TIGERHAWK TECHNOLOGIES

SEPTEMBER 2026 NEWSLETTER

SMART TIPS. TECH INSIGHTS. STRONGER BUSINESS.

BACK UP SMARTER. STAY PROTECTED.

Costly backup myths and identity protection reminders

PROTECT WHAT KEEPS YOUR BUSINESS RUNNING

This issue looks at two areas that are easy to overlook until there is a problem: business backups and identity protection. A backup plan is only valuable if it is tested, secure, and ready when your business needs it. ID Shield adds another layer of awareness for exposed

VERIFY YOUR BACKUPS. WATCH YOUR IDENTITY.

WHAT'S INSIDE THIS ISSUE:

The 4 Most Expensive Backup Assumptions Businesses Make
Avoid the common myths that can make recovery slower, harder, and more expensive.

ID Shield
A simple look at identity monitoring, alerts, and why quick response matters.

RELIABLE You can count on us.

SECURE Protecting your data is our priority.

LOCAL Proud to support our community.

FORWARD Technology solutions for what's next.

TIGERHAWK INSIDER

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

SEPTEMBER 2026

THE FIRE DRILL NO BUSINESS OWNER WANTS TO RUN

When a fire alarm goes off at a school, nobody stops to figure out what to do next. Students line up, teachers move them through the exits and everyone knows where they're supposed to go because they've done it before.

Your backup strategy should work the same way. But most businesses have never tested whether they can actually recover.

Why fire drills save lives and businesses

Fire drills do more than satisfy a policy. They prepare people before pressure sets in and answer one critical question: Will this work when we need it?

When everyone knows what to do, panic stays under control. If the plan fails, they discover it during the drill, not during a real emergency.

That is the value of practice. It removes guesswork before it matters.

The business version of a fire drill

Most businesses have backups. Far fewer have tested whether they'll work.

They don't find out until something goes wrong and they're scrambling to restore systems and get the business running again.

That's when the real cost begins.

What recovery testing looks like

Recovery testing is not theoretical. We restore from your backups, measure how long recovery takes and identify which systems come back first and where gaps exist.

The process answers questions every business should know before an outage:

- Will your backups restore successfully?
- How long will recovery take?
- Which systems should come back first?
- Can your team keep working during recovery?
- Are there gaps in your backup strategy?

That is the difference between having backups and being ready to recover.

What happens when you skip the drill

When recovery has never been tested, even a routine disruption can become a major business problem. Employees lose access to critical systems, customer service can't help customers, sales can't process orders and leadership is left waiting for answers.

The cost isn't just lost time. It's lost revenue, damaged customer trust and unnecessary disruption.

Don't wait for the emergency

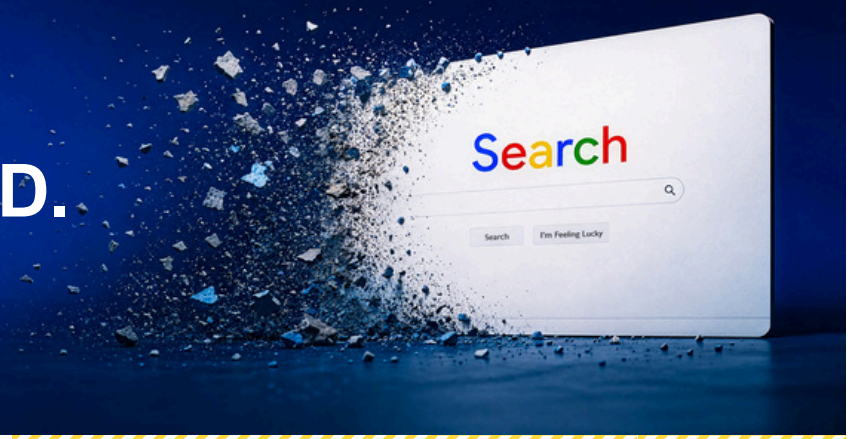
Nobody runs a fire drill because they expect a fire tomorrow. They do it because an emergency is the worst time to discover the plan doesn't work.

Backup and recovery deserve the same preparation. If you haven't tested recovery, you're relying on assumptions. A controlled recovery test will tell you whether your plan is ready before you depend on it.

TIGERHAWK Technologies Est. 2005

THE SEARCH ENGINE CHANGED.

Did Your Marketing?



Think about the last time you needed a quick recommendation.

Maybe your AC stopped working or maybe your kid needed a dentist. A few years ago, you probably would've Googled it, skimmed a few websites, compared reviews and maybe asked someone nearby for a second opinion. Now, more people are skipping that whole process.

They're asking AI tools the same way they'd ask a trusted friend. "Who should I call?" "Which one is reliable?" "Who won't overcharge me?" "What's the best option near me?"

When the answer comes back, many of them don't keep searching. They call the name they were given.

That's the shift small business owners need to understand. Search isn't just about showing up on Google anymore. It's about showing up in the AI-generated answer.

For years, a solid website and a strong Google Business Profile did the heavy lifting. A customer searched "plumber near me" or "bakery near me," got a page of blue links and started comparing. Your job was to climb to the top of that list and stay there. From there, your site carried the visitor toward a call or a booking.

That faucet is shutting off, without so much as a warning.

Consider the numbers. Most B2B buyers already turn to AI tools before they call a vendor. On the consumer side, most Google searches now end without a single click, meaning the AI tool answers the question and the search is over before anyone lands on a website.

AI doesn't always recommend businesses in the same order Google ranks them.

Businesses that never crack page one are getting named by AI tools anyway, while page-one veterans get skipped. Even worse, most people don't double-check what the AI tells them. They just go with it.

That means when a user asks which plumber, dentist or accountant to use, the AI is making the call almost by itself, without ever seeing your reviews, your storefront or your years of good work. If your name doesn't come up, you're invisible, wondering why the phone stopped ringing.

The businesses that win this shift will do it the old way. They'll become so clearly credible that both the algorithm and the human on the other end have no real choice but to point their way.

That kind of credibility comes from good service, strong results and proof people can actually verify.

What that looks like in practice

First, ask a friend to open their own ChatGPT and ask for the best business in your category near them. See if your name shows up. If it doesn't, treat that as a wake-up call.

Second, take stock of your real proof: case studies with numbers, reviews with full names attached, press mentions, awards, anything specific and verifiable. If that list is short, you have a credibility gap, not a marketing gap.

Third, pick one piece of proof and build it out this month. A short book of customer stories, a real review push or a well-written piece in your own voice. Publish it now. Fourth, lean into strategies that build trust in person: partnerships, local events, direct mail followed by a phone call, referral programs. These still move faster than anything online.

The old rules of search are gone. The only question left is whether the machine finds you or hands your next customer to the business down the street with a fraction of your experience and a better AI footprint.

Mike Tyson once said, "Everyone has a plan until they get punched in the mouth."

In business, that punch usually comes in the form of a disruption you assumed you were ready for. It might be a failed backup, an unexpected outage or a security incident that exposes a weakness nobody knew existed.

That's the thing about assumptions. They feel like facts until they're tested.

Here are four that regularly catch businesses off guard.

Assumption #1: 'We're backed up'

Having an untested backup is like carrying a spare tire in your trunk and finding out it's flat when you're stranded on the side of the road.

Most businesses know backups exist. They've seen the reports, the notifications and the green checkmarks. However, only a few can confidently say when they last tested a restore, how long recovery would take or whether every critical application and file is included.

A backup proves its value only when it helps you recover. The most dangerous backup is the one you've never tested. Until you've restored from it successfully, you're relying on hope, not proof.

Assumption #2: 'Someone would tell us if there was a problem'

You can spend big bucks on the latest monitoring tool that's really good at catching problems fast and alerting you immediately. Confusing detection with protection is an assumption that costs businesses money.

A weather alert can tell you a hurricane is coming. It doesn't board up your windows or move your family to safety. The alert is useful only if you know what to do next.

Your monitoring tool works the same way. It tells you something is wrong. What happens after that alert goes off is up to you. Without a response plan, an alert is just another notification demanding your attention.

Assumption #3: 'Our team knows what to do'

Every team looks prepared until game day.

Late one Friday afternoon, a critical system goes offline and suddenly nobody can agree on who's in charge, what to fix first or how long it's going to take.

When there's no documented plan and no practice run, even a good team is starting from zero.

continued on page 4 ...

SHINY NEW GADGET OF THE MONTH

A Monitor That Works Smarter:

BenQ RD280UG

Some upgrades don't transform the way you work. They simply make every day a little easier. The BenQ RD280UG's taller 3:2 display fits more on screen, so you spend less time scrolling and switching windows. Built-in eye care features, USB-C connectivity and an anti-glare display make long workdays more comfortable. It's a thoughtful upgrade that helps you stay focused without adding complexity to your workspace.

Tech of the Month

Darrin Tallmage
IT Specialist

Congratulations to Darrin, Our Tech of the Month!

Darrin has been absolutely killing it onsite, tackling challenges head-on and making sure our customers receive the support they need. His reliability, positive attitude and willingness to step in wherever he is needed make a real difference every day. We appreciate everything Darrin brings to the Tigerhawk team and are proud to recognize him as this month's Tech of the Month. Congratulations, Darrin.

FREE REPORT

12 Little-Known Facts Every Business Owner Must Know About Data Backup and Disaster Recovery

Download this eBook to discover:

- How to ensure your data can be recovered if lost, corrupted or deleted.
- Seven things you should absolutely demand from any off-site backup service.
- Where many backups fail and give you a false sense of security.
- The number one cause of data loss that businesses don't even think about until their data is erased.

CARTOON OF THE MONTH

"First day jitters never really go away."

... continued from page 3

You don't carry a spare tire because you expect a blowout tomorrow. You carry it so that if one happens, you're not standing on the shoulder trying to figure out what to do next.

A recovery plan works the same way. When something goes wrong, you don't want your team figuring things out on the fly. You want them to follow a plan.

Chaos rarely comes from the disruption itself. More often, it comes from not knowing what to do next. The more familiar the process, the faster your business gets back on its feet.

Assumption #4: 'It won't happen to us'

Nobody thinks they'll be the one until they are. When you're focused on growth, customers and keeping things moving, disruption feels like something that happens to other companies. Not yours.

But most disruptions are ordinary, like an employee clicking a bad link in a phishing email, a power outage hitting or a piece of hardware finally giving out. They don't arrive with much warning, and they don't care how busy your business is.

The question isn't whether something unexpected will happen. It's whether you'll be ready when it does.

The businesses that recover fastest didn't get lucky. They got ready. Preparation doesn't stop every incident, but it does determine how quickly you recover from one.

You can't block a punch you didn't prepare for

In our experience, it's never the big dramatic event that catches businesses off guard. It's the ordinary one that happens on a Wednesday when nobody's expecting it.

You don't need the biggest IT budget to recover fast. You need a plan for the day something breaks.

A good plan tells the team what needs to come back first, who's responsible for what and how they'll keep the business moving while systems are restored.

The good news is that most of these risks can be addressed before they become business problems.

Testing your backups, reviewing your recovery plan and making sure people know their role can make the difference between a short interruption and a long recovery.

Preparation won't prevent every outage, but it will determine how quickly you recover and how much disruption your business has to absorb.

IDShield: An Extra Layer of Identity Protection

Cybercriminals are not only interested in passwords. Social Security numbers, financial information, medical records and other personal details can all be used to impersonate someone or open fraudulent accounts in their name.

IDShield is an identity-theft protection service designed to help individuals monitor their personal information and respond when suspicious activity is detected.
What Does IDShield Monitor?

That's the thing about assumptions. They feel like facts until they're tested.

What Does IDShield Monitor?
Depending on the selected plan, IDShield can monitor areas such as:

- Credit reports and new credit inquiries
- Social Security numbers
- The dark web
- Public and court records
- Address changes
- Financial accounts
- Social media activity
- Personal information found on data-broker websites

Members receive alerts when potentially suspicious activity is detected. IDShield offers plans with either one-bureau or three-bureau credit monitoring.

What Happens If Your Identity Is Stolen?

Monitoring can alert you to a potential problem, but recovery assistance is what helps after identity theft occurs. IDShield provides access to licensed private investigators who can help members investigate fraud and work through the identity-restoration process.

Certain plans also include coverage for eligible expenses and losses resulting from a covered identity-theft event. Coverage limits, requirements and exclusions should always be reviewed before enrolling.

Is IDShield Right for You?

No identity-monitoring service can prevent every form of identity theft. These services are designed to provide earlier warnings and professional support when something goes wrong.

Before subscribing, compare IDShield with any protection you may already receive through your bank, credit-card company, insurance provider or employer. Review exactly what information is monitored, how alerts are delivered and what restoration assistance is included.

Even with monitoring in place, continue using strong, unique passwords, multifactor authentication and caution when sharing personal information online.

Back to School Means Back to Phishing
Busy schedules, new accounts and school related messages give scammers the perfect disguise.

September brings a return to familiar routines. Students head back to class, parents adjust their schedules and businesses prepare for the final months of the year. At the same time, inboxes begin filling with password resets, invoices, shared documents, delivery notices, event registrations and account updates.

Cybercriminals know these messages are expected. They create convincing phishing emails that blend in with legitimate communication and encourage recipients to act before thinking. One careless click can expose a password, install malicious software or give an attacker access to sensitive company information.

Watch for These Warning Signs

- Urgent pressure: The message claims your account, payment or access will be suspended unless you act immediately. Scammers often create urgency because they do not want you to stop and investigate.
- An unexpected link or file: Be cautious when you receive an attachment or login link you were not expecting. Even a message that appears to come from a coworker, school or trusted vendor could be fraudulent.

Common September Bait
Phishing attempts during this time of year may pretend to be school portals, event registrations, package notices, payroll updates, shared calendars or password reset requests. Attackers may also imitate

Microsoft 365, banks, delivery companies or familiar vendors.

The subject may change, but the goal remains the same: get you to click a dangerous link, open an infected attachment or provide information that can be used against you or your business.

Pause Before You Click
Before opening a link, hover over it to see where it leads. If the address looks unfamiliar, do not open it. Instead, visit the organization's official website by entering the known address yourself.

If a coworker, customer or vendor sends an unusual request, contact that person using a phone number or email address you already trust. Do not use the contact information provided in the suspicious message.

Taking a few extra seconds to verify a request is far easier than recovering from a compromised account. It's always better to be be safe than sorry.

f **You Think It Is Phishing**

1. Stop. Do not click the link, reply to the message, download the file or open the attachment.
2. Report it. Send the message to your IT or security team so they can investigate it and protect others who may have received the same email.
3. Speak up quickly if you clicked. Fast reporting gives your IT team the best chance to reset passwords, secure your account and limit the damage. Do not try to hide the mistake.

If you entered a password, change it immediately from a trusted device and avoid reusing that password anywhere else. If you provided financial information, contact your bank or payment provider using a verified phone number.

Continue watching your accounts for unusual activity and follow any instructions from your IT or security team.

Phishing succeeds by making ordinary messages feel urgent. A 30 second pause can protect your account, your business and everyone connected to it. When something does not feel right, stop and verify before taking action. Reporting suspicious messages also helps protect your coworkers, customers and community from the same attack.