vulnerabilities and giving you the insights to strengthen your defenses so you can stay protected, compliant, and confident.

CONDUCT A
DARK WEB EXPOSURE
ASSESSMENT



SCAN ME

CONDUCT A
NETWORK EXPOSURE
ASSESSMENT



SCAN ME