



CTTS TECH TALK

YOUR TECHNOLOGY NEWSLETTER

OCTOBER 2026



JOSH



SARA



KURT



MICHELLE



CHAIM



KEN



KURT



CORNELIUS



SARONNA



ALEX



JENNY



DANNY



It's easy to believe that cyberattacks always involve sophisticated hackers, that trusted employees pose little risk, or that improving security requires expensive new technology. Unfortunately, these misconceptions can leave serious gaps in your defenses.

Inside this issue, we challenge those beliefs. You will learn why legitimate credentials can be more dangerous than a forced break-in, how insider threats can put your business at risk, and six practical cybersecurity improvements you can make today without increasing your technology budget.

The takeaway is simple: Better cybersecurity starts with questioning what you think is already protected. Sometimes the most effective improvements are the ones hiding in plain sight.

INSIDE THIS ISSUE

TECH NOTES



The Breach That Did Not Need a Hacker

PAGE 2

ADVANCED TECH



Your Biggest Cybersecurity Risk
Might Be Inside the House

PAGE 3

BIZTECH



6 Free Cybersecurity Improvements You
Can Make Today

PAGE 4



TECH NOTES FROM JOSH WILMOTH

The Breach That Did Not Need a Hacker



"The most dangerous person on your network is not a stranger. Most days, it is someone with a badge and a password." Josh Wilmoth, President and CEO, CTTS

Two headlines from the past month made me sit up straight at my desk.

CenterPoint Energy, right here in Texas, confirmed in mid-September that a hacker obtained personal information tied to roughly 7.5 million customer accounts. Another campaign hit McDonald's and Vodafone, where an attacker calling himself TheHatman pulled more than two million employee records from Microsoft systems using credentials that were already exposed.

Here is what ties those stories together: In 2026, the break in rarely looks like a break in. It looks like someone logging in like they belong there.

Why The Front Door Matters More Than The Walls

Security researchers reported that password spraying attacks, where criminals try common passwords across large numbers of accounts, increased 155 times compared with last year. One campaign generated more than 81 million login attempts in two weeks.

Many businesses in the study had multi-factor authentication turned on. They just had gaps. A forgotten application. An older sign-in method. An excluded user group. Criminals do not need to defeat all your security. They only need to find the one door you forgot to lock.

Who Still Has a Key?

If someone left your company eight months ago, do they still have access to anything? If a vendor project ended last spring, did someone remove their access?

This is one of the most common gaps we find during security

assessments. It might be a former employee's email account, an administrator account nobody remembers creating, or a password shared among several people. None of that requires a sophisticated hacker. It just requires someone finding it.

The Part That Costs You Nothing

The good news is that many of these risks can be reduced without increasing your technology budget. Enforcing multi-factor authentication everywhere, removing old accounts, and reducing unnecessary administrator privileges are basic security housekeeping. The problem is that housekeeping gets skipped when everyone is busy running the business. Criminals are counting on it.

Three Questions Worth Asking This Week

Before you set this newsletter down, ask your team:

- Do you know exactly who has administrator access to your systems?
- If an employee or contractor left tomorrow, would their access be removed that same day?
- Is multi-factor authentication enabled for every account that touches company data, without exceptions for convenience?

If you answered all three confidently, you are ahead of many businesses we assess. If you hesitated, it is worth taking a closer look.

Why This Matters to Me

I have spent 24 years building CTTS around one idea: Technology should make your business stronger, not be the thing that quietly takes it down.

The businesses hurt worst by security incidents are rarely the ones with no security. They are often the ones that assumed the basics were covered and never checked.

Do not let that be your business.

Schedule a free strategy session with CTTS. We will review who has access to your systems, identify gaps that may cost nothing to fix, and give you a clearer picture of where your business actually stands.

P.S. My wife asked why I was laughing at my laptop last week. I had just found a password on a sticky note in a prospect's server closet. The password was "Password1." The sticky note was labeled "Do Not Share." I have never seen an instruction followed so poorly in my life.

ADVANCED TECH

Your Biggest Cybersecurity Risk Might Be Inside the House



When most businesses think about cybersecurity, they picture an outside hacker trying to break into the network. But some of the biggest risks may already have legitimate access to your systems.

Employees, vendors, contractors, partners, and executives can create cybersecurity risks through malicious actions or simple mistakes.

Insider threats generally fall into six categories.

Data theft occurs when someone removes or copies confidential information without authorization.

Sabotage involves deliberately damaging systems, deleting information, disabling security controls, or disrupting business operations.

Unauthorized access happens when someone views information they do not need for their job.

Negligence and human error include mistakes such as sending sensitive information to the wrong person, clicking phishing links, losing devices, or ignoring security procedures.

Credential sharing creates unnecessary risk because multiple people using the same account makes activity harder to control and track.

Unauthorized AI use is a growing concern. Employees may unknowingly expose customer or company information by entering it into public AI tools that have not been approved by the business.

Warning signs can include unusual access to confidential files, large data downloads, repeated requests for unnecessary permissions, use of unauthorized devices, disabled security tools, or sensitive information being uploaded to unapproved AI platforms.

Businesses can reduce these risks by taking a few practical steps.

- Require strong passwords and multi-factor authentication. Give only the access employees need.
- Review permissions regularly.
- Train employees on cybersecurity and safe AI use.
- Maintain tested backups.
- Have an incident response plan ready before something goes wrong.

These protections matter across healthcare, legal, professional services, construction, manufacturing, and nonprofit organizations because every business depends on people having access to important systems and information.

The goal is not to distrust your employees. It's to make sure a single mistake, stolen password, or compromised account cannot become a major business interruption.

CTTS helps businesses across Central Texas build proactive cybersecurity strategies that protect users, systems, and data before an incident occurs.

Not sure who has access to your systems or how well your business could detect an insider threat?

Schedule a free consultation with CTTS and let us help you identify the gaps before they become problems.

Help Us Celebrate October Birthdays at CTTS!



KEN



KURT

6 Free Cybersecurity Improvements You Can Make Today



Cybersecurity does not always require another product or a bigger budget. Some of the most important improvements involve fixing basic security practices that have been overlooked or applied inconsistently.

Here are six things your business can start improving today.

1. Turn on multi-factor authentication

A password should not be the only thing protecting important company accounts.

Enable MFA for Microsoft 365 or Google Workspace, banking, payroll, cloud storage, remote access and other critical applications. Whenever available, use stronger options such as passkeys, authentication apps, biometrics or security keys.

2. Remove accounts you no longer need

Former employees, contractors and vendors may still have access long after they need it.

Regularly review accounts and remove anything that no longer serves a business purpose. Employee offboarding should always include disabling access to email, cloud applications and company systems.

3. Reduce administrator access

Administrator accounts can install software, change settings

and modify security controls, which makes them especially valuable to attackers.

Give employees only the access they need to do their jobs. Limiting administrator privileges can reduce the damage caused by a compromised account or employee mistake.

4. Turn on automatic updates

Software updates often fix known security vulnerabilities.

Make sure computers, phones, browsers, Microsoft Office, security software and other common applications receive updates promptly. Specialized business systems may require managed testing before updates are installed, but patches should not be ignored indefinitely.

5. Use a password manager

Expecting employees to remember a different complex password for every account is unrealistic.

Password managers can create and store strong, unique passwords while reducing password reuse. Many platforms already include basic password management tools.

6. Test your backups

Having backups is not the same as knowing they will work.

Confirm when your last successful backup occurred, what data is protected and whether someone has recently tested restoring it. You should also know how long recovery would take after an outage, ransomware attack or equipment failure.

Small Changes Can Close Big Gaps

These steps are useful for almost every organization, whether you run a healthcare practice, legal firm, professional services company, construction business, manufacturing operation or nonprofit.

The challenge is making sure these protections are applied consistently. CTTS helps businesses take a proactive approach by finding weaknesses before they become outages, security incidents or expensive recovery projects.

Schedule a 10-minute discovery call with CTTS to identify practical cybersecurity improvements you can make now.



Central Texas
Technology Solutions

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