August 2026

GIO Tech Times

Putting the Power of IT Back in Your Business with Insider Tips for Speed, Simplicity, and Profit

Many businesses store their files in Microsoft 365 or Google Workspace and assume that's all the data protection they need. It isn't.

If files get overwritten, deleted or encrypted, the platform won't restore them. That job falls to you.

WHAT CAN STILL GO WRONG IN THE CLOUD?

Cloud platforms sync fast - great for productivity, until something goes wrong. That speed means deleted, changed or encrypted files spread across every device before anyone notices.

1. Accidental file deletion:
Someone removes a shared folder by mistake, and the deletion syncs across every device. Employees lose access to needed files, and work stalls while the team scrambles to recover them.

2. Overwritten data:
An employee saves the wrong version of a file, overwriting the correct one. The team loses time rebuilding it, delaying customer work.

3. Ransomware on synced files:
Ransomware encrypts files on one device, and those encrypted versions sync to the cloud. Recovery becomes harder without a clean backup from before the attack.

4. Expired retention limits:
Cloud platforms only keep deleted or changed data for a limited window. If an issue surfaces after that, a single missing file can snowball into billing, customer or compliance problems.

5. Misconfigured permissions:
A small permissions error can lock employees out of needed files, or expose sensitive data - pulling managers into an unplanned recovery process. Each one causes problems that reach beyond the original issue. The fix starts with testing your backups.

Testing proves your safety net works
Having backups isn't the same as knowing they're complete, current and recoverable. Regular testing reveals corrupted files, missing folders and coverage gaps before a real disruption forces the issue.

Your team should know exactly what can be restored, and how long it will take.

The Backup Truth

Every business owner thinks a disaster won't happen to them - until it does. A server fails. A laptop gets stolen. Ransomware locks up a shared drive on a Friday afternoon, of course, right before a big deadline. It's not a question of if. It's when.

Here's what I've learned after years of doing this: the difference between a bad day and a business-ending one usually comes down to one thing - whether your backups actually work. Not whether they exist. Whether they're complete, current, and ready the moment you need them. I've seen too many businesses learn the hard way that "we have backups" and "we can actually recover" are two very different things.

I think about this constantly, because the stakes are real for the people I care about - our clients, our community, our team. So do yourself a favor: know what's protected in your business right now, and how fast you could really get back up if something went wrong. It's worth the ten minutes it takes to find out.

Dan Giordano
dan@giotechnologies.com

5 Ways Skipping Backup Testing Can Disrupt Your Business

Most businesses trust their backups completely, right up until the moment they don't work. If you've never tested yours, you don't know what you have. A file sitting in storage without a proven restore process isn't a recovery plan. Testing shows whether your systems, files and recovery procedures can keep your business running when something breaks. Skip the tests, and your first live restore becomes your first live drill with no room to fail. The stakes are simply too high.

Here are five major risks you take when backup testing isn't on the calendar.

1. FAILED RANSOMWARE RECOVERY

Ransomware attackers don't go after just your systems. They go after your backups, too. If backup files were infected or your recovery process has never been run end to end, you could be unable to restore what your business depends on right when you need it most.

Regular testing confirms backup copies are clean and restorable. It also tells you how long a real recovery takes. An extra two hours of downtime impacts revenue, customer commitments and operations.

2. PERMANENT DATA LOSS

Data loss doesn't always come from cyberattacks. Hardware failures, accidental deletions, software corruption and natural disasters can erase important files without warning.

Without backup testing, you operate on the assumption that everything is saved correctly. When a recovery fails and the data is gone, that assumption is all you have left.

Testing confirms the recovery process holds up under real conditions. Your team can check whether files open without errors and critical applications run as expected.

3. SILENT DATA CORRUPTION

Some backup failures happen quietly for weeks or months before anyone notices. Files corrupt over time, configurations drift after software updates and important data can stop saving correctly without triggering an alert. You won't know until you try to restore something and find it's missing or unusable.

Running regular tests means you catch these problems before a real disruption forces the issue.

4. EXPENSIVE DOWNTIME

Every minute of downtime costs money, but the outage isn't always the biggest problem. Finding out mid-crisis that your team has never completed a restore is the bigger issue.

Without a tested recovery process, what should take 20 minutes stretches into hours. Under pressure, employees cannot work, customers are waiting and the situation keeps deteriorating.

When you test regularly, recovery becomes familiar before it becomes urgent.

5. COMPLIANCE AND LEGAL PENALTIES

Healthcare providers, financial firms and legal organizations face serious consequences when they fail to recover protected data.

Regulators need evidence that your recovery process works. A failed restore resulting in missing customer data can trigger penalties, legal liability and a compliance audit your business isn't prepared for.

YOUR BACKUPS ARE ONLY AS GOOD AS YOUR LAST SUCCESSFUL RESTORE

A backup file sitting in storage isn't protection. A tested, verified and documented recovery process is.

Key Takeaway:
Without backup testing, what should be a fast recovery can quickly spiral into downtime, data loss and compliance risk.

What AI Can't Do When Your Systems Go Down

AI monitoring tools identify unusual activity and notify the right people faster than ever before. But they can't restore your data or get your team back to work. Detection and recovery are different problems. The gap between them is where businesses get hurt.

DETECTION AND RECOVERY AREN'T THE SAME THING

Most businesses have spent big money on tools that tell them when something is wrong. Recovery planning gets significantly less attention.

Think about a fire alarm. It alerts you to danger, but it doesn't extinguish fires. It can't protect your building, your belongings or get people to safety.

What it does is give you time. Whether the incident is contained or spreads depends on the preparation and safeguards you already had in place.

AI monitoring tells you a server is down, flags unusual activity and alerts you to a failed backup. What it can't tell you is the true cost of lost productivity or the impact of having your team sit idle waiting for direction.

For a growing business like yours, what happens next often comes down to one thing: how quickly you're able to recover.

YOUR REAL SAFETY NET

As a business owner, you know disruptions are inevitable. It's not a question of if they'll happen, but when.

The businesses that recover quickly aren't the ones with the most expensive or sophisticated tools. They're the ones that knew exactly what to do the moment something went wrong.

Two businesses hit by the same cyberattack on the same day can have completely different outcomes. One spends three days figuring out what to do while the other is back online within hours.

That doesn't happen by chance. It comes from having a recovery plan that's been tested, verified and confirmed to work before it's ever needed.

The difference? One had a documented playbook spelling out every step: who's responsible, what needs to happen, the exact sequence. They practiced it; it failed during a test; they learned what broke and fixed it. When the real incident hit, they were executing a plan, not inventing one.

TEAM GIO

Powered by Kaitlyn

Yes, You Still Need to Back Up Microsoft 365

Here's a common misconception: if your email, files, and Teams chats live in Microsoft 365, they're already backed up. Not quite. Microsoft guarantees the uptime of its platform, but protecting against accidental deletions, malicious attacks, or human error falls on your IT provider - not Microsoft.

This is called the Shared Responsibility Model, and it applies to most SaaS platforms. If an employee accidentally deletes a critical folder, or a phishing attack encrypts your files, Microsoft's built-in recycle bins and retention policies only go so far - and they don't last forever.

At GIO, backing up Microsoft 365 has been part of our standard protection for every client - quick recovery of emails, SharePoint files, and OneDrive data, no matter what caused the loss.

If you're not sure whether your business has this in place, it's worth asking the question. "The cloud" doesn't automatically mean "backed up" - and that's a gap many businesses don't discover until it's too late. The peace of mind is worth it.

-Kaitlyn Neal
support@giotechnologies.com

That's what a tested recovery plan looks like in practice. It's not a document that sits on a shelf, but a living, proven process your team knows how to execute under pressure.

HOW PREPARED ARE YOU? ASK YOURSELF THESE QUESTIONS

Vendors get added quickly. An integration here, a new app there, a tool someone on your team recommended. Each one often comes with some level of access to your systems or data.

When your AI tool notifies you of unusual activity, the answers to these questions separate a quick recovery from a long, costly disruption:

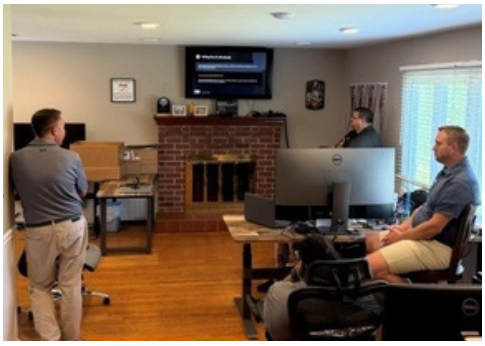
- When did we last test our backups, and did the restore work?
- If something went wrong today, how long would recovery take?
- Does everyone know their role if a critical system goes down?
- Are we confident our backups would work if we needed them right now?
- If a disruption happened today, could we get employees back to work within a timeframe we can live with?

HOW WE HELP

Your AI monitoring tool alerts you when something breaks. What it can't tell you is whether you're ready to recover.

That's where GIO Technologies come in.

We work with businesses like yours to test backups, validate recovery processes and identify gaps before they become costly interruptions. Most of our clients discover their backups are incomplete or corrupted the first time we test them. Better to find that out in a controlled test than during a crisis.



Team GIO Discussing Ai Safe Practices

When something goes wrong, you want a plan that's already been tested and proven to work. A smarter alarm is worth something only if you're ready for what comes after it fires. Schedule a 10-minute discovery call and get a clear picture of where your business stands.

Key Takeaway:
Detection tells you something's wrong. Recovery requires a tested plan you already had ready before the alert fired.

GIO MONTHLY MOMENTS

TEAM GIO UPDATES

Our recent team meeting came with a sweet twist - local ice cream, because National Ice Cream Day doesn't celebrate itself. Between scoops, we dug into where AI is heading and what it means for how we support our clients. It's a fast-moving space, and staying ahead of it (instead of playing catch-up) is exactly the kind of thing we geek out about.
It's been a big month around the office too - we welcomed new customers, celebrated a perfect score on a client's CMMC Level 2 assessment, and got our permit approved to get our office build underway.
As always, moments like these are a good reminder that even in an industry built on solving problems, we like to have a little fun along the way.

CMMC Level 2 Certification - Perfect Score

Congratulations to one of our clients DAS this month on earning a perfect score on their CMMC Level 2 certification assessment! A perfect score means there wasn't a single gap. Their assessment came a couple weeks before a shift in the federal requirement status - so while the mandate has since changed, this achievement stands as a genuine, hard-earned milestone. Special thank you to Greg on our team, who led the charge and helped make it happen. Great work, and congratulations!