



CTTS TECH TALK

YOUR TECHNOLOGY NEWSLETTER

AUGUST 2026



JOSH



SARA



KURT



MICHELLE



CHAIM



KEN



EVAN



KURT



CORNELIUS



SARONNA



ALEX



JENNY



DANNY

CTTS TechTalk
When Technology Alerts You, What's Next?
AUGUST 2026
Cloud Backup, AI Monitoring & Recovery Planning
CENTRAL TEXAS LOCAL PARTNERS PROVEN SOLUTIONS
PREPARED TODAY. RESILIENT TOMORROW.
We help Central Texas businesses stay protected, productive, and prepared.
Central Texas Technology Solutions

Technology can tell you when something goes wrong. It cannot guarantee your business is ready to recover. Cloud platforms keep teams connected. AI monitoring can identify problems faster than ever. Backup systems may report that everything is running normally. But none of those tools can replace a tested recovery plan, clear responsibilities, and confidence that your data can actually be restored.

Inside this issue, we look at the assumptions that often create a dangerous blind spot. You will learn why cloud storage is not the same as cloud backup, what AI monitoring cannot do during an outage, and why a successful alert or backup notification does not always mean your business can recover quickly.

The goal is simple: help you move beyond detection and build a practical plan for what happens next.

INSIDE THIS ISSUE

TECH NOTES



Two Alerts, One Blind Spot:
What Your Technology Can't Do For You

PAGE 2

ADVANCED TECH



Think Your Cloud Data Is Safe? Think Again.

PAGE 3

BIZTECH



What AI Can't Do When
Your Systems Go Down

PAGE 4



TECH NOTES FROM JOSH WILMOTH

Two Alerts, One Blind Spot: What Your Technology Can't Do For You



"Technology can tell you something broke. Only a plan can tell you what happens next."
— Josh Wilmoth, CTTS

A few weeks ago, a client called me after his monitoring system flagged an issue in the middle of the night. His dashboard did exactly what it was supposed to do. It caught the problem early, sent the alert, and gave his team a head start.

Then he asked the question that actually matters. Okay, now what?

That pause is more common than most business owners want to admit.

We are living through a stretch where the tools genuinely are impressive. Cloud platforms keep every file synced across every device without anyone thinking about it.

AI monitoring watches your network around the clock and rarely misses a beat. It is easy to look at that stack of technology and assume you are covered.

Two Assumptions That Keep Showing Up

The first assumption is that storing something in the cloud

means it is backed up. It is not. Microsoft and Google keep the platform running, but the files inside it, the folders your team built, the retention settings, the recovery plan, that part is still on you. It is called the shared responsibility model, and most business owners have never heard the phrase until they need it.

The second assumption is that a good alert equals a good outcome. An alert only tells you something is wrong. It does not rebuild a server, restore a file, or get your team back to work. That part still depends entirely on what you set up before the alert ever fires.

Both assumptions come from the same place. Impressive technology feels like protection, and it is easy to stop asking the harder question underneath it. If this actually happened, could we recover, and how fast?

Twenty Two Years Has Taught Me One Thing

In twenty two years of running CTTS, I have never had a client tell me their backup failed at a convenient time. It is always the week of a big deadline, the week a key employee is out, or the week everyone assumed someone else was watching it. A tested plan does not care what week it is. That is the whole point of testing it.

How CTTS Helps

We spend a lot of our time with clients answering the "now what" question before it ever has to be asked out loud. That means testing recovery, not just scheduling it. It means walking through what happens step by step if a server goes down or a cloud account is compromised, and making sure everyone on the team, not just IT, knows their role.

Call CTTS at (512) 388-5559 or visit www.CTTSONline.com to schedule a conversation.

P.S. I have sat in enough client meetings to know the exact moment a business owner realizes their backup was never actually tested. It is not panic. It is more of a slow drop in the stomach, followed by, wait, so what actually happens now. Do yourself a favor and find that answer on a quiet Tuesday afternoon instead of during a real emergency. Sleep well, Central Texas.



CTTS, Inc. 557 S. Interstate 35, Suite 201, Georgetown, TX 78626
www.CTTSONline.com | (512) 388-5559

ADVANCED TECH

Think Your Cloud Data Is Safe? Think Again.



Many businesses store files in Microsoft 365 or Google Workspace and assume their data is fully protected. That assumption can create a serious recovery problem.

Cloud platforms are excellent for keeping employees connected and productive. However, cloud access is not the same as having a reliable backup.

When files are deleted, overwritten, corrupted, or encrypted by ransomware, your cloud provider may not be able to restore everything you need. Protecting and recovering your business data is still your responsibility.

This is known as the shared responsibility model. Microsoft and Google protect the cloud platform and keep the infrastructure running. Your business remains responsible for its files, user accounts, permissions, retention settings, and recovery plan.

Five Ways Cloud Data Can Be Lost

Cloud platforms sync changes quickly across users and devices. That helps teams work efficiently, but it also means mistakes and security incidents can spread before anyone notices.

1. Accidental File Deletion

An employee may delete a shared folder without realizing other departments depend on it. That deletion can quickly

sync across the cloud and connected devices. Employees may lose access to contracts, customer records, project files, or financial documents. Work slows down while the team tries to determine what was deleted and whether it can still be recovered.

2. Overwritten Files

Someone may replace the correct version of a document with an incomplete or outdated copy. By the time the mistake is discovered, the original version may be difficult to locate. Employees may spend hours searching through email attachments, downloads, and file histories. Meanwhile, customer work, billing, or important decisions may be delayed.

3. Ransomware on Synced Files

Ransomware can encrypt files on an employee's computer. When those files are connected to cloud storage, the encrypted versions may sync to Microsoft 365 or Google Workspace. Without a separate, clean backup, the business may lose access to project documents, customer information, and other critical records.

4. Expired Retention Periods

Cloud platforms may retain deleted or changed data for a limited amount of time. Once that retention period expires, recovery can become difficult or impossible. A missing file can create significant problems when it affects compliance, payroll, legal matters, customer service, or project delivery.

5. Incorrect Permissions

A permissions error can prevent employees from accessing the information they need. It can also expose sensitive files to people who should not have access. Both situations create risk. Employees lose time, managers get pulled into troubleshooting, and the business may face security or compliance concerns.

These challenges affect organizations across Central Texas.

A Cloud Backup Strategy Protects More Than Files

A reliable cloud backup strategy helps protect productivity, customer service, security, and business continuity. The goal is not simply to create another copy of your data. Your backup system should allow your business to recover the right information quickly and confidently.

Celebrate August Birthdays at CTTS!



JOSH



MICHELLE

What AI Can't Do When Your Systems Go Down



It's 4 a.m., and an alert wakes you up. A critical system is down.

Your AI monitoring platform detected unusual activity, triggered an alert, and notified the right people. The technology worked exactly as expected.

Now comes the harder question: What happens next?

AI can detect problems quickly, but it cannot guarantee your data can be restored, rebuild a failed server, or get employees back to work. That depends on the recovery systems and plans you put in place before the alert arrives.

Detection Is Not Recovery

Modern monitoring tools can identify failed hardware, suspicious logins, network problems, and backup errors faster than a person could. That visibility is valuable, but detection and recovery are not the same thing.

Think of AI monitoring like a fire alarm. It can warn you about danger, but it cannot put out the fire or restore what was damaged.

When ransomware locks files or a server fails, AI may tell you what happened. It cannot decide which systems should be restored first, how employees will continue working, or how customers should be notified.

Those decisions must be made in advance.

Downtime Affects Every Part of the Business

When a critical system goes down, employees may lose access to email, shared files, accounting software, scheduling systems, and customer records.

The impact varies by industry. AI can alert these organizations to a problem. It cannot keep the business running while recovery is underway.

A Tested Recovery Plan Is the Real Safety Net

Businesses that recover quickly are not always the ones with the most expensive tools. They are the ones that have prepared and tested their response.

Without a tested plan, leadership is forced to make important decisions during the crisis.

A Backup Is Only Useful If It Can Be Restored

Many businesses assume they are protected because they have backups. That assumption can create a false sense of security.

Backups may be incomplete, corrupted, outdated, or inaccessible during a cyberattack. A successful backup notification does not always mean a successful recovery is possible.

The only dependable way to know whether a backup works is to test a restoration.

Businesses should know what is being backed up, where copies are stored, how they are protected, and how long a full recovery would take.

Prepare Before the Alert Arrives

CTTS helps organizations identify critical systems, test backups, document recovery procedures, clarify responsibilities, and fix weaknesses before they cause extended downtime.

The goal is not simply to detect problems. It is to keep your business operating with as little disruption as possible.

A smarter alarm is valuable, but only when your business is ready to respond.

Schedule a discovery call with CTTS to review your recovery strategy and find out whether your systems, backups, and response plan are truly ready.