CTTS TECH TALK

YOUR TECHNOLOGY NEWSLETTER

May 2025


JOSH


SARA


KURT


MICHELLE


CHAIM


KEN


EVAN


KURT


WILSON


NICHOLAS

Cloud computing has completely transformed the way businesses operate, offering incredible flexibility, scalability, and efficiency. But as your business moves more operations to the cloud, security can no longer be an afterthought.

Imagine a luxury high-rise with no security guard at the front door; anyone could walk in unnoticed. Without strong cloud security, your business faces the same risk: leaving sensitive data wide open to cyber threats.

At CTTS, we believe you should be able to take full advantage of the cloud without worrying about vulnerabilities. In this month's Technology Newsletter, we'll show you what it takes to keep your cloud environment secure, so you can focus on growing your business with confidence.

INSIDE THIS ISSUE

TECH NOTES

What I Learned from That Client Who Waited Too Long

PAGE 2

ADVANCED TECH

What Every Business Owner Should Know About Cloud Protection

PAGE 3

BIZTECH

The Convenience of the Cloud Comes with Hidden Costs

PAGE 4

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

TECH NOTES
FROM JOSH WILMOTH

What I Learned from That Client Who Waited Too Long

Back in 2014, CTTS was called into a large professional services firm in downtown Austin. Longstanding organization. Great people. Outdated technology.

Their IT environment was being run on **Novell NetWare** and **GroupWise**—which, even back then, was like using a rotary phone in a smartphone world. We saw immediate risks and put together a full modernization proposal. But the decision was sent to the Board of Directors… and that's where things stalled.

They said they'd "circle back next quarter."

While the board debated, the inevitable happened. An intern opened an innocent-looking email that contained a ransomware payload. Within minutes, the intern's machine was encrypted. Then the file server running on ancient NetWare went down too—*and they had zero backups*. Years of client data, legal records, financials—gone.

We were in full damage-control mode. And because it was 2014, there wasn't exactly a Bitcoin ATM around the corner. I had to drive to **Walmart**, wire money to a sketchy exchange, and wait while we jumped through hoops to secure just $500 worth of bitcoin. That's how we paid the ransom.

CTTS was eventually able to unencrypt the files and build version 1.0 of their new file system and email server—the same one they still use today. But it cost them.

- **The delay cost them over $100,000 in legal cleanup.**
- **They lost access to critical documents for two weeks.**
- **Client trust took a hit.**
- **And every new upgrade after that had to be rushed and reactive.**

I'll never forget what the Chairman of the Board told me a few months later:

"We thought waiting would give us clarity, but it just bought us disaster."

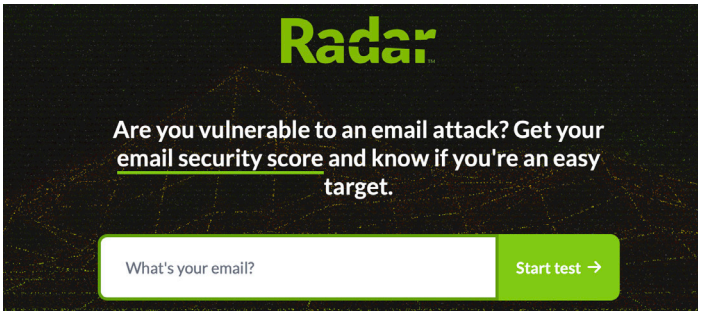
That stuck with me. And I see versions of this same story play out even today. Businesses wait to modernize their cloud setup. They wait to add proper backups. They wait to enforce MFA. Until something breaks—and suddenly, the budget appears.

Look, I understand boards, budgets, and bottlenecks. But in 2025, waiting too long isn't strategic—it's risky.

If it's been a while since you've reviewed your cloud security or backup strategy, **don't wait** until something breaks. Let's talk through your current setup and make sure it's keeping up with your business.

Call me today at (512) 388-5559 to schedule your next Quarterly Business Review.

We'll keep you ahead of the game—and out of Walmart's wire transfer line.



At CTTS, we've helped hundreds of businesses across Central Texas secure their email systems, and one thing we know for sure: what you don't know about spam protection can hurt you.

Run Your Free Email Security Test Today:
https://ctts.email.security/radar

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

ADVANCED TECH

What Every Business Owner Should Know About Cloud Protection

Running a business today without using the cloud is a bit like trying to compete in Formula 1 with a tricycle. The cloud gives us flexibility, scalability, and efficiency we could only dream of a few years ago. But—like a lot of good things—it also comes with risks that many business owners either don't realize or mistakenly think someone else is handling.

Here's the reality: cloud protection isn't just your provider's job. It's a shared responsibility. And in 2025, with cyberattacks growing faster than AI-generated deepfakes, understanding your role has never been more important.

The Biggest Myth About Cloud Security

There's a dangerous myth out there: "Once my data is in the cloud, it's safe."

I wish it were that easy. The truth is, cloud providers like Microsoft, Amazon, and Google are responsible for securing the foundation—the infrastructure, servers, and networks. But your data, your applications, your user access? That's firmly on you.

Think of it like renting a high-end office suite. The building provides locks, security guards, and maybe even a fancy coffee bar. But if you leave your office door wide open with your files spread out on the conference table, well… that's not their fault.

Your Role in Cloud Protection

If you're not actively managing your part of the cloud, you might be leaving the front door wide open without realizing it. Here's where most businesses need to pay attention:

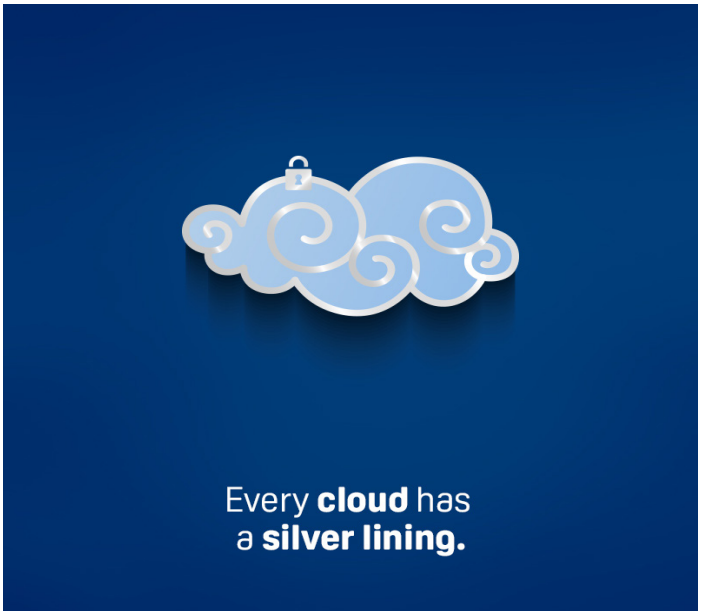
Your Data: Encrypt it. Protect it. Back it up somewhere other than the same cloud it's stored in. (And yes, that still matters even if you "trust the brand.")

Your Applications: Keep your Microsoft 365, Google Workspace, and other tools updated. Monitor who's logging in, from where, and why. If you wouldn't let a stranger walk into your office and use your desk, don't let unknown devices connect to your cloud apps.

Your User Credentials: Password123 isn't a strategy. Strong passwords, multi-factor authentication (MFA), and limited access rights are your best friends.

Your Configurations: Misconfigured cloud settings are one of the biggest causes of breaches today. Make sure your storage isn't "accidentally public," your alerts are turned on, and your old employee access is cleaned up faster than leftover office birthday cake.

The Good News: You Don't Have to Figure This Out Alone



A strong cloud protection strategy doesn't have to be complicated or expensive. You just need a partner who knows what they're doing and cares about your business like it's their own.

That's where CTTS comes in. We work with CEOs and business owners across Central Texas every day to:

- Identify gaps in your current cloud environment
- Implement the right security practices tailored to your needs
- Monitor and manage your cloud so you can focus on growing your business (and maybe getting that round of golf in once in a while)

When you know exactly where your responsibilities begin and end, you take back control. You don't just "hope" you're protected—you know you are.

Let's Get Your Cloud Strategy Locked Down

The worst time to find out you have a security gap is after an attack. (Kind of like realizing you forgot to pack the sunscreen once you're already burnt to a crisp at the beach.)

Let's fix it before it becomes a problem. Schedule a free, no-obligation cloud security review with CTTS today.

We'll make it simple, clear, and actionable—because protecting your business shouldn't be rocket science.

Call (512) 388-5559 or visit CTTSonline.com to schedule your review.

BIZTECH

The Convenience of the Cloud Comes with Hidden Costs

When you first moved your business operations to the cloud, you probably felt a little like you'd discovered the secret to working smarter, not harder. Faster deployments, easier collaboration, and the ability to scale without needing a room full of servers—it delivered exactly what it promised.

But now that cloud use is standard for just about every business, a new reality is sinking in: convenience sometimes comes with hidden risks. And in 2025, where ransomware attacks are predicted to hit a business every 11 seconds, cloud security can no longer be an afterthought.

Why Cloud Security Deserves More of Your Attention

It's easy to assume cybercriminals are out to target the big names you see on the news. But the truth is, hackers aren't chasing Fortune 500s—they're chasing opportunities. And smaller businesses, especially those using the cloud without strong security practices, are often the path of least resistance.

If your cloud environment isn't locked down, you could be exposing your business to:

- **Data breaches:** Sensitive customer, financial, or proprietary data could be stolen or leaked.
- **Account hijacking:** Weak or recycled passwords make it easy for bad actors to impersonate legitimate users.
- **Misconfigured settings:** One wrong permission or an open port could leave your entire infrastructure vulnerable.
- **Insider threats:** Accidental mistakes—or intentional misuse—by employees can create massive security gaps.

And with hybrid work environments here to stay, protecting your cloud isn't just important—it's essential.

The Misunderstanding That Could Cost You

A lot of CEOs and business owners assume that if they're paying Microsoft, Google, or Amazon for cloud services, the security piece is "baked in." Unfortunately, that's only partly true.

Cloud platforms operate under something called the shared responsibility model:

- The provider secures the infrastructure (servers, storage, networking).
- **You** are responsible for securing your data, managing user access, and ensuring apps are protected.

Think of it like leasing a car. They hand you the keys, but it's still your job to lock the doors, drive safely, and park it somewhere smart.

How to Build a Strong Cloud Security Foundation

Cloud security isn't about doing everything all at once—it's about doing the right things consistently. Here's a short list to get you moving in the right direction:

- **Encrypt your data:** Both in transit and at rest. Make it unreadable without the right encryption keys.
- **Use strong identity and access management:** Limit access based on roles, require multi-factor authentication (MFA), and regularly review permissions.
- **Conduct regular security audits:** Don't wait for a crisis to find out what's wrong. Routine checks can catch vulnerabilities early.
- **Stay compliant:** Regulations like HIPAA, PCI, and GDPR are only getting stricter. Falling behind could cost you more than money—it could cost your reputation.
- **Have an incident response plan:** Know exactly who will do what if an attack happens. Quick action can mean the difference between inconvenience and disaster.
- **Keep reliable backups:** Don't trust your cloud provider alone with your data. Have offsite backups ready so your business can bounce back fast if needed.

Consistency Is the Secret Weapon

The good news? Cloud security doesn't have to be complicated. You don't need a battalion of cybersecurity engineers or a seven-figure budget. What you do need is consistency, clarity, and a trusted partner who can make sure nothing falls through the cracks.

That's where CTTS comes in. We specialize in helping businesses like yours secure their cloud environments without slowing down innovation or adding unnecessary complexity. We'll help you spot hidden risks, build a strategy around your business goals, and keep your team protected while you keep growing.

Let's Strengthen Your Cloud Security Before It's Tested

Cyberattacks aren't slowing down in 2025. And waiting for a "wake-up call" could cost you dearly.

Let's get ahead of it together.

Call (512) 388-5559 or visit CTTSonline.com today to schedule your free Cloud Risk Review.

Central Texas
Technology Solutions