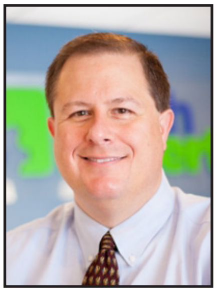
January 2026

TechTidbit.com

brought to you by Tech Experts

You Absolutely Need To Back Up Your Cloud Services Like Office 365



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

Most businesses today rely heavily on Microsoft 365 for email, documents, calendars, and collaboration. It's the backbone of day-to-day operations.

Because Microsoft has massive data centers and strong uptime, many people assume their data is automatically "fully backed up." That's a dangerous assumption.

Microsoft 365 runs on a shared responsibility model. Microsoft does a great job keeping the platform running, but protecting your data is still your responsibility. In other words, they keep the lights on - but what happens to your files, emails, and Teams data is ultimately on you.

Yes, Microsoft includes some built-in safety nets. Things like file versioning in OneDrive and SharePoint, recycle bins that typically keep deleted items for up to three months, and basic retention policies can help recover from simple mistakes. Accidentally delete a file or overwrite a document? You may be able to get it back - if you catch it in time.

That "if" is the problem. Once those retention windows expire, your data is gone. There's no rewind button. And these tools aren't designed for full, point-in-time restores or long-term archiving across your entire environment.

Human error alone makes this risky. Someone deletes the wrong folder. An email with an important attachment is purged. A departing employee's mailbox is removed before something critical is discovered.

These things happen every day, often without anyone realizing it until it's too late.

Security threats raise the stakes even higher. Ransomware and account takeovers increasingly target Microsoft 365 environments through phishing and stolen credentials.

Even with good security controls in place, breaches still happen. When attackers encrypt or delete cloud data, Microsoft's native tools don't always provide a clean, fast way to roll everything back.

Then there are outages. While rare, Microsoft 365 service disruptions do occur. When access is interrupted, organizations without independent backups may find themselves completely stuck, unable to retrieve email, files, or records when they need them most.

Compliance requirements add another layer. Industries governed by HIPAA, GDPR, or financial regulations often need longer retention, audit trails, and reliable recovery options. Microsoft's built-in tools help, but they're usually not enough on their own.

That's where third-party Microsoft 365 backups come in. Dedicated backup solutions capture your data regularly, store it independently, and let you restore exactly what you need when you need it. They're affordable, easy to automate, and dramatically reduce risk.

Bottom line: Microsoft 365 is an excellent productivity platform, but it is not a complete backup solution. If your data matters to your business, relying on built-in tools alone is a gamble you don't need to take.

Microsoft does a great job keeping the platform running, but protecting your data is still your responsibility. In other words, they keep the lights on - but what happens to your files, emails, and Teams data is ultimately on you.

It’s Time To Prepare For The Era Of Agentic AI

“To do that safely and effectively, it needs clean data, reliable systems and secure paths to the information it uses. That’s where lots of businesses will need to prepare.”

A quiet shift is happening in the digital world. But most businesses won’t notice it until it’s already reshaped how work gets done.

We’re entering the era of agentic AI. Smart, autonomous systems that don’t only assist people, but act on their behalf.

While that might sound futuristic, the foundations are already in place today.

Unlike traditional tools that wait for someone to click, type or browse, agentic AI can read data, talk to other systems, and complete entire tasks end-to-end.

It can negotiate prices, fill out forms, run processes and make decisions within rules you set.

To do that safely and effectively, it needs clean data, reliable systems and secure paths to the information it uses. That’s where lots of businesses will need to prepare.

Most companies have grown their technology stack over years, adding apps, cloud services, storage locations and workflows along the way.

It works, but it’s often messy behind the scenes. Data sits in different places. Integrations are fragile. Permissions aren’t always up to date. These things might not cause major problems today, but they’re exactly the areas agentic AI depends on.

Identity Systems
Data Governance
Secure API
Reliable Automation Pathways
Clean Data

For example, AI agents rely heavily on APIs, the simple, secure digital doors that allow one system to talk to another.

If those doors don’t exist, don’t work properly or aren’t secure, the agent’s capabilities become limited or worse, risky.

The same goes for identity management. If your business still relies on shared passwords, old login methods or inconsistent MFA, an autonomous system can only do so much safely.

Then there’s data quality. AI agents don’t guess, and they don’t “work around” human mistakes.

If your data is duplicated, inconsistent or outdated, the agent will simply act on whatever it sees. Even if that leads to poor decisions.

Good data governance suddenly becomes a business essential, not a nice-to-have.

You may also need to rethink how automations run inside your business.

Many companies already use basic workflow tools, but agentic AI expects deeper, more reliable automation pathways that don’t break the moment a system changes.

Luckily, it’s simply a case of strengthening the digital foundations you already rely on. Better identity systems, cleaner data, solid cloud infrastructure, modern security and well-designed integrations.

Agentic AI will introduce incredible opportunities, but only for businesses whose tech environments are ready for it. If you need help getting those foundations right, get in touch.

Upgrading Your Technology Could Reduce The Impact Of Sick Leave

Most businesses have felt the pain of sick leave at some point.

A key person off for a few days can slow everything down. A longer absence can put entire projects on hold.

But did you know that upgrading your technology can help offset some of that lost time?

When people talk about tech upgrades, they often think it means buying shiny new devices. Really, it's mostly about removing the daily friction your team faces.

You know the thing. Slow systems, unreliable tools, old software, and clunky processes. They may seem small, but over a year, they quietly drain hours, days, even weeks of productivity.

Recent research shows that improving workplace connectivity - that's the speed and reliability of your internet and internal systems - could help employees reclaim the equivalent of several working days per year.

Why?

Because when systems are fast, secure and stable, people get more done with less frustration. And frustration is a bigger problem than most business owners realize.

A large share of employee sick leave around the world is connected to stress and mental health. And many workers say outdated or unreliable tech is part of what increases their stress.

Think about how it feels when you're trying to do something important and your device freezes or a system keeps crashing. Modern tools remove that emotional strain by simply… working.

Better tech can also give employees more flexibility.

Cloud systems (software and data stored securely online rather than on a local computer) make it easy for people to work effectively from anywhere. And AI tools, which help automate repetitive tasks or surface information quickly, free up time and reduce cognitive load.

When people feel in control of their work, they tend to feel less stressed, more productive, and more satisfied.

There's another benefit too: Training.

Many workers say they want better skills and clearer support as businesses adopt new tools. The advent of AI and AI-assisted tools means your team is working with new technology regularly.

When people understand the technology they're using, confidence goes up and mistakes go down.

So while you can't stop illness entirely, you can build a workplace where lost time hurts a lot less.

If you need help making an investment in productivity, well-being and long-term resilience, please give us a call at (734) 457-5000, or email us at info@MyTechExperts.com.

> *"Because when systems are fast, secure and stable, people get more done with less frustration. And frustration is a bigger problem than most business owners realize."*

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).

Why Hackers Love Small Businesses... And It Isn't The Reason You Think

When people hear about cyberattacks, they usually picture giant corporations, government agencies, or well-known brands making the news.

That leads many small business owners to a dangerous conclusion: "Why would anyone bother with us?"

The reality is the opposite.

Small businesses are often more attractive targets than large enterprises - not because they're famous or wealthy, but because they're easier.

Hackers aren't usually looking for a specific company. They're running automated scans and phishing campaigns across thousands of businesses at a time, searching for the lowest resistance. The goal isn't drama. It's efficiency.

Large organizations invest heavily in cybersecurity teams, advanced monitoring, and formal response plans.

Small businesses, by contrast, are more likely to rely on basic protections and the hope that nothing bad happens. From a hacker's perspective, that's a much simpler equation.

One of the biggest reasons small businesses get hit is inconsistent security habits.

Passwords get reused. Updates get postponed. Old employee accounts linger longer than they should.

These aren't signs of carelessness, they're just signs of busy people juggling a lot of responsibilities. But they create openings that attackers know how to exploit.

Email is another favorite entry point. A convincing phishing message doesn't need to fool everyone. It just needs to fool one person on a hectic morning.

Once an attacker has access to an email account, they can quietly monitor messages, reset passwords, or launch follow-up attacks from a trusted address.

By the time anyone notices, the damage is already underway.

There's also a misconception that cybercrime is always about stealing money directly. In many cases, it's about stealing access.

Email accounts, cloud files, and login credentials can be resold, reused, or leveraged for ransomware later. Even a small company's data has value in the wrong hands.

Another factor is recovery. Large organizations expect incidents and practice responding to them. Small businesses often don't.

When something goes wrong, they're left scrambling, figuring out who to call, what data is affected, and how long systems will be down. That chaos is exactly what attackers count on.

Ironically, many small businesses do have good tools in place, but they're not consistently configured, monitored, or tested.

Backups may exist but haven't been verified. Security features may be available but not fully enabled. The gap between "having technology" and "actively managing it" is where problems start.

The good news is that this isn't about spending enterprise-level money or turning your office into a high-security bunker.

Most successful attacks rely on very basic weaknesses - things that can be addressed with the right planning, consistency, and oversight.

Hackers don't love small businesses because they're small. They love them because they're busy, trusting, and often stretched thin. When security becomes intentional instead of reactive, that appeal fades quickly.

The goal isn't to be perfect. It's to be prepared. And in today's environment, preparation is one of the smartest business decisions you can make.

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