CST TECHNOLOGY TIMES

NOVEMBER 2026

Insider Tips to Make Your Business Run Faster, Easier and More Profitably

Tech Talk With Lisa

NO CLICK REQUIRED

You can train your employees, warn them about suspicious emails, and remind them not to click on unfamiliar links. But what happens when a cybercriminal doesn't need anyone to click on anything? That is something I want every business owner and municipal leader to understand.

We spend a lot of time talking about phishing emails, fraudulent text messages, and the importance of cybersecurity awareness training. And we should. Employees are an important part of protecting an organization.

But there is another side of cybersecurity that doesn't always get the attention it deserves.

Sometimes, a cybercriminal doesn't need your employees to do anything wrong. They just need to find something in your technology that hasn't been properly secured.

Your Internet Connection Is That Entry Point
Think about all the technology your organization uses every day.

Cont. On Page 5



CST Group Inc.

This monthly publication is provided courtesy of Shawn & Lisa Brown, Owners.

OUR MISSION:

CST Group Inc. is a PROACTIVE technology management firm who's mission it to SECURE, PROTECT and MANAGE technology for Small to Medium Businesses like yours.

The Hidden Side of AI:
Is Your Business Prepared?



AI is changing the way businesses work. It's also changing the way cybercriminals operate.

The same technology helping businesses improve productivity and security is making scams more convincing, phishing emails harder to detect and sensitive data easier to expose when it's used carelessly.

While businesses are using AI to boost security and productivity, cybercriminals are using the same technology to make attacks more convincing.

AI impersonation: Sounding right isn't enough anymore

Video and audio used to help distinguish someone real from someone trying to scam you. Now, AI lets cybercriminals create realistic voice messages, phone calls and videos that make their requests seem legitimate.

Even if you can spot telltale signs of AI-generated content today, those clues are disappearing quickly. Many of the warning signs people once relied on are already outdated.

Instead of depending on employees to detect a fake, establish verification procedures for sensitive requests such as money transfers or account changes.

AI may be able to imitate a person's voice or appearance, but it can't bypass strong security procedures and multi-factor authentication.

AI-generated phishing: Harder to spot than ever

Phishing messages once contained spelling mistakes, grammatical errors and awkward wording that made them easier to recognize. Typos, generic greetings and urgent language became familiar warning signs.

Today, many phishing emails are well written, personalized and difficult to distinguish from legitimate communication. AI has made these scams more polished and convincing than ever before.

Rather than focusing only on how a message looks, pay attention to what it's asking you to do. Don't trust a message simply because it gets the details right.

Shadow AI: Think before you share sensitive data

When employees use AI tools that haven't been approved by the business, they may unintentionally expose sensitive company information to platforms that haven't been properly vetted.

An AI tool can't read every file in your organization on its own, but it won't stop someone from pasting confidential financial reports, customer information or internal business plans into a prompt and asking for help.

Before employees use any AI tool for work, your business should understand how it handles data, where that information is stored and whether it meets your security and compliance requirements.

A good IT partner doesn't tell you to avoid AI. They help you use it confidently by putting the right safeguards, policies and security controls in place, so your business can embrace new technology without creating unnecessary risk.

Your Cybersecurity Needs an Immune System, Not a Medicine Cabinet



Most medicine cabinets tell a story. There's cold medicine left over from last winter, vitamins bought in bulk, half-used bottles of cough syrup and a prescription that should probably have been thrown out months ago.

Cybersecurity can end up looking much the same. A new threat prompts one purchase, an insurance requirement leads to another and a vendor recommendation adds something else. Over time, the more useful question becomes whether your business has the right protections in place and if they're doing what they need to do.

Cyber myth: More tools mean better cybersecurity

It's an easy assumption to make. If one security product adds protection, then adding more should make your business even safer. But that's where the myth starts to break down.

Multiple layers of protection can be valuable, but only when each one serves a clear purpose. Adding another product may address a specific concern, but it can also create unnecessary overlap or additional complexity if no one considers how everything fits together.

What matters is whether the right safeguards are in place, properly managed and working together to address the risks your business faces.

Healthy cybersecurity works like a system

Your immune system isn't a shelf of individual remedies. It's a coordinated system designed to recognize problems and respond to them.

Your company's cybersecurity should work the same way, but for many businesses, the pieces don't always come together that neatly.

Tools get purchased to solve specific problems. Employees receive policies and training. New safeguards are added as risks change or requirements evolve. Each decision may make sense on its own, but over time, those individual pieces can become disconnected from the bigger picture.

That's where coordination matters. The right safeguards should complement each other rather than simply coexist.

Security tools are part of that system, but they're most effective when they work as part of a broader approach that still fits the business's needs.

Give your security a check-up

You don't need to understand the technical details of every cybersecurity product your company uses. But you should be able to get clear answers to a few basic questions.

1. What are we currently using, and why?

Someone on your team or a trusted outside partner should be able to explain what your major security protections do and why they're there. If nobody can give you a clear answer, that's worth looking into.

2. Where do our protections overlap, and where are the gaps?

Overlap isn't automatically a problem. Sometimes layered protection is intentional. What matters is knowing whether your security approach was designed that way or simply grew over time without much coordination.

3. Who is making sure everything is working?

A tool can generate alerts around the clock, but that doesn't help much if nobody is reviewing them or knows what should happen next. The important thing is knowing that someone is responsible for the outcome and paying attention.

4. When did we last reevaluate what we need?

Businesses change. People join and leave, new applications get adopted and teams start working in different ways. Cybersecurity that made sense when it was first implemented may no longer fit the business as it exists today.

Cybersecurity Myth Busters:

6 Things Small Businesses Still Get Wrong



Cybersecurity advice is everywhere, but not all of it is accurate. It's worth taking a step back every so often to separate what you know from what you only think you know.

Some have circulated for so long that it's taken on a life of its own, repeated until it sounds like fact even when it's outdated or wrong.

When bad advice goes unchallenged, it creates blind spots. And blind spots are exactly what cybercriminals look for.

The good news is these gaps are simple to close once you know where they are. Here are six myths we hear regularly from small business owners, along with the truth behind each one.

Myth 1: We're too small for cybercriminals to care about

There is no such thing as a business too small for an opportunistic cybercriminal. It doesn't matter if you're a one-person operation, a small business with a dozen employees or a large corporation. If you have exposed accounts or vulnerable systems, bad actors will take advantage of it. A small business offers valuable data, access to bank accounts or entry points to customers and vendors.

Fact: Hackers choose targets based on opportunity, not size.

Myth 2: Employees will recognize a phishing email

Some myths have circulated for so long that they've taken on lives of their own, repeated until they sound like fact even when they're outdated or wrong.

Thanks to AI, it's become harder to catch a scam email from the text alone. Instead, your team needs to think about sender behavior. For example, ask yourself if the supposed sender would:

- Make an unusual request
- Change payment instructions
- Request sensitive information
- Send a new or unusual login link

If anything seems off, double-check before clicking or responding.

Fact: A convincing email can still be a scam.

Myth 3: MFA fully protects our accounts

Multi-factor authentication (MFA) is important, but it's not invulnerable. Hackers use MFA fatigue to their advantage, counting on employees approving requests out of habit. For example, "prompt bombing" floods your phone with requests in hopes you'll approve access just to get them to stop.

continued on page 4 ...

SHINY NEW GADGET OF THE MONTH

A Webcam That Keeps You in the Frame

OBSBOT Tiny 3 is built for people who move when they present. Its motorized camera tracks the speaker and keeps them in frame during calls, presentations and training sessions. So you can move around the room or step up to a whiteboard without stopping to readjust the camera. It supports 4K video, voice and gesture controls, and dedicated desk and whiteboard modes for more flexible hybrid meetings.



CST Group Is Growing in the Sunshine State!

Big news! We're expanding our reach in the Sunshine State, and we've launched a brand-new Florida website!

We're excited to build new relationships and help more Florida businesses with their I.T. and cybersecurity needs.

Know a business in Florida? We'd love an introduction! Your referrals mean the world to us!

Visit our new website: www.cstgroupfl.com

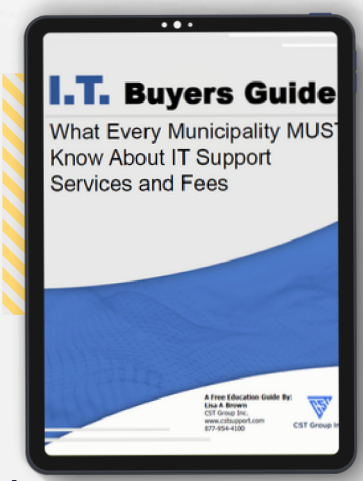


FREE REPORT

What Every Small Business Owner Should Know Before Hiring an IT Provider

Two IT providers can look similar on paper and deliver very different levels of support. Our free IT Buyer's Guide shows you what good IT support should include, where extra costs and gaps can hide and the questions to ask before you sign or renew.

You don't need to be an IT expert.
You just need to know what to look for.



Download your FREE copy today at: https://www.cstsupport.com/itbuyersguide or call our office at (877) 954-4100.

CARTOON OF THE MONTH



"Do you still have regular coffee?"

... continued from page 3

Keep in mind, MFA is a tool, not a shield. Hackers are finding ways to get around weaker authentication methods, which is why MFA needs support from the controls around it.

Fact: MFA should be part of a broader security strategy.

Myth 4: Our backups have us covered

Ask yourself: If your business was hit with a ransomware attack tomorrow, could you restore your data? How long would it take?

A backup is great when you know it's going to work. However, an untested backup isn't something you can rely on during an incident. Knowing how long your business will be down can save you time and money.

Fact: Having backups is not the same as being able to recover.

Myth 5: Cybersecurity is only IT's responsibility

Your IT department does a lot to keep your business safe, but they can't control every click employees make. Cybersecurity decisions happen across every department. It takes only one bad click to open your systems to threats.

Employee security awareness training matters. When everyone knows what to look for and when to ask for help, they become part of your cybersecurity defenses.

Fact: Training employees to make good decisions strengthens your cybersecurity.

Myth 6: We know what to do if something happens

It's Tuesday morning. Several employees suddenly can't access their files. Many teams discover in that moment that nobody has answered the basic questions:

- Should employees shut down their computers?
- Who calls IT?
- What do you do if communication systems are down?
- When does the insurance company get involved?
- Who communicates with customers?

Don't rely on memory in the moment. Have an incident response plan.

Fact: Your recovery plan shouldn't debut during an incident.

Cybersecurity awareness starts with the facts

Strong cybersecurity starts with the facts. Many security gaps come from assumptions that go unchallenged.

If any of these myths sound familiar, it may be time to reassess your cybersecurity strategy. The businesses that stay ahead work with a trusted IT partner to identify gaps, strengthen their defenses and stay ahead of evolving threats.

Tech Talk With Lisa Cont.

You have computers, servers, firewalls, websites, email systems, software applications, and possibly remote access tools. These systems communicate over the internet and every one of them needs to be properly configured, maintained, and updated.

When software becomes outdated, security patches aren't installed, or internet-facing systems are improperly configured, cybercriminals may be able to exploit those weaknesses without ever sending a phishing email.

They don't need someone to open an attachment. They don't need an employee to share a password and from inside your organization, no one will know they are there. They simply need to find a vulnerability they can exploit.

A Recent Reminder: The Security Concerns Surrounding PHP
Recently, we brought attention to security concerns involving PHP, a programming language used behind the scenes by many websites, including WordPress websites.

Most business owners have probably never heard of PHP, and that's understandable. You don't need to know how to program a website to operate a business. But you do need to know that the software running your website requires maintenance and security updates, just like the computers in your office.

When outdated or vulnerable versions of PHP remain in use, attackers may be able to exploit security weaknesses, depending on the specific vulnerability and how the website is configured.

Here is what concerns me. How many organizations actually know what software is running their website, who is responsible for maintaining it, or when it was last updated? That is the bigger issue.

The same concern applies to firewalls, servers, remote access software, and other technology connected to your network.

Patching Isn't Optional
Software manufacturers regularly release updates to correct security vulnerabilities. We call these updates ***patches***. When a vulnerability is discovered, cybercriminals may begin looking for systems that haven't received the necessary updates.

In some cases, automated tools scan internet-facing systems for known weaknesses. This means an organization doesn't have to be specifically targeted to become a victim. It may simply have an exposed system that an attacker discovers.

While installing updates is important, it isn't enough to assume everything is protected simply because someone says the patches are being done. Someone needs to verify that updates were successfully installed, identify systems that failed to update, and address software that is no longer supported. That is what CST does for you!

A Firewall Is Important, But It Isn't a Complete Solution
A properly configured and maintained firewall is an important part of protecting your network which is why CST requires this equipment. It helps control traffic entering and leaving your organization and can reduce exposure to unauthorized connections.

But simply having a firewall doesn't mean your organization is secure. Firewalls require updates, monitoring, appropriate security settings, and regular reviews. A firewall cannot automatically correct every vulnerability in an application or website that is intentionally accessible from the internet.

Security requires multiple layers of protection working together.

You Can't Protect What You Don't Know You Have.
This is one of the biggest concerns I see when we begin working with a new organization. There is often technology in place that nobody has documented.

Maybe it's an old server that still runs an important application. Maybe it's a website maintained by a company nobody has spoken with in years. Maybe it's a remote access tool installed by a previous IT provider. If nobody knows it exists, who is making sure it is secure?

Every organization should maintain an accurate inventory of its technology, including software, hardware, websites, cloud services, and the vendors responsible for supporting them.

Documentation isn't just about being organized.

It's about knowing what needs to be protected and who is responsible for protecting it. CST creates a Detailed Technology Manual (DTM) for every client. Be sure you review yours annually to ensure the information is updated. If you start working with a new company, be sure to let us know so we can have an accurate DTM.

Four Questions You Should Be Asking Your IT Provider.

1. Are all of our computers, servers, firewalls, and applications receiving security updates?
2. Do we have a complete inventory of our technology?
3. When was our firewall last reviewed?
4. Are we regularly checking for vulnerabilities?

If you are a CST client, know that we are taking care of all of the above for you but feel free to discuss this during your next Technology Business Review.

Oh, and don’t forget to contact your website company to ensure your site is updated and secure. Be sure to ask them about the PHP vulnerability.

I will always encourage organizations to provide cybersecurity awareness training. Your employees need to recognize threats and understand their responsibilities.

But training alone will not protect an outdated server, an improperly configured firewall, or a vulnerable website.

That requires ongoing technology management, documentation, monitoring, and accountability.

At CST Group, we believe protecting an organization means looking at the entire technology environment, not just the people using it. Because sometimes the greatest risk isn't what someone clicks. It's about those things that nobody knows have been left unprotected.

As we approach the end of 2026, this is a great time to finalize and update your businesses cybersecurity posture.

Please reach out to me to discuss security protocols and actions that you can take to help keep your business safe from cybercriminals

Lisa

The Two Words We Don't Say Enough: Thank You

November is the month when we are reminded to be thankful. But I've been thinking lately about how often we actually take the time to tell people we appreciate them.

I don't mean a quick "thanks" as we're rushing off to the next meeting. I mean genuinely letting someone know that what they do matters.

After all my years in business, I can tell you that nobody builds a successful company alone. I've had employees who have gone above and beyond, clients who have trusted us for decades, vendors who have helped us through difficult situations, and family members who have supported us through it all.

And I wonder sometimes if I've thanked them enough.

We're all busy. We get caught up in deadlines, problems that need solving, and everything that didn't get done today. It's easy to overlook the people who quietly make our lives easier.

So here's my challenge to you this Thanksgiving season.
Think of someone who has made a difference in your life or business and tell them.

Don't assume they already know.

Sometimes the most meaningful thing we can give someone doesn't cost us anything at all.

It's simply two words.

Thank you.

*And to everyone who continues to support CST, our team, and our mission, please know how grateful I am for **YOU**.*









WHAT I'M READING

UNREASONABLE HOSPITALITY: THE REMARKABLE POWER OF GIVING PEOPLE MORE THAN THEY EXPECT BY WILL GUIDARA

Last week, I had the opportunity to meet Will Guidara at our Quarterly Conference in Franklin, TN, where he was the keynote speaker. What a great experience!

Will is the author of Unreasonable Hospitality: The Remarkable Power of Giving People More Than They Expect, a book that reminds us that exceptional service isn't just about doing your job well. It's about making people feel valued, appreciated, and cared for.

One of the biggest takeaways for me is that people may expect good service, but it's the unexpected personal touches that make an experience memorable.

After 26 years in business, I still believe relationships are what set companies apart. Technology is what we do at CST, but taking care of people is why we do it.

If you lead a team, own a business, or simply want to make a greater impact on the people around you, this book is worth reading!

My takeaway: Don't just meet expectations. Look for opportunities to exceed them in ways that matter.

What You Don't Know CAN Hurt You

Have you ever assumed something was being taken care of, only to find out later that it wasn't?

I have and I am willing to bet that if you own a business, manage a team, or lead an organization, you have too.

We all have responsibilities that we delegate to other people. We have to. There simply aren't enough hours in the day to do everything ourselves. But there is a difference between delegating responsibility and assuming everything is getting done and sometimes, we learn that lesson the hard way.

Recently, I was reminded of this while working through some cybersecurity concerns involving outdated website software. Now, before you stop reading because you think this is going to be another article about cybersecurity, stay with me. Because what I want to talk about isn't really technology.

It's about leadership.

We spend a tremendous amount of time teaching people what NOT to do. Don't click suspicious links. Don't share passwords. Don't open attachments from people you don't know.

All good advice.

But here's the interesting part.

Like I mentioned in my Tech Talk article, sometimes a cybercriminal doesn't need anyone to make a mistake. They simply find something that hasn't been maintained, updated, or properly secured.

Nobody clicked anything. Nobody opened a suspicious email.

Something that should have been taken care of simply wasn't. That got me thinking about how often this happens in business.

How many things in our organizations do we assume are being handled because we have assigned someone the responsibility?

We assume the bills are being paid on time. We assume our employees understand what is expected of them. We assume our customers are happy because nobody is complaining.

We assume our processes are working because nobody has told us otherwise. We assume our technology is secure because we hired someone to manage it.

But are we verifying any of those assumptions?

I have been in business a long time and one thing I continue to learn is that you cannot manage a business on assumptions. Believe me, I am still learning.

As business owners, we want to trust the people around us. We should trust them. We hire good people, give them responsibilities, and expect them to follow through. But trust and accountability are not opposites. You can trust someone and still ask questions. You can delegate a responsibility and still expect updates. You can have confidence in your team and still verify that important work is being completed.

In fact, I believe that is part of being a responsible leader. The challenge is finding the balance.

Nobody wants to be the boss who constantly looks over everyone's shoulder. I certainly don't.

But I also don't want to be the business owner who discovers a problem six months after it started because I assumed someone else had it under control. Sometimes, the problem isn't that someone failed to do their job. Maybe expectations weren't clear. Maybe nobody understood who was responsible. Maybe a process changed and nobody updated the documentation. Or maybe something simply fell through the cracks because everyone was busy.

Sound familiar?

I think most business owners can relate.

The answer isn't to stop delegating. It's to create a way to know that the important things are actually getting done.

That might mean regular meetings, written procedures, documented responsibilities, or simply asking better questions.

Not because we don't trust our people, but because we care about the outcome.

There is another side to this that I think is equally important.

When we discover something isn't being done correctly, how do we respond? Do we immediately look for someone to blame or do we ask what happened, why it happened, and what we can change to prevent it from happening again?

I have learned that asking the right questions is far more productive than pointing fingers and I think our employees appreciate that approach too.

As leaders, we set the tone. We can create an environment where people are afraid to admit something went wrong, or we can create one where problems are brought forward before they become bigger problems. I know which one I would rather have.

So here is my challenge to you this month.

Think about one important area of your business that you haven't checked on lately. Maybe it's your finances, your customer relationships, your employee training, your operations, or yes, even your cybersecurity.

Ask yourself three questions.

Do I know who is responsible? Do I know what is actually being done? How do I know it's working?

If you can't answer those questions, maybe it's time for a conversation. Not an interrogation. Not a lecture. Just a conversation. Because leadership isn't about having your hands in everything. It's about making sure the important things don't get overlooked.

Sometimes, what you don't know really **CAN** hurt you.

Stay passionate, not pushy.

Lisa

Spreading a Little Client Appreciation!



Tasha, Tracy, and Sara

Sara and Tasha have been out and about visiting our amazing clients, sharing smiles and showing just how much we appreciate their continued trust and partnership!

At CST Group, we know our clients are the heart of what we do. Our team will continue making client appreciation visits throughout the rest of 2026, so don't be surprised if we pop in to say hello!

Because great partnerships deserve a little extra appreciation!

Your Phone System Is a Turkey. And Not the Good Kind.

Still dealing with dropped calls, outdated phones, and a phone system that belongs at the kids' table?
This Thanksgiving, the only thing that should be getting roasted is the turkey. Not your business communications.

With CST Group's VoIP solutions, you can enjoy crystal-clear calls, flexibility to work from anywhere, and features that make your business sound like a million bucks
(without spending it).

Don't let your outdated phone system gobble up your productivity!

Give Michelle a call and book your FREE VoIP demo today!

Because the only thing you should be putting on hold this Thanksgiving is a second helping of mashed potatoes.

Is Your IT Provider Finding Problems BEFORE They Become Problems?

Just because your computers are working doesn't mean they're secure!
When was the last time your IT provider checked for security vulnerabilities?
Cybercriminals are constantly looking for weaknesses, and your business could be at risk without even knowing it.

Your IT provider should regularly check for:

- Missing security updates
- Outdated software
- Firewall weaknesses
- Unsecured remote access
- Known security vulnerabilities

Finding problems isn't enough. They need to be FIXED!

At CST Group, we believe in preventing problems, not just responding when something breaks.

Here's my challenge to you:

Ask your IT provider:
"When was our last vulnerability assessment, what did you find, and what was done about it?"

If they can't answer, it's time for a conversation!

Don't wait for hackers to find the weaknesses first. Contact CST Group today to discuss your cybersecurity needs!