April 2026

TechTidbit.com

brought to you by Tech Experts

Would Your Business Survive A Serious Cyberattack?

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

It's not a comfortable question, and it's one many SMB owners assume they never really need to answer.

Cyberattacks feel like something that happens to other people. Big brands. Global companies. Organizations with huge IT teams and budgets.

The reality is very different.

Recent research shows that a worrying number of businesses believe they simply wouldn't survive a major cyber incident.

That might sound dramatic, but it's a fair reflection of how exposed many businesses still are.

Cyberattacks have changed. They're no longer just a hacker guessing a password. Attacks today are faster, more targeted, and often designed to shut a business down completely.

Ransomware, for example, is a type of attack where criminals lock your systems and demand payment to unlock them. If you can't access your data, your systems, or your customer information, normal business stops very quickly.

What's interesting is that most business leaders know the risk is rising. Many openly admit they expect their staff to fall for a phishing attack.

Phishing is when a fake email or message pretends to be legitimate, tricking someone into clicking a link or handing over login details.

That single mistake can be all an attacker needs.

Despite this awareness, the basics are still being missed.

Password reuse is a big one. If someone uses the same password at work and across multiple personal accounts, one breach can quickly turn into many.

Cybercriminals know this, which is why stolen passwords are so valuable.

Basic cyber awareness training is another gap. Many employees have never been shown what to look out for or how to spot common scams.

But it's not all doom and gloom.

High-profile attacks have made business owners more alert, especially around newer threats like AI-driven scams and deepfake video calls that pretend to be senior leaders. That growing skepticism is healthy.

The most important thing to understand is that surviving a cyberattack doesn't need expensive tools or complex technology.

Preparation is your best tool.

Simple steps like strong, unique passwords and regular staff training make a real difference.

Do you think your business would survive a serious cyberattack? If you're not sure, we can help you strengthen your defenses. Give us a call at (734) 457-5000.

High-profile attacks have made business owners more alert, especially around newer threats like AI-driven scams and deepfake video calls that pretend to be senior leaders. That growing skepticism is healthy.

The Real Reason You're Struggling With AI

"Without clear guidance, people either avoid AI altogether or use it quietly and inconsistently. That creates risk and limits the benefits."

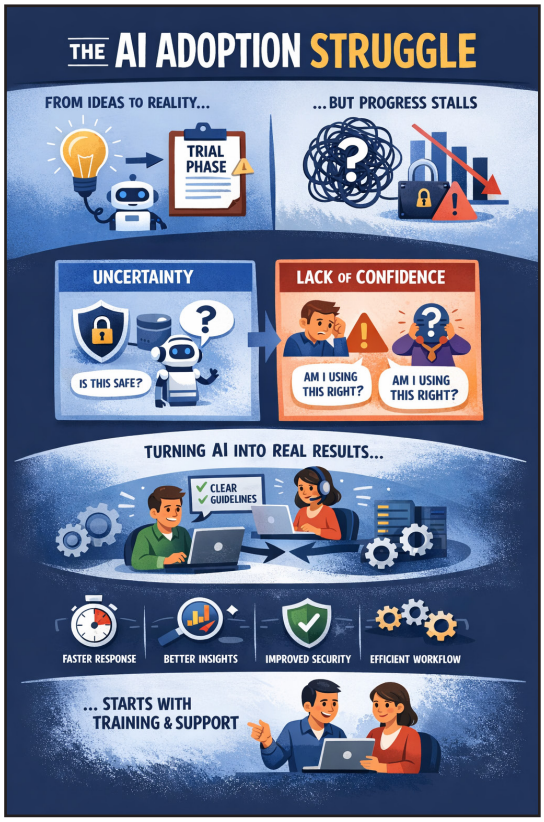
AI has become a regular topic in business conversations.

It comes up in meetings, strategy days and vendor pitches.

Yet for all the talk, many organizations are still struggling to turn AI from an interesting idea into something that genuinely helps people do their jobs.

In many organizations, AI is stuck in a trial phase.

Someone experiments with a tool. A small pilot runs for a few weeks. Then progress slows.



The AI works, but businesses struggle to move from experimentation to everyday use. The return on investment everyone expects stays just out of reach.

Uncertainty is usually to blame.

Leaders worry about security, privacy and compliance. They're unsure what data AI tools are allowed to see or how decisions are being made. Others admit they don't yet have a clear business case, so AI becomes something interesting rather than something essential.

Another big factor is confidence.

Many employees are curious about AI, but also nervous. They worry about making mistakes, relying on the wrong answers, or using tools incorrectly.

Without clear guidance, people either avoid AI altogether or use it quietly and inconsistently. That creates risk and limits the benefits.

It's a shame, because when AI is used properly, the gains are very real. Teams can respond to customers faster, spot issues earlier, analyze data more easily and reduce time spent on repetitive admin.

In technical areas, AI can help monitor systems, improve security, and surface problems before they turn into outages.

These are practical, everyday improvements that add up quickly.

The businesses seeing progress tend to take a steady, human-first approach. They set clear rules around how AI should be used, what it can and can't do, and where human judgment still matters. They focus on giving staff training and reassurance, not just new tools.

AI becomes a support act, not a replacement.

AI projects don't usually stall because the technology isn't ready. They stall because people aren't. If you need help giving your team the confidence to use AI effectively, get in touch.

We Love Referrals!

The greatest gift anyone can give us is a referral to your friends and business colleagues. Referrals help us keep costs down so we can pass the savings to our clients.

If your friend ends up becoming a client - we'll give them their free first month of service (for being a friend of yours) AND we'll give you a $250 Amazon Gift Card.

Simply introduce us via email to sales@mytechexperts.com and we'll take it from there. We'll look after your friend's business with a high level of care and attention (just like we do with all our clients).

Stop Ransomware In Its Tracks: A Five-Step Proactive Defense Plan

Ransomware isn't a jump scare. It's a slow build.

In many cases, it begins days, or even weeks, before encryption with something mundane, like a login that never should have succeeded.

That's why an effective ransomware defense plan is about more than deploying antimalware. It's about preventing unauthorized access from gaining traction.

Here's a five-step approach you can implement across small-business environments without turning security into a daily obstacle course. Each step is practical and repeatable across small-business environments.

Step 1: Phishing-resistant sign-Ins

"Phishing-resistant" sign-ins are authentication methods that can't be easily compromised by fake login pages or intercepted onetime codes.

It's the difference between "MFA is enabled" and "MFA still works when someone is specifically targeted."

• Enforce strong MFA across all accounts, with priority given to admin and remote accounts

• Eliminate legacy authentication methods that weaken your security baseline

• Implement conditional access rules, such as step-up verification for high-risk sign-ins, new devices, or unusual locations

Step 2: Least privilege + separation

"Least privilege" means each account gets only the access it needs to do its job - and nothing more.

"Separation" means keeping administrative privileges distinct from everyday user activity, so a single compromised login doesn't hand over control of the entire business.

• Keep administrative accounts separate from user accounts

• Eliminate shared logins and minimize broad "everyone has access" groups

• Limit administrative tools to only the specific people and devices that genuinely require them

Step 3: Close known holes

"Known holes" are vulnerabilities attackers already know how to exploit, typically because systems are unpatched, exposed to the Internet or running outdated software.

• Set clear patch guidelines: critical vulnerabilities addressed immediately, high-risk issues next, and all others on a defined schedule

• Prioritize Internet-facing systems and remote access infrastructure

• Cover third-party applications

Step 4: Early detection

Early detection means identifying ransomware warning signs before encryption spreads across the environment. Think alerts for unusual behavior that enable rapid containment.

A strong baseline includes:

• Endpoint monitoring that can flag suspicious behavior quickly

• Rules for what gets escalated immediately vs what gets reviewed

Step 5: Secure, tested backups

"Secure, tested backups" are backups that attackers can't easily access or encrypt, and that you've verified you can restore successfully when it matters most.

Both NIST's ransomware guidance and the UK NCSC emphasize that backups must be protected and restorable. NIST specifically calls out the need to "secure and isolate backups."

• Keep at least one backup copy isolated from the main environment

• Run restore drills on a schedule

• Define recovery priorities ahead of time, what needs to be restored first, and in what sequence

If you'd like help assessing your current defenses and building a practical, repeatable ransomware protection plan, contact us today.

"Early detection means identifying ransomware warning signs before encryption spreads across the environment. Think alerts for unusual behavior that enable rapid containment."

What Happens The Day After An IT Disaster?

It's easy to think about an IT disaster in dramatic terms.

A ransomware attack. A server failure. A cybercriminal locking down systems. A major internet outage. Maybe even a fire, flood, or power issue that suddenly takes critical technology offline.

But the real question for most businesses isn't just how the disaster happens.

It's what happens the day after.

That's the moment when the headlines and panic wear off, and reality sets in. Staff still need to work. Customers still expect answers. Orders still need to be processed. Vendors still need to be paid. Phones still need to be answered.

If your systems are unavailable, even for a short time, the disruption spreads quickly across the business.

This is where many companies discover a hard truth: they may have thought about prevention, but they never fully planned for recovery.

Most businesses have at least some level of protection in place. They may use antivirus, firewalls, cloud services, or data backups. Those are all important. But recovery is about more than simply having tools. It's about knowing how the business will function when something critical is suddenly unavailable.

For example, if your main files were inaccessible tomorrow morning, would your team know what to do first? If email was down, how would employees communicate internally and with customers? If your line-of-business software stopped working, could you still access the information needed to keep operations moving? If phones were affected, would calls be rerouted somewhere else?

These questions are uncomfortable, but they matter.

A business continuity plan is what helps answer them. It doesn't need to be a huge binder gathering dust on a shelf. In fact, the most effective plans are often simple, practical, and easy to follow.

The purpose is to define what is most important, what needs to happen first, and who is responsible for making decisions during a disruption.

The starting point is identifying your critical systems. Every business depends on certain tools more than others. That might be your email, accounting platform, CRM, file server, phones, remote access system, scheduling software, or industry-specific applications.

Not every system needs to be restored immediately, but some absolutely do. If you don't define those priorities in advance, the recovery process becomes slower, more chaotic, and more expensive.

Communication is another major piece that often gets overlooked.

During an outage, confusion can become just as damaging as the technical issue itself. Employees need to know where updates will come from. Customers may need reassurance. Vendors may need instructions. If the usual communication channels are down, you need a backup plan. That could mean alternate email accounts, mobile phones, a cloud-based phone failover option, or even a documented call tree for urgent updates.

Backups are also a big part of the conversation, but businesses sometimes misunderstand what backups really solve. Having backups is important, but backup files alone do not guarantee a fast or smooth recovery. You also need to know how long restoration will take, which systems get restored first, and whether the restored data has been tested recently. A backup that has never been verified is more of a hope than a plan.

Then there's the people side.

When something goes wrong, employees are often unsure whether they should keep working, shut devices off, report suspicious activity, or wait for instructions.

Without clear guidance, people make inconsistent decisions, and that can make a bad situation worse. Even a basic incident response checklist can go a long way toward reducing panic and helping staff respond appropriately.

The businesses that recover best are rarely the ones with the fanciest technology. They're usually the ones that prepared in advance, practiced their response, and made sure people understood their role. They know which systems matter most. They know how to communicate. They know how to restore operations in a sensible order.

An IT disaster doesn't have to become a business-ending event.

But survival depends on more than prevention alone. It depends on recovery, coordination, and preparation before the crisis begins.

Because when the day after arrives, you don't want to be figuring everything out for the first time.

You want a plan.

If you're not sure how your business would operate after a serious IT disruption, now is the time to find out. We can help you build a practical recovery and continuity plan before you ever need it.

Contact Information

Tech Experts
Support Team
(734) 240-0200
support@MyTechExperts.com

Main Office
(734) 457-5000
info@MyTechExperts.com

Sales Inquiries
(888) 457-5001
sales@MyTechExperts.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com