CST TECHNOLOGY TIMES

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

Tech Talk...

with Lisa Brown, CEO of CST Group Inc.

I didn't think it was possible, but I recently found myself in a weeklong argument with artificial intelligence. Yes, you read that right — an argument with a robot.

On August 17th, I placed an order for a small appliance, a birthday gift for my daughter whose birthday is August 27th. For once, I was ahead of schedule and feeling proud of myself for being proactive. But that celebration didn't last long.

Just two days later, I received an email that my order had been cancelled. No explanation, just cancelled — with a "helpful" phone number to call if I wanted to try again. So, I called.

That's when the fun began. Instead of a person, I was greeted by an AI Assistant who politely instructed me to "speak in normal conversational tones" and she would be happy to help. Have you ever tried reasoning with a machine that only understands the limited algorithms it's been given? Let's just say it doesn't go well. After twelve minutes of circular conversation, the AI gave up and put me on hold for a live representative.

Sixteen minutes later,

continued on page 4

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.

IS YOUR BUSINESS TRAINING AI TO HACK YOU?

There's a lot of excitement about artificial intelligence (AI) right now, and for good reason. Tools like ChatGPT, Google Gemini and Microsoft Copilot are popping up everywhere. Businesses are using them to create content, respond to customers, write e-mails, summarize meetings and even assist with coding or spreadsheets.

AI can be a huge time-saver and productivity booster. But, like any powerful tool, if misused, it can open the door to serious problems – especially when it comes to your company's data security.

Even small businesses are at risk.

Here's The Problem

The issue isn't the technology itself. It's how people are using it. When employees copy and paste sensitive data into public AI tools, that information may be stored, analyzed or even used to train future models. That means confidential or regulated data could be exposed, without anyone realizing it.

In 2023, engineers at Samsung accidentally leaked internal source code into ChatGPT. It became such a significant privacy issue that the company banned the use of public AI tools altogether, as reported by *Tom's Hardware*.

Now picture the same thing happening in your office. An employee pastes client financials or medical data into ChatGPT to "get help summarizing," not knowing the risks. In seconds, private information is exposed.

continued on page 2...

...continued from cover

A New Threat: Prompt Injection

Beyond accidental leaks, hackers are now exploiting a more sophisticated technique called prompt injection. They hide malicious instructions inside e-mails, transcripts, PDFs or even YouTube captions. When an AI tool is asked to process that content, it can be tricked into giving up sensitive data or doing something it shouldn't.

In short, the AI helps the attacker – without knowing it's being manipulated.

Why Small Businesses Are Vulnerable

Most small businesses aren't monitoring AI use internally. Employees adopt new tools on their own, often with good intentions but without clear guidance. Many assume AI tools are just smarter versions of Google.

They don't realize that what they paste could be stored permanently or seen by someone else.

And few companies have policies in place to manage AI usage or to train employees on what's safe to share.

What You Can Do Right Now

You don't need to ban AI from your business, but you do need to take control.

Here are four steps to get started:

1. Create an AI usage policy.

Define which tools are approved, what types of data should never be shared and who to go to with questions.

2. Educate your team.

Help your staff understand the risks of using public AI tools and how threats like prompt injection work.

3. Use secure platforms.

Encourage employees to stick with business-grade tools like Microsoft Copilot, which offer more control over data privacy and compliance.

4. Monitor AI use.

Track which tools are being used and consider blocking public AI platforms on company devices if needed.

The Bottom Line

AI is here to stay.

Businesses that learn how to use it safely will benefit, but those that ignore the risks are asking for trouble.

A few careless keystrokes can expose your businessto hackers, compliance violations, or worse.

FREE DOWNLOAD:

If You Are Considering Cloud Computing For Your Company, DON'T, Until You Read This...

If you are considering cloud computing or Office 365 to save money and simplify IT, it is extremely important that you get and read this special report: **"5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud."**

This report discusses in simple, nontechnical terms the pros and cons of cloud computing, data security, how to choose a cloud provider and three little-known facts that most IT consultants don't know or won't tell you about cloud computing that could end up causing you MORE problems and costing you more money than you anticipated. **Even if you aren't ready to move to the cloud yet**, this report will give you the right information and questions to ask when the time comes.

Get your FREE copy today: www.cstsupport.com/cloudreport

CARTOON OF THE MONTH

"I'm just sayin' a little conflict resolution trainin' might not be unwarranted."

BILLY BEANE

SHARES HIS WINNING DATA-DRIVEN STRATEGY FOR BUSINESS

A failed 2001 draft led former Oakland A's General Manager Billy Beane to overhaul how he managed talent—sparking a transformation that revolutionized baseball and inspired industries worldwide.

Using a data-driven strategy, Beane turned the low-budget Oakland A's into consistent playoff contenders. The team won seven American League Western Division titles and made 10 postseason appearances, all while operating with one of the lowest payrolls in Major League Baseball.

Beane's approach, known as the "Moneyball" philosophy, emphasized objective analysis over tradition and intuition. It gained widespread recognition through a best-selling book and Oscar-nominated film chronicling his unconventional path to success.

At a recent leadership event, Beane outlined how businesses can adopt similar principles to build high-performing teams despite resource limitations.

Make Data-Backed Decisions

"Baseball had been tracking stats since the 1800s, but none of it influenced decision-making," Beane said. "I turned running a team into a math equation." He replaced gut instinct and subjective scouting with analytics, reshaping how talent was evaluated.

Identify Undervalued Assets

"There's a championship team you can afford—you just need to find what others undervalue," Beane explained. He focused on on-base percentage, a metric more predictive of winning than traditional stats, uncovering overlooked players who delivered strong results.

Be Relentless With Execution

"You can't go back and forth," Beane said. "If you commit to data, you have to use it every time." His team stayed disciplined throughout each season, trusting the math to guide decisions rather than reacting emotionally to short-term outcomes.

Maximize The Middle

Rather than spending big on stars, Beane focused on building depth. "We couldn't afford top players, so we made sure we didn't have bad ones," he said. "A strong middle roster outperforms one with gaps."

Hire Differently

Beane recruited talent from outside traditional pipelines. One example was hiring a Harvard economics major as assistant GM—unusual in a role typically filled by former players. This fresh thinking helped the A's stay ahead.

Redefine Culture With Data

"If we did what everyone else was doing, our results would match our budget," Beane said. "We challenged the norm, used data to value skills differently and changed our outcomes."

Lead With Transparency

"Data explains decisions," he noted. "Even when you're not always right, clarity builds trust."

Level The Playing Field

Beane's philosophy proves that success isn't solely dictated by budget. With innovation, discipline and a data-first approach, even smaller organizations can compete with giants.

As he put it: "Data isn't an opinion. It's a fact."

SHINY NEW GADGET OF THE MONTH

Logitech MX Mechanical Wireless Keyboard

The Logitech MX Mechanical Wireless Keyboard delivers a premium, quiet typing experience with tactile mechanical switches for precise, low-noise feedback. Its low-profile, full-size layout enhances comfort and ergonomics, while smart backlit keys illuminate as your hands approach, adapting to lighting conditions. Seamlessly pair with up to three devices across multiple operating systems via Bluetooth or the Logi Bolt receiver. Customizable through Logi Options+, it supports efficient workflows, and its rechargeable battery lasts up to 15 days with lighting or 10 months without.

CLIENT SPOTLIGHT:

Decker Plumbing & Drains

Family owned and operated, honest and dependable with over 25 years of experience. Able to service all your plumbing and drain needs In Southwest Florida. Whether it is your home's bathroom shower or restaurant's kitchen sink, trust the experts at Decker Plumbing & Drains to get the job done right!

Residential or Commercial Properties

(941) 979-0896

http://DeckerPlumbingandDrains.com/

WHY PHISHING ATTACKS SPIKE IN THE SUMMER

You and your employees may be getting back from vacation, but cybercriminals never take a day off. In fact, data shown in studies from vendors ProofPoint and Check Point indicate that phishing attempts actually spike in the summer months. Here's how to stay aware and stay protected.

Why The Increased Risk?

Attackers use your summer travel bug to their advantage by impersonating hotel and Airbnb websites, says Check Point Research. They've uncovered a sharp increase in cyberthreats related to the travel industry – specifically, a 55% increase in the creation of new website domains related to vacations in May 2025, compared to the same period last year. Of over 39,000 domains registered, one in every 21 was flagged as either malicious or suspicious.

August/September is also back-to-school time, which means an uptick in phishing attempts imitating legitimate university e-mails, targeting both students and staff.

While these threats might not affect your industry directly, there's always a chance that employees pursuing their master's degree or planning a vacation will check their personal e-mail on their work computer – and it takes only one wrong click for cyberattackers to have access to all of your business's data.

What To Do About It

While AI is making cybersecurity stronger and workflows smoother, it's also making phishing attacks more convincing. That's why it's important to train yourself and your team on what to look for, to avoid clicking on a malicious link.

Safety tips to prevent attacks:

- **Keep an eye out for shady e-mails.** Don't only check for misspellings and poorly formatted sentences in the body of e-mails; AI can write e-mails for attackers just like it can for you. Also examine the e-mail address of the sender and the text of the link itself, if visible, to make sure everything looks legitimate.
- **Double-check URLs.** Misspellings in the link text or unusual domain endings, like .today or .info, can be an indicator of an attack. Domain endings like these are often used in scam sites.
- **Visit websites directly.** It's always better to search for the website yourself, rather than clicking on links in any messages or e-mails.
- **Enable Multifactor Authentication (MFA).** Setting up MFA ensures that even if a breach does occur within your company, your login credentials will remain protected – and so will any data secured behind them.
- **Be careful with public WiFi.** If you need to use public WiFi, use a VPN for additional protection when accessing secure information, like booking portals or bank accounts.
- **Don't access personal e-mail on company devices.** Accessing personal e-mail, messaging or social media accounts on business devices increases your risk. Keep personal accounts on your personal devices, and work-related accounts on the work devices.
- **Ask your MSP about endpoint security.** Endpoint detection and response (EDR) software can monitor your desktops and mobile devices, detect/block phishing attempts, malicious downloads and alert your MSP immediately in the event of a breach, limiting your data's exposure.

Phishing attempts become more sophisticated every day, and AI is only speeding that process along. Because of this, it's essential to keep your team well-informed of the risks; knowledge is the best defense against phishing attacks. Stay informed and stay safe!

Back-to-School Cyber Safety: Protecting Your Technology This Fall

September means new routines, busy schedules, and lots of devices connecting back into classrooms, workplaces, and home networks. With so much activity, cybercriminals see this as the perfect opportunity to target individuals and organizations alike. Whether you're a parent, student, or employee, here are some back-to-school technology safety tips to keep in mind:

1. Students and employees often log in to multiple portals (school accounts, work email, cloud apps). Weak or reused passwords are one of the easiest ways for hackers to gain access.
2. Back-to-school season brings an uptick in fake emails pretending to be from schools, HR departments, or even IT support. Be cautious of emails asking you to "verify" account details or download attachments. Double-check sender addresses before clicking links.
3. Kids bring home school laptops, and employees may be switching between personal and work devices. A compromised home network can put workplace data at risk. So be sure to keep devices updated with the latest security patches and use antivirus and endpoint protection.
4. With remote learning and hybrid work, Wi-Fi security is critical. Change default router passwords and avoid public Wi-Fi without a VPN.
5. Cybersecurity awareness starts early. Parents and managers alike should take time to talk about safe online practices. This should be an ongoing conversation. Encourage kids not to overshare personal info online and remind employees that one careless click at home can put business systems at risk.

As families and workplaces transition into the busy fall season, cybercriminals are hoping someone will let their guard down. By reinforcing good cyber hygiene — strong passwords, cautious clicking, and updated devices — you'll keep your data, your business, and your family safe.

....Tech Talk Continued from Front Page

a human finally came on the line. I explained the situation and was told my order was flagged as fraud since the billing address was in New York but the gift was shipping to Florida. On one hand, I understand and appreciate this — after all, cybersecurity is my world. On the other hand, wouldn't it have been easier for them to simply call me to confirm? I'm sure they process millions of orders with different billing and shipping addresses every month.

I was then transferred to the fraud department, where—of course—another AI Assistant answered. After another ten minutes of going in circles, the call disconnected. At this point, I had wasted over an hour.

Still determined, I called back. This time, I had learned the secret to beating the bot: repeat the words "live person" over and over until it gets confused enough to surrender. Sure enough, it worked, and I was connected to another live agent who apologized and explained I would need to be transferred again. By this point, I was told the fraud department didn't even answer phones live—I would need to leave a voicemail. Yes, you read that correctly. A billion-dollar company with decades of history requires customers to leave a message with their order number and phone number to get fraud cleared.

Fast forward to August 22nd. Still no call back. I tried again, but the AI had caught on to my trick and no longer fell for the "live person" request. I was stuck in another lengthy conversation with the bot before being transferred to a representative. Thankfully, she understood my frustration, escalated the issue to her manager and corporate, and encouraged me to leave yet another message with fraud.

Here's the thing. As aggravating as this entire ordeal was, it's also a clear reminder: if you think artificial intelligence won't affect you, you're mistaken. AI is already woven into our daily lives in ways most people don't even realize. Your email filters, smart replies, GPS navigation, traffic predictions, shopping recommendations, streaming suggestions, Alexa, Siri, banking fraud alerts — all powered by AI. And this is just scratching the surface. AI is not going away. But as my experience proves, it's not foolproof either. Without the right human oversight, guardrails, and processes, AI can create more frustration than efficiency.

So here's my question to you: how is your business using AI? Even if you're not ready to put a full-blown policy in place, you should have written guidelines to direct how your team interacts with AI and to make sure sensitive information is protected. You need those guardrails now — not later.

If you'd like guidance, training, or simply have questions about putting AI practices in place for your business, contact Jessica at 518-483-4100 or jessica@cstsupport.com.

And in case you're wondering — yes, the fraud department finally called me back on August 23rd and released the order. They promised it wouldn't happen again. Unfortunately, the gift is scheduled to arrive on September 2nd — six days after my daughter's birthday. Not exactly the proactive win I was hoping for!

Lisa

BIG REWARDS

For Your Referrals

We'll offer you **$50** as a gesture of appreciation, once you introduce CST Group to a qualified colleague and they complete the initial appointment whether they become a client or not.

If your referral becomes a managed client, we'll provide you with a **$500** bonus at the end of their first month of service.

SO, YOU MIGHT BE WONDERING – WHO MAKES AN IDEAL REFERRAL?

- **Any business with 10 or more computers**
- **Needs help with its network, backup, compliancy, support, and security**
- **Wants 24x7x365 peace of mind**

Full Details Here: https://www.cstsupport.com/about-us/referral-program/
or call us at 1-877-954-4100

Passionate NOT Pushy
WITH LISA BROWN

SCAN HERE

The Gift of Honest Conversation

Last week, I had the privilege of sitting down with a friend who also happens to be both a mentor and a client. We met for lunch at our local coffee shop, a familiar spot that has hosted many of my best conversations. I came prepared with a neatly organized list of business growth ideas I wanted to discuss and over lunch, we went through them one by one.

What struck me most during our time together wasn't just the exchange of ideas, it was the way she listened, the way she responded, and the way she made me feel heard. There's a certain kind of trust that comes from having someone in your corner who will never ridicule or dismiss your thoughts but instead offer insight with honesty and kindness. That kind of support is rare, and it's something I treasure deeply.

Part of what makes this relationship so meaningful is our history. I've known her since before CST Group was even a company. She has stood beside me through trials, tribulations, and turning points, always offering steady encouragement and wise perspective. Having someone who has witnessed the full arc of your journey, from the messy early days to the present, adds an extra layer of trust to every conversation. She doesn't just know where I am now, she knows how far I've come. I've always believed that preparation matters. Coming into the meeting with a list kept our conversation focused and ensured I didn't lose sight of the priorities I wanted her feedback on.

But the list itself was only half the equation - the real value came from her perspective. She pushed me to think beyond the surface, challenged me to look at opportunities differently, and confirmed when my instincts were on the right track. It wasn't about telling me what I wanted to hear; it was about telling me what I needed to hear.

Honest input, when given from a place of care, is one of the most powerful tools for growth. Praise feels good in the moment, but it's honest, constructive feedback that propels us forward. Having someone you can trust to deliver that feedback in a thoughtful way makes all the difference.

It's not easy to be vulnerable about your ideas, especially the ones that matter most, but it becomes possible when you know the person sitting across the table has your best interests at heart.

This conversation reminded me of the importance of friendship as the foundation of mentorship. Yes, she is a client and yes, she is a mentor, but before all of that, she is my friend. Our mutual respect allows us to navigate those roles seamlessly. I can speak openly, share ideas in their rough form, and know she will handle them with care while still giving me the truth. As business leaders, entrepreneurs, or simply as people navigating life, we all need those trusted voices. Mentors don't always come in the form of formal titles or professional coaches. Sometimes, they're sitting across from you at a coffee shop, blending the wisdom of experience with the loyalty of friendship.

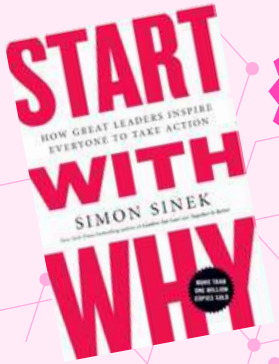
Walking out of that meeting, I felt grateful, not just for the ideas we discussed, but for the reminder that growth doesn't happen in isolation. It happens when we open ourselves up to honest conversation, when we let others challenge us with kindness, and when we surround ourselves with people who want to see us succeed.

Passion, after all, isn't meant to exist in a vacuum. It grows stronger when nurtured in trust.

I want to thank Andrea Stewart, friend, mentor and Supervisor for the Town of Malone. Andy, I appreciate you so much for indulging my crazy and I can't wait for people to hear our talk in the Passionate Not Pushy Podcast!

WHAT I'M READING....

This month I'm reading Start With Why by Simon Sinek. As a leader, I believe knowing your "why" fuels passion, purpose, and impact. It's a reminder that success isn't just about what we do—but why we do it.



<BOOK> <OF_THE> <MONTH>

Is Your Business Still Running on "Stone Age" Equipment?

In today's fast-paced digital world, using outdated technology isn't just inconvenient—it's risky. If your computers, servers, or network devices are more than five years old, they could be slowing down your business and leaving you vulnerable to cyber threats.

Old equipment often lacks the processing power, storage, and security features needed to keep pace with modern software. That means slower response times, more system crashes, and greater exposure to hackers who target outdated systems. In fact, unsupported hardware and operating systems no longer receive critical security patches, making them an easy entry point for cybercriminals.

Upgrading your equipment isn't just about staying current—it's about protecting your business, your clients, and your data. Fresh technology helps your team work faster, improves reliability, and ensures you're meeting compliance standards.

Take a look around your office. Are you still relying on "stone age" equipment? If so, it may be time for an upgrade.

Passionate NOT Pushy WITH LISA BROWN

New Podcast Episode Alert!

This month on Passionate Not Pushy, Lisa sits down with Andrea Stewart. From shaping state legislation to managing millions in town finances, Andrea Stewart's career is a masterclass in public service and leadership. After more than 30 years of dedicated work in Malone's town government, Andrea thought she was ready to retire—only to return as Town Supervisor, leading with resilience and vision.

In this episode of Passionate Not Pushy, Lisa sits down with Andrea to talk about leadership that lasts, the power of community, and what it really takes to turn challenges into opportunities. Don't miss this conversation—you'll walk away inspired to lead with purpose, no matter where you serve.

Listen Now On Spotify!

Andrea Stewart

SEPTEMBER EVENTS

Sep 1st- Labor Day (OFFICE CLOSED)
Sep 9th -Carrie's CST Anniversary
Sep 11th- 911 Remembrance Day
Sep 18th- National Cheeseburger Day
Sep 22nd- Business Women's Day
Sep 26th- Michelle's CST Anniversary

CONCERNED ABOUT THE SAFETY AND SECURITY OF YOUR ONLINE IDENTITY? YOU SHOULD BE!

If you've been following the latest news in cybersecurity, you know that attacks have only continued to grow in both size and sophistication. However, you might not be aware that small and mid-sized businesses like yours are the most targeted by Dark Web criminals. Would you be among the 60% of SMBs that would be bankrupted by the average cost of a data breach?

If you are reading this, you are eligible for a free and comprehensive Dark Web scan to identify how many of your credentials (DOB, SSN, User ID's and Passwords) have been compromised. To get your FREE Scan instantly, contact us today at 518-483-4100 or 941-249-3520 or email sara@cstsupport.com.