# CTTS TECH TALK

## YOUR TECHNOLOGY NEWSLETTER

JULY 2026


JOSH


SARA


KURT


MICHELLE


CHAIM


KEN


EVAN


KURT


CORNELIUS


SARONNA


ALEX


JENNY


DANNY


**The biggest risks in business are often the ones no one is watching closely enough.**

**A trusted vendor has access. A backup has not been tested. A payment request looks routine. An IT conversation gets pushed to the next quarter. None of these feels urgent in the moment, but each one can create real exposure if the fundamentals are not being checked on purpose.**

**Inside this issue, you will find guidance on reviewing vendor access, asking better questions during quarterly IT conversations, spotting hidden cybersecurity risks, and making sure your team knows how to slow down when something feels off.**

**The goal is simple: help your business stay secure, productive, and prepared by paying attention to the risks that are easiest to overlook.**

## INSIDE THIS ISSUE

### TECH NOTES



### ADVANCED TECH



### BIZTECH



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

# TECH NOTES
# FROM JOSH WILMOTH

## Three Million Texans Just Got a Hard Lesson From a Vendor They Never Met


**"Almost nobody gets beaten by brilliance anymore. They get beaten on the fundamentals they quit checking." Josh Wilmoth, CTTS**

If you bought a hunting or fishing license in Texas, you may want to check your credit this month.

In mid June, the Texas Parks and Wildlife Department announced that the outside company handling its license sales had been breached. The exposure included driver's license numbers, passport numbers, and contact details for more than 3 million hunters and anglers.

The state's own systems were fine. Texas did not get hacked in the way most people picture it. A vendor most of those people had never heard of became the weak spot. That is the part every business owner should pay attention to.

Most people hear a story like that and picture a hooded genius in a dark room running code they could never understand. Then they quietly decide there was nothing they could have done anyway.

That feeling is dangerous because it is wrong.

**It Is Not Just State Agencies**

The same kind of problem is showing up everywhere.

A prediction market called Polymarket reportedly lost millions after attackers used a third party vendor breach to place malicious code on its site. Nintendo also had employee data exposed through an outside survey tool, while its own gaming systems were not compromised.

Different industries. Same story.

**The Word Underneath All of It**

Sit with these stories long enough and they collapse into one word - **Fundamentals**.

A vendor connection nobody reviewed. A payment change nobody verified. A login nobody questioned. A backup nobody tested.

That is not master criminal work. That is a skipped step.

The attackers did not get smarter this summer. They just kept betting that the rest of us would stay distracted.

So far, that bet keeps paying.

The good news is that if the problem is fundamentals, the problem is fixable. You do not have to outsmart a genius. You have to stop beating yourself.

**How CTTS Helps**

This is the work CTTS does quietly in the background for businesses across Central Texas.

Most importantly, we sit down with you on a regular rhythm so the fundamentals get checked on purpose, not by accident after a breach.

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

P.S. I will admit something. The one summer I remembered to buy my fishing license early instead of in the truck on the way to the lake is the summer the license data gets breached. There is probably a lesson in there about doing the right thing at the right time, but mostly I am impressed the universe waited until I was being responsible. If you got the credit monitoring letter too, welcome to the club. Our official summer hobby is now refreshing our credit reports. The bass were not biting anyway.

# ADVANCED TECH

## 6 Questions Smart Companies Ask Their IT Provider Every Quarter


If you are only talking to your IT provider when something breaks or when your contract is up for renewal, your business may be missing important warning signs.

The right IT provider should not just fix problems after they happen. They should help you prevent downtime, reduce risk, improve productivity, and plan ahead with confidence. Here are six smart questions every business should ask its IT provider each quarter.

**1. What Security Problems Do We Need to Address?**

Every business has vulnerabilities. The key is knowing whether your IT provider is actively finding and fixing them before they become costly.

Ask whether systems need security patches, whether there have been unusual login attempts, and whether users, devices, or processes are creating unnecessary risk.

**2. Have You Tested Our Backups Recently?**

A backup is only valuable if it works when you need it. Ask when the last recovery test was completed, how long restoration would realistically take, and whether your backups are stored securely away from your main systems.

**3. Where Is Our Technology Slowing Us Down?**

Not every IT problem is an emergency. Some problems quietly slow your team down every day.

Ask your provider where performance issues are showing up, what systems generate the most complaints, and what should be optimized or replaced.

**4. Are We Still Compliant With Industry Regulations?**

Compliance is not a one-time project. Requirements can change, documentation can fall behind, and employee habits can create gaps.

Ask whether any compliance expectations have changed, whether your policies are current, and whether your team needs additional security training.

**5. What Should We Be Budgeting For Next Quarter?**

Good IT planning helps eliminate surprise expenses. Your provider should be tracking aging hardware, expiring warranties, software renewals, infrastructure needs, and security investments worth planning for.

Quarterly reviews give you time to spread out costs, make smarter decisions, and avoid emergency purchases.

**6. Where Are We Falling Behind That Leaves Us Exposed?**

This question helps separate a reactive IT vendor from a strategic IT partner.

Ask whether there are new tools, automations, security protocols, or technology improvements your business should consider. Also ask what other businesses your size are doing that you are not.

If your IT provider does not have clear answers to these questions, or if they are not offering to meet with you regularly, you may not be getting the support your business needs.

Your company needs more than someone who responds when things break. You need a proactive partner who helps prevent problems, protect your data, improve productivity, and align technology with your business goals.

### July Employee Anniversaries at CTTS!

**KURT RINEAR**

# BIZTECH

## The Most Dangerous Risks in Your Business Don't Swim on the Surface


On the surface, everything may look calm.

That is what makes Shark Week so fascinating. The danger is not always visible. It is often moving quietly underneath. Cybersecurity works the same way. The most dangerous threats facing businesses today are often designed to blend in with normal operations until money moves, systems go down, or sensitive information is exposed.

During the summer months, the risk can increase. Employees travel. Schedules shift. Key decision-makers may be out of the office. Temporary stand-ins may approve requests they do not normally handle. Cybercriminals know this, and they use the distraction to their advantage.

Here are three risks that may already be circling beneath the surface.

**1. Fake Invoices and Vendor Impersonation**

Attackers do not always need to hack your systems. Sometimes, they only need to send one believable email.

This is often called business email compromise. A cybercriminal impersonates a vendor, supplier, executive, or trusted contact and asks your team to approve an invoice, update payment instructions, or send money quickly.

The email looks normal. The request sounds reasonable. The timing feels urgent. By the time anyone realizes the request was fake, the money may already be gone.

**The solution is simple:** create a verification process for every financial request received by email. If a vendor changes payment instructions or someone requests an urgent transfer, confirm it using a known phone number already on file. Do not use the number or link inside the suspicious email.

**2. Phishing Attacks That Target Distracted Employees**

Phishing works because people are busy. A team member sees a password reset email and clicks the link. Someone receives a text that looks like it came from IT. A manager gets an urgent approval request right before a meeting. Nobody stops to verify because stopping feels like losing time. That is what attackers count on.

Speed is a weapon attackers use against your business. Slowing down is how your team takes that weapon away.

**3. Third-Party Risks That Travel Fast**

When a vendor with access to your systems is compromised, the threat may not stay contained to them. It can move directly into your business through the connection they already have.

This is called third-party or supply chain risk.

Many businesses have more exposure than they realize. Software providers, cloud tools, copier vendors, phone providers, contractors, and former employees may still have access that no one has reviewed in months.

**CTTS Helps You See What Is Beneath the Surface**

The biggest cybersecurity risk is assuming everything is fine because nothing appears broken.

CTTS helps businesses in Austin, Round Rock, Georgetown, Cedar Park, and across Central Texas move from reactive IT support to proactive protection.

**If you are not sure what risks are hiding beneath the surface, schedule an IT assessment with CTTS today.**

Central Texas
Technology Solutions

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