



CTTS TECH TALK

YOUR TECHNOLOGY NEWSLETTER

SEPTEMBER 2026



JOSH



SARA



KURT



MICHELLE



CHAIM



KEN



EVAN



KURT



CORNELIUS



SARONNA



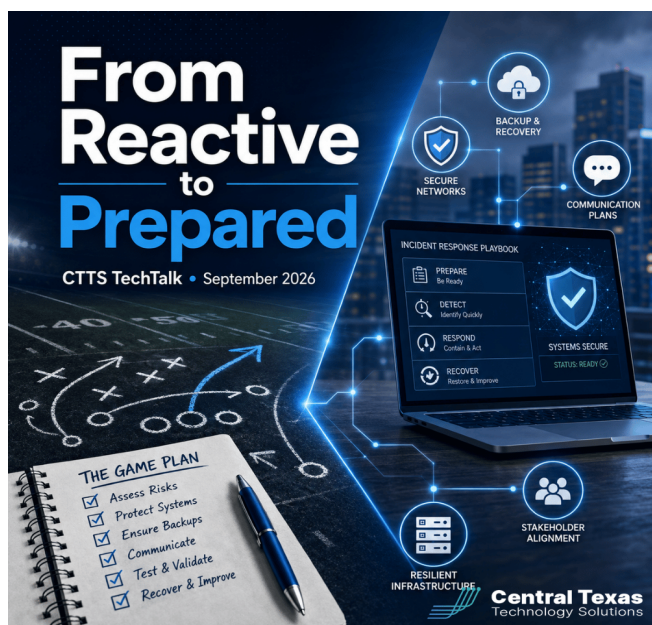
ALEX



JENNY



DANNY



Technology problems become business problems when teams are forced to make critical decisions under pressure.

A cyberattack, outage, or system failure can expose unclear responsibilities, weak communication plans, untested backups, and uncertainty about what needs to be restored first.

Inside this issue, we look at how to move from reactive to prepared. You will learn what every incident response plan should include, which recovery mistakes create the biggest risks, and why preparation often determines how quickly a business recovers.

The goal is simple: build your playbook before you need it. A proactive approach to IT starts with knowing where your gaps are before an emergency finds them.

INSIDE THIS ISSUE

TECH NOTES



The Game Is Won Before Kickoff

PAGE 2

ADVANCED TECH



6 Things Every Incident Response Plan Needs

PAGE 3

BIZTECH



The Recovery Mistakes That Cost Small Businesses the Most

PAGE 4



TECH NOTES FROM JOSH WILMOTH

The Game is Won Before Kickoff



From the Desk of Josh Wilmoth

"Everybody has a plan until they get punched in the mouth."

Mike Tyson said that about boxing, but after 24 years of leading CTTS, I can tell you it applies just as well to business technology.

September means football is back in Central Texas. Friday night lights in Georgetown, tailgates in Round Rock, and watch parties from Austin to Cedar Park. And here is what every good coach knows: the game is not won on Friday night. It is won in the practices nobody sees.

The past month handed us three reminders of why that matters.

On July 28, American Airlines suffered a technology issue that triggered a nationwide ground stop. Every plane that was not already in the air sat on the tarmac. Here is the part worth noticing: they were back up in about 45 minutes. That is not luck. That is an organization that knew exactly who does what when things break.

Closer to home, Nutex Health, a hospital operator that runs emergency facilities right here in Texas, told the SEC on

August 24 that attackers had gotten into its servers and taken data. Weeks into the investigation, the company still could not say exactly what was stolen. Patient records? Employee files? Financials? They are still finding out.

And in one of the strangest incidents I have seen in a while, a ransomware group hit the AnMed health system, stole what they claim was six terabytes of data, and then posted their ransom demands on the hospital's own Facebook page. Think about that. While leadership scrambled to respond, the criminals were running the hospital's public communication channel.

Three organizations. Three very different outcomes. One difference: preparation.

These were not small operations with no IT budget. These were billion dollar companies with security teams. The punch in the mouth is coming for all of us eventually. The only question is whether your team knows the next play when it lands.

So here is my challenge to you this month. Ask yourself three questions. If your systems went down tomorrow morning, who is in charge of the response? If email and phones are part of what went down, how does your team communicate? And which system has to come back first for you to keep serving your customers?

If you answered all three without hesitating, congratulations. You are ahead of most businesses in Central Texas. If you hesitated on even one, you are exactly who I wrote this for, and the rest of this issue will show you how to close those gaps.

You have worked too hard building your business to let one bad morning undo it. Let us make sure your playbook is ready before the season gets interesting.

Schedule a free strategy session with CTTS. It costs you nothing but an hour, and it might save you a season.

Josh Wilmoth
President and CEO, CTTS

P.S. I asked our helpdesk team why the football team's server never goes down. They said it has the best backup quarterback in the league. I promise our actual backup strategies are better than our jokes.

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

ADVANCED TECH

6 Things Every Incident Response Plan Needs



Every business hopes it will never face a cyberattack, outage, data breach, or other major disruption.

But hope is not what determines how well a business recovers. Preparation does.

A strong incident response plan gives your team clear instructions before the pressure is on. Here are six things every plan should include.

1. Roles and Responsibilities

Decide who will lead the response, communicate with employees, coordinate with your IT provider, contact customers and vendors, and make important business decisions.

Clear responsibilities prevent confusion and delays.

2. Emergency Contact Information

Keep current contact information for:

- Leadership
- Your IT provider
- Software and technology vendors
- Cyber insurance
- Legal counsel
- Key business partners

Make sure the list is available even if your network or email is offline.

3. Communication Procedures

If email or Teams stops working, how will employees communicate? Establish backup communication methods and determine who is responsible for updating employees, customers, vendors, and other stakeholders.

4. Critical Systems and Priorities

Not every system needs to be restored at the same time. Identify the applications, systems, and processes your business cannot operate without. Establish the order in which they should be recovered and how much downtime is acceptable.

5. Recovery Procedures

Give employees and leadership clear steps for reporting incidents, escalating problems, containing threats, restoring systems, communicating progress, and returning to normal operations. The goal is to eliminate guesswork when time matters most.

6. Testing and Review

Your business changes, and your incident response plan should change with it.

Regularly review contact information, recovery priorities, procedures, and backups. Conduct tabletop exercises so employees can practice responding to realistic scenarios. Testing often reveals gaps that look fine on paper but fail in practice.

Be Ready Before It Happens

The most effective incident response plans are not created during an emergency. They are built beforehand and updated as the business evolves.

Healthcare organizations, legal firms, professional services companies, construction businesses, manufacturers, and nonprofits all depend on technology differently, but they share the same challenge: when critical systems stop working, the business needs a clear path forward.

CTTS helps businesses prepare before an incident forces them to make important decisions under pressure.

Not sure whether your incident response plan covers the essentials? Schedule a 10-minute discovery call with CTTS and let us help you identify the gaps.



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

BIZTECH

The Recovery Mistakes That Cost Small Businesses the Most



The best football teams do not just prepare for the game. They prepare for what happens when the game plan falls apart. Businesses should do the same.

A cyberattack, outage or system failure can expose recovery gaps that are easy to overlook when everything is working normally. Here are five mistakes that can make a manageable disruption much worse.

1. Assuming backups are enough

Backups help recover data, but they do not tell your team what should be restored first, who is responsible or how quickly systems need to return.

Recommendation: Document your recovery priorities, sequence and responsibilities.

2. Not testing the recovery plan

A plan may look good on paper and still fail when you need it. Testing can uncover bad backups, outdated instructions, missing applications and recovery times that are longer than expected.

Recommendation: Test your plan at least annually and after major technology changes.

3. Not defining roles

When an incident occurs, someone needs to make decisions quickly. If nobody knows who is responsible, valuable

recovery time can be lost.

Recommendation: Decide who leads, who contacts IT, who communicates with employees and when issues should be escalated.

4. Forgetting about communication

Employees, customers and vendors may all need information during a disruption. Your normal email or phone system may also be unavailable.

Recommendation: Establish backup communication methods and assign someone to provide updates.

5. Treating recovery planning as a one-time task

Employees change. Systems change. Vendors change. Your recovery plan needs to change with them.

Recommendation: Review the plan regularly and whenever significant changes are made to your people, technology or operations.

Recovery Favors the Prepared

Whether you operate a healthcare practice, law firm, professional services company, construction business, manufacturing operation or nonprofit, a tested recovery plan can reduce confusion, minimize downtime and help your team make better decisions under pressure.

CTTS helps businesses throughout Austin, Georgetown, Round Rock, Cedar Park and Central Texas identify recovery gaps before they become emergencies.

Not sure your recovery plan is ready? Schedule a 10-minute discovery call with CTTS today. (512) 388-5559.

Celebrate September Anniversaries at CTTS!



JOSH



SARA



KURT



KEN



CORNELIUS