AvTek Chronicle



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.

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.

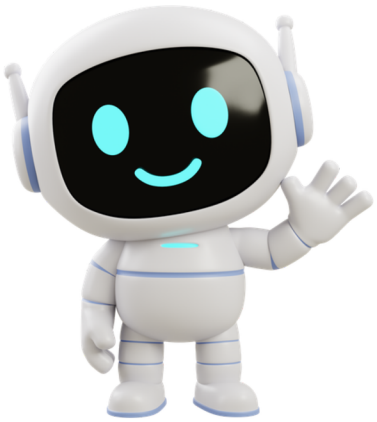
The businesses that recover quickly aren't the ones with the most expensive or sophisticated tools. They're the ones that knew exactly what to do the moment something went wrong.

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.



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.

CMMC Update: Don't Hit Pause on Cybersecurity

The Department of Defense has temporarily suspended CMMC Phase II requirements while it reviews the program, but that doesn't mean cybersecurity efforts should slow down. Organizations handling Controlled Unclassified Information (CUI) are still responsible for meeting existing DFARS requirements and protecting sensitive government data.

Use this time to strengthen your security program by addressing control gaps, documenting policies, and improving your overall cybersecurity posture. Regulations may evolve, but investing in a strong security foundation is never wasted effort. Organizations that focus on readiness today will be better prepared for whatever compliance requirements come next.