August 2026

D2IT Tech Times

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

Think Your Cloud Data Is Safe?

Think Again

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

Your cloud provider keeps the infrastructure running and the platform available. Protecting and recovering your data is entirely your responsibility.

When files get overwritten, deleted or encrypted, the platform won't restore them. That job falls squarely on you.

WHAT CAN STILL GO WRONG IN THE CLOUD?

Cloud platforms sync fast, which is great for productivity. But when something goes wrong, that same speed works against you. Deleted, changed or encrypted files sync across every connected device before anyone catches the issue.

The most common ways businesses lose cloud data are the following.

1. Accidental file deletion:
Someone removes a shared folder by mistake. That deletion syncs instantly across the cloud and every connected device. Employees lose access to the files they need and work stalls while the team figures out what's missing and how to get it back.

2. Overwritten data:
An employee saves the wrong version of a file, replacing the correct one without realizing it. The team loses time trying to rebuild what was lost, and customer work gets pushed back.

3. Ransomware on synced files:
Ransomware encrypts files on one device and those encrypted versions sync straight to the cloud. Your business loses access to key documents, and 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 window closes, one missing file can cascade into a larger disruption affecting billing, customers or compliance.

5. Misconfigured permissions:
A small permissions error can lock employees out of files they need or expose sensitive data to the wrong people, pulling managers into a recovery process they didn't plan for.

Each of these creates problems that reach well beyond the original issue.

Making sure your backups can stand up to that starts with testing.

TESTING PROVES YOUR SAFETY NET WORKS

Having backups in place is not the same as knowing whether they are 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.

Key Takeaway:
Cloud storage alone won't save your business when data loss hits. You're fully responsible for your data.

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.

CLIENT SPOTLIGHT

"Tony Olson and his team have consistently demonstrated expertise and dedication in providing IT solutions and support for Boys and Girls Home and Family Services. Their commitment to our success, technical proficiency, and outstanding customer service make them a top choice for any company in need of reliable IT services. D2 Worldwide continues to be an invaluable partner in enhancing our IT capabilities, and I strongly endorse them to any organization seeking a reliable and proactive IT partner."

Terri Dooley | Executive Vice President of Development

Boys and Girls Home and Family Services

The First Hour After Your Backup Fails

This is how things look after a crisis when your untested backup fails:

0 min: Systems go down

5 min: Guesswork replaces a plan

10 min: Work stops

20 min: Customers notice

30 min: Leadership shifts into crisis mode

45 min: Damage compounds

60 min: No timeline or answers

With a tested backup, the story can stop before the 10-minute mark.

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 we 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.

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.

D2 IT

CASE STUDY

During an annual technology review, a longtime client with ties to a national service organization identified that they needed updated AI policies for staff. First and foremost, policies had to safeguard data and comply with legal obligations and best practices. They also had to be tailored to our client. By aligning AI policies with their mission and values, we could promote ethical AI use and address potential biases within the technology.

Check out the full case study on our website, or **click here** to read more case studies.

COMING NEXT MONTH

FROM REACTIVE TO PREPARED

Next month, we're focusing on disaster preparedness and the costly setbacks that follow when businesses wait too long to plan. September is Disaster Preparedness Month, making it the right time to take a hard look at how your business would hold up under pressure. We'll break down what slows recovery and the decisions that can stop disruption before it spreads to your most critical systems.