CTTS TECH TALK

YOUR TECHNOLOGY NEWSLETTER

DECEMBER 2025

JOSH

SARA

KURT

MICHELLE

CHAIM

KEN

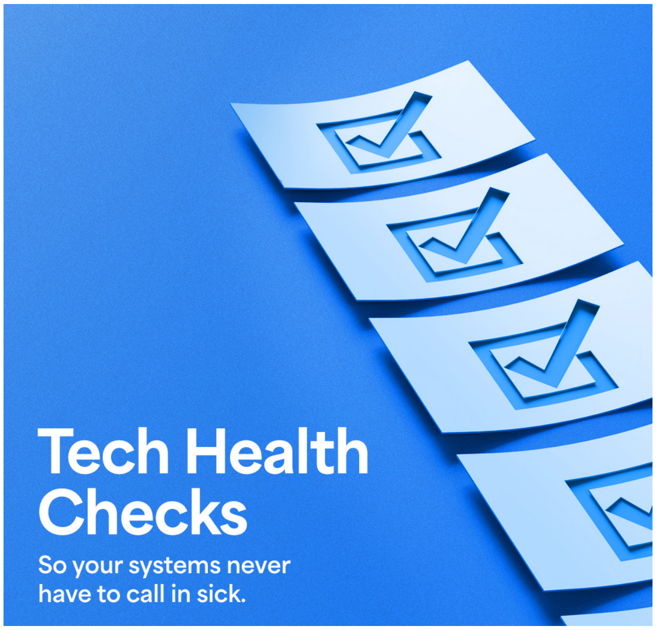
EVAN

KURT

CORNELIUS

LANG

SARONNA



Technology works best when it is regularly checked, tuned, and aligned with your goals. Yet many organizations move into the new year without realizing their systems are running slower, less securely, and with more risk than they can see on the surface.

In this month’s Tech Talk, we are focusing on Tech Health Checks and why they are one of the smartest ways to protect performance and strengthen security. Inside, you will find insights on the dangers of neglected technology, the financial impact of reactive repairs, and the blind spots attackers often rely on.

With a clear view of your technology’s health, you can enter 2026 confident that your systems are ready to support your goals instead of slowing them down.

INSIDE THIS ISSUE

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

TECH NOTES
FROM JOSH WILMOTH

The One Thing Most Leaders Skip Before the New Year

"If you don't schedule maintenance, your systems will schedule it for you."

December is the month when everyone promises next year will be more organized, more efficient, and less stressful. New goals. New plans. New priorities.

But there's a pattern I see every single year.

Business leaders focus on strategy, revenue, staffing, and growth...while their technology quietly limps across the finish line.

Slow systems. Missed updates. Security gaps. Backup processes nobody has tested since Easter.

Everything appears to be "working" — until it suddenly isn't.

That's the danger zone.

Your technology doesn't usually fail loudly. It fails slowly. And by the time it gets your attention, the damage is already expensive. That's why one of the smartest things you can do before 2026 begins is one simple move: schedule an IT Health Check.

Not because something is broken.

But because success depends on what you don't see.

This year alone, we've seen organizations lose productivity from aging equipment, struggle with outdated permissions that created security holes, and discover backups that had been quietly failing for months. None of those leaders thought they were at risk. They just hadn't looked closely enough.

A true IT Health Check isn't about scare tactics. It's about clarity.

We evaluate how your systems perform day-to-day, where security vulnerabilities are hiding, whether backups are actually recoverable, and how well your current technology supports your 2026 business goals. No fluff. No jargon. Just real insight into what's helping you grow and what's holding you back.

The healthiest organizations are proactive, not reactive. They know where they stand. They budget intentionally. They upgrade strategically. And they sleep better at night.

That's the common thread between strong tech health, strong security, and strong growth.

Technology that's healthy performs better, costs less, and scales cleaner. Technology that's neglected becomes expensive, unpredictable, and risky.

At CTTS, we help business owners across Central Texas keep their systems aligned with how they actually operate — not how they operated three years ago. Our Tech Health Checks uncover blind spots, improve performance, and create a clear roadmap so your IT supports your vision instead of limiting it.

Here's my ask before you unplug for the holidays: Schedule your CTTS Tech Health Check now, while calendars are still sane and before 2026 starts demanding your attention.

Call (512) 388-5559
Visit CTTSonline.com
Or email me at Josh.Wilmoth@CTTSonline.com — I'll take care of it personally.

Let's make sure your technology is ready for the goals you're setting, not just surviving the year you've finished.

P.S. If your IT strategy is "If it ain't broke, don't fix it," just remember... that's also how people end up stranded on the side of I-35 with smoke coming out of the hood.

ADVANCED TECH

The Hidden Cost of Ignoring Tech Health

Every business leader understands the value of technology. It keeps teams productive, drives customer experiences and supports mission critical operations. Yet many organizations across Austin wait until something breaks before paying attention to their tech health. The result is higher costs and greater risk than if issues were handled proactively.

The real danger is that most technology problems stay invisible for a long time. Systems seem to be working, teams adapt to slowdowns and small errors go unnoticed. Then one unexpected outage or cyber incident brings work to a halt. Instead of building momentum and staying competitive, the business becomes reactive and expensive repairs become unavoidable.

Proactive IT support is not just maintenance. It is one of the smartest financial decisions a growing organization can make.

The True Cost of Ignoring Tech Health
Businesses often underestimate how much money and reputation are on the line when IT systems are neglected. The cost of doing nothing is rarely zero. It typically becomes one of the most expensive decisions a company ever makes.

Financial Losses From Poor Tech Health
Neglect creates financial risk at every level. Common costs include:

- Lost productivity during downtime when systems fail without warning
- Cyberattack and breach expenses due to unpatched vulnerabilities
- Regulatory fines for missing compliance requirements such as HIPAA
- Emergency repair costs that exceed the price of ongoing support

Security Threats That Grow Over Time
Ignored systems become easy targets for attackers. When security is not monitored, the business faces:

- Data theft from outdated software and unsecured devices
- Unauthorized access to old accounts and unmonitored user privileges
- Malware spreading across unprotected workstations and servers

Operational Setbacks Caused by Weak Tech Health
It is easy to overlook the day to day friction caused by outdated systems and tools that are poorly maintained. These issues often slow growth, reduce team confidence and weaken collaboration.

How Poor Tech Health Affects Business Operations

- Decreased performance from slow software, limited storage and aging hardware
- Projects delayed or derailed because technology cannot support new needs
- Leadership decisions based on incomplete data due to system blind spots
- Difficulty scaling as the business grows without a reliable IT foundation

Organizations that invest in strong IT health gain a noticeable advantage. Teams work faster, planning becomes easier and leadership can innovate without fear of system failure.

When Tech Health Fails, Your Brand Suffers Too
Customers and partners expect reliable, secure and professional service. A technology mistake can quickly turn into a public issue that impacts trust and reputation.

Brand Damage Caused by IT Neglect

- Loss of confidence after outages or leaked information
- Reduced credibility when the business cannot serve customers quickly
- Market disadvantage when competitors invest in stronger tech strategies

Ready to Improve Your Tech Health?
Do not let silent tech failures turn into costly emergencies. The earlier you take action, the easier it is to prevent financial loss and disruption. Schedule a comprehensive IT health assessment with CTTS today and protect your business before issues become expensive problems.

Central Texas
Technology Solutions

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

BIZTECH

Cybersecurity Blind Spots That Put Austin Businesses at Risk

Every business leader understands how important Cybersecurity is for protecting sensitive data, customer relationships, and long-term growth. Yet the biggest danger often isn't the threat everyone is watching for. It's the routine chores that go undone, the forgotten settings that no one reviews, and the tools that quietly get outdated. Hackers look for these overlooked weaknesses because they rarely get fixed in time, and that makes them the easiest way into a business network.

Austin organizations in Healthcare, Legal, Professional Services, Construction, Manufacturing, and Nonprofits face growing pressure to safeguard their systems. A single overlooked password rule or inactive user account can become the spark that triggers a major breach. The good news is that these blind spots are preventable when they are caught early and managed with discipline.

Cybersecurity Issues That Hide in Plain Sight

What employees ignore, attackers target. Below are common blind spots that often go unnoticed until it is too late.

Cybersecurity Vulnerability: Unpatched Systems and Software

Hackers track patch released vulnerabilities and strike companies that fall behind on updates. Every unpatched system creates a doorway into your network.

Action Steps

- Automate patch management for every device
- Set alerts for outdated or failed updates
- Track patch compliance every month

Central Texas Technology Solutions

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

Cybersecurity Threat: Shadow IT and Rogue Devices

An employee installs a random app. Another connects a personal device to the network. These small actions create big risks, especially if malware remains hidden until the attacker is ready.

Action Steps

- Create clear device and app usage policies
- Scan all network endpoints on a recurring schedule
- Control remote access through a secure solution

Cybersecurity Risk: Weak Access Controls

Giving employees more access than they need increases vulnerabilities. Hackers love over-permissive accounts because they open doors to entire systems.

Action Steps

- Use the principle of least privilege
- Require multifactor authentication company-wide
- Audit access permissions whenever roles change

Cybersecurity Failure: Outdated Security Tools

Security tools age quickly. Antivirus programs, endpoint protection, and detection tools must evolve with new threats. If they are outdated, attackers bypass them easily.

Action Steps

- Evaluate your security stack twice a year
- Retire outdated tools before they become a risk
- Use solutions that detect behavior, not just signatures

Cybersecurity Weakness: Inactive or Orphaned Accounts

When employees leave, unused accounts often remain open for months or even years. Cybercriminals actively search for these forgotten accounts because they are valid and rarely monitored.

Action Steps

- Automate employee offboarding permissions
- Review all accounts quarterly
- Remove accounts immediately after departure

Why Austin Businesses Choose CTTS for Cybersecurity

Finding blind spots is only step one. Fixing them quickly, correctly, and without disrupting your team is what protects your business. CTTS provides structured Cybersecurity services that help you see every risk clearly and close gaps before attackers can exploit them. Our experts work daily with companies across Austin and Central Texas to strengthen their defenses with proven processes and modern security tools.

You deserve confidence in your security strategy. Start with a simple, objective tech health check and discover where your Cybersecurity posture truly stands.