

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

### Tech Talk With Lisa

#### Faster Decisions, Bigger Risks: The Truth About AI in Business

How are you and your team using AI?

And if you think nobody is using it, let me stop you right there. Unless you are living in a cave, you are probably mistaken.

Artificial Intelligence is both a blessing and a risk. What matters is how you use it and what your team may be doing with it that could jeopardize your company.

AI is powerful. I use it every day, and I know my team does too. If I had to estimate the time and money it has saved me, it is easily in the thousands.

Why? Because it can gather information from millions of sources in seconds and organize it into something usable. It helps draft content, write emails, and even analyze data. Tasks that used to take days now take minutes.

Do I trust it? Absolutely not...

Cont. On Page 3



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.

## FEELING LUCKY? THAT'S NOT HOW WELL-RUN BUSINESSES OPERATE

### Why 'We've Been Fine So Far' Doesn't Hold Up

Here's the trap: When nothing bad has happened, it feels like proof that nothing will.

Every business that's had a long, chaotic, how-did-this-happen day said "we've been fine" the morning before.

Luck isn't a system. It's just risk you haven't met yet.

Think of it like driving without insurance. You might get away with it for years, but the day something goes wrong, you'll wish you had a plan.

### Prepared vs. Hoping for the Best

Most businesses don't discover how unprepared they are until they're in trouble.

#### That's when the questions start:

- Do we have a backup?
- How recent is it?
- Who handles this?
- How long will we be down?

Luck is fun and festive, but well-run businesses don't operate on luck.

#### No owner would ever say:

- "Our hiring strategy is whoever walks in."
- "Our sales plan is hoping customers find us."
- "Our accounting approach is the numbers working themselves out."

That would be absurd.

### The Quiet Double Standard

Somewhere along the way, technology unintentionally gets a pass.

*"We've never had an issue."  
"It's probably backed up somewhere."  
"We'll deal with it if something happens."*

That's not a plan. That's superstition dressed up as strategy. Unless you've got a leprechaun assigned to your IT systems, it's a risky bet.

Most owners would never leave payroll, taxes or customer service to chance. Yet when it comes to technology recovery, hope somehow feels acceptable.

Prepared businesses already know the answers. Luck-reliant businesses find out in real time.

Being prepared doesn't mean expecting disaster. Think about it this way: When your systems are tested and documented, a hiccup is just another Tuesday.

When they're not, that same hiccup can turn into a full-blown crisis.

Customers notice, employees get frustrated and suddenly you're spending more time fixing problems than running your business.

### The Reality Check

If your accountant managed books the way you manage tech recovery, would you be okay with that? Why give technology a pass?

# YOUR ACCOUNTANT IS STRESSED.

## HACKERS KNOW IT.



Your accountant is buried. Your bookkeeper is scrambling. Deadlines are looming. Emails are flying faster than anyone can keep up. Everyone is heads down, trying to get through tax season. This isn't news to you, and it's not news to hackers either.

Phishing attempts surge during tax season. Their messages aren't dramatic. They blend in with everyday business requests, right when people are busiest. That's not coincidence. That's strategic timing.

### The Stressed Supply Chain

Here's what most people miss: Hackers aren't just targeting accounting firms; they're targeting the chaos around them.

#### During tax season:

- Clients rush to send sensitive documents
- Staff shortcut normal checks to keep up with volume
- "Just send me the file" replaces usual caution
- Verification gets skipped because everyone is slammed

The whole ecosystem speeds up, making mistakes more common. Hackers don't go after calm, methodical businesses. They go after the busy ones.

### What These Attacks Look Like

This isn't a movie plot. It's an email that

looks exactly like the others in your inbox:

- A message from "your accountant" asking you to resend documents because something didn't come through
- A note from a vendor saying their bank information has changed and needs updating
- A DocuSign request that "needs your signature today"
- An urgent email from "your CEO" who's traveling and needs help immediately

None of these feel suspicious. They feel like normal business. That's why they work.

### Why Busy People Get Caught

Falling for these scams isn't about being careless. It's about being human. When inboxes are full and deadlines are tight, people don't read carefully. They scan. They assume. They react.

Bad actors know this. Their messages are designed for people who are moving too fast to notice the one detail that's off. They don't need you to be reckless. They need you to be busy.

### 4 Simple Ways to Avoid Being an Easy Target

You don't need fancy tools or a security team to reduce your risk. You just need a few intentional habits during busy months.

#### 1. Verify payment changes by phone

If an email says a vendor's banking details have changed, don't reply to the message. Call a number you trust to verbally confirm.

#### 2. Slow down requests for sensitive information

Urgency should be a signal to pause, not to rush. If someone asks for bank statements, tax documents or other financial files "right now," take a moment to verify.

#### 3. Confirm urgent requests through a second channel

If an email claims something is urgent, verify it another way. A quick call, text or internal message can stop a bad decision before it starts. Real urgency can survive a two-minute check.

#### 4. Give your team a five-minute heads-up

Remind your team that it's okay to slow down, double-check and ask questions when something feels off. That small permission shift can prevent a lot of unnecessary cleanup later.

### The Takeaway

The attacks showing up during tax season aren't clever. The power is in their timing. You don't have to overhaul your systems to avoid becoming the easy target, but you do need to slow down when it matters and verify when things feel urgent.



It starts like any normal morning. Coffee in hand. Laptop open. You're settling in, ready to get moving.

Then your elbow clips the mug.

Time slows just enough for you to watch coffee spill across the keyboard and disappear into places coffee should never go.

The screen flickers.

The keyboard stops responding.

The laptop makes a noise laptops shouldn't make.

No hackers. No ransomware. No dramatic warning screens.

This completely normal moment that suddenly changes the day is how many business disruptions start.

### The Problem Isn't the Mistake — It's What Happens Next

Most businesses picture downtime as something dramatic. Servers down, systems dead and everything grinding to a halt.

In reality, downtime is often as boring as a spilled drink on a laptop, a file that "definitely got saved" but now doesn't exist, an update that doesn't finish or a computer that won't boot for any obvious reason.

The real damage doesn't come from the mistake itself. It comes from the stall that follows: the waiting, the guessing, the "do we know how long this will take?"

Work doesn't fully stop. It half-stops. And half-working can be as bad as not working at all.

### The Hidden Cost of Waiting

Here's what that stall usually looks like.

One person can't work, so they wait. Two others try to help but aren't sure what to do. Someone messages IT. Someone else switches tasks "for now."

Ten minutes turn into 30. Thirty turns into an hour.

Now multiply that by the number of people affected, the interruptions, the mental context switching and the momentum that never quite comes back.

Even small delays add up quickly. Not in dramatic, headline-worthy ways, but in quiet, frustrating ways that drain the day without anyone noticing until it's gone.

### Same Problem, Different Outcomes

Let's rewind the coffee spill.

### SHINY NEW GADGET OF THE MONTH

#### UGREEN NASync DXP4800 Plus

Imagine a server that not only stores files but also understands them. This AI-ready home and office server organizes your data by content, faces and locations. Instead of digging through folders, you can simply ask for a signed contract from last quarter or a video from a meeting.

It's fast, secure and sits right on your desk. Your data stays private and confidential, accessible only to you.



### AI Accuracy: What the Data Shows

How reliable is AI-generated information?

<b>1%–10%</b> <small>Controlled environments</small>	<b>10%–30%</b> <small>Typical business use</small>	<b>30%–80%</b> <small>Complex scenarios</small>
---	---	--

#### What is a hallucination?

AI presenting incorrect or fabricated information as fact

#### Reality Check:

- AI predicts answers. It does not verify truth
- Confident responses can still be wrong

#### Business Impact:

- Reliable for drafting and summaries
- Risky for accuracy, compliance, decisions

**Best Practice: Trust, but verify**

Source: Industry benchmarks and AI research studies

...continued on page 4

## FREE REPORT DOWNLOAD

### The Business Owner's Guide To IT Support Services And Fees

#### You'll learn:

- The three most common ways IT companies charge for their services and the pros and cons of each approach
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate



Get your FREE copy today: [www.cstsupport.com/itbuyersguide](http://www.cstsupport.com/itbuyersguide)

### CARTOON OF THE MONTH



...continued from page 3

In one business, there's no clear next step. No one knows who handles recovery. Someone suggests, "Maybe Dave knows," but Dave's on vacation. People wait just in case. By lunch, half the day is gone.

In another business, the issue gets reported immediately. The response is clear. Files are restored. The employee is back to work.

Same coffee. Same mistake. Completely different day. The difference isn't luck. It's recovery speed and clarity.

#### Why Well-Run Businesses Make Problems Boring

Here's the shift most businesses miss: The goal isn't to prevent every possible problem. That's impossible.

The goal is to make mistakes boring. Boring means no scrambling, no guessing, no long pauses, no "who's on this?" moments.

When problems are boring, they don't derail the day. They get handled and everyone moves on.

#### This Is a Leadership Issue, Not a Tech Issue

When small problems cause big slowdowns, it's rarely because of the tools themselves.

It's because:

- There's no clear plan for what happens next
- Responsibility is fuzzy
- Recovery depends on the right person being available
- The business hasn't defined what back to normal means

What people feel isn't the error or the outage; it's the uncertainty.

Well-run businesses remove that uncertainty.

#### A Simple Question Worth Asking

You don't need a dramatic audit to start thinking differently about this. Just ask one question: If something small went wrong today, how long would it take for everyone to get back to work?

If the answer is unclear, that's not a failure. It's information that guides the first step toward smoother days, less downtime and work that keeps moving even when a hiccup inevitably happens.

#### What This Really Comes Down To

Businesses that stay productive when a normal day quietly goes sideways aren't the ones that avoid mistakes. They're the ones that recover so quickly the mistake barely registers. That doesn't require perfection. It requires clarity.

When recovery is clear and quick, problems become forgettable, momentum remains and a cup of coffee stays just a cup of coffee.

*Continued from Cover*

That is the point of this article. I use AI, but I do not rely on it as my only source of information. I fact-check. I cross-check. I apply common sense.

My concern is that many people are using AI to move decisions forward without ever validating the output. AI results are only as good as the prompts behind them. If you are not clear in what you are asking, you increase your chances of getting the wrong answer.

In AI, this is called a hallucination rate. It is the percentage of responses that contain false or unsupported information. This directly impacts trust and risk.

AI does not know facts. It predicts likely answers based on patterns. That is why hallucinations happen. The system prioritizes fluency and completeness, not truth.

So what does that mean for you?

In general business use, studies show that 10% to 30% of AI responses can be incorrect. In more complex scenarios, that number can rise to 30% up to 80%.

That may not sound significant at first. But in industries like legal, insurance, healthcare, financial reporting, and cybersecurity, those numbers are unacceptable. The cost of being wrong is simply too high.

So let me ask again. How are you and your team using AI?

Are you uploading company information? Using it to draft emails? Do you have clear guidelines in place?

To help you move forward safely and productively, here are five steps you should implement right now:

1. Never input sensitive data into free AI tools - Use internal or secured platforms for anything confidential.
2. Verify all critical information - AI can sound confident and still be wrong. Always cross-check.
3. Define clear use policies for your team - Uncontrolled use creates risk quickly.
4. Limit access and use secure platforms - Not all AI tools meet business-grade security standards.
5. Use AI to assist, not replace decision-making - AI improves productivity, but accountability stays with people

**Bonus tip:** Watch for AI-generated phishing scams - AI is making attacks more convincing. Train your team to question polished emails, verify unexpected requests, and check sender details carefully. Multi-factor authentication should be standard across your organization.

The reality is this. Technology is evolving faster than most teams can keep up.

AI is not just a tool. It is changing how decisions are made, how data is handled, and how risk shows up inside your organization. If your team is not trained in how to use it properly, you are leaving your business exposed.

That is why education matters more than ever. Technology alone cannot protect your business. Educated employees can.

As we close the first quarter, I am excited to introduce **CST Academy**, our new training division designed to help organizations navigate exactly these challenges.

We are launching our signature program, The **CST Cyber Aware Organization Framework**. This program is built to help your team understand real-world risks, including AI, and develop safer, smarter habits through practical cybersecurity education, leadership awareness, and measurable employee engagement.

If you are thinking about how to safely adopt AI in your organization, this is where you start.

More information and training opportunities will be released soon. In the meantime, I encourage you to take the first step.

Contact Jessica at [Jessica@cstsupport.com](mailto:Jessica@cstsupport.com) or 518-483-4100 to learn more and get registered.

As we enter the Easter season, it is a time to reflect on renewal, purpose, and new beginnings. It reminds us to slow down, be intentional, and focus on what truly matters. As you continue to adopt tools like AI, take this time to reset and ensure your decisions are grounded in clarity, integrity, and wisdom. Technology will continue to evolve, but strong values and thoughtful leadership will always be what guides long-term success.



Lisa

HAPPY  
Easter

## Easter Tech Tip: Look Beyond the Sweet Surface

Just like a chocolate Easter bunny, cyber threats often look harmless on the outside. A friendly email, a shared document, or a quick request from a “coworker” can hide something much more dangerous underneath.

Cybercriminals rely on one thing: someone taking the first bite.

### Quick Tip:

Before clicking a link or opening an attachment, pause and ask:

- Do I recognize the sender?
- Was I expecting this message?
- Does anything feel unusual or urgent?

That simple pause can stop a cyberattack before it starts.

Want your team to spot threats before they spread?

Security Awareness Training teaches employees how to recognize phishing attempts, suspicious links, and social engineering tactics.

Ask us about CST Group’s Security Awareness Training and build a stronger human firewall.

## Hop To It!

Now’s the time to schedule your annual cybersecurity awareness training. Don’t wait until a threat “cracks” your defenses—be proactive and keep your organization secure year-round.

If you haven’t booked your training yet, reach out today. Let’s make sure your team is prepared to spot every hidden “egg” a cybercriminal might leave behind.

Email: [Jessica@cstsupport.com](mailto:Jessica@cstsupport.com)

# Passionate NOT Pushy



## What I'm Reading

### **Simple Numbers, Straight Talk, Big Profits!** by Greg Crabtree

I have had the opportunity to learn directly from Greg and his approach is exactly what you see in this book. Practical, direct, and grounded in real business results.

**Simple Numbers** breaks down what actually drives profitability in a way that is easy to understand and apply.

One of the biggest takeaways is this. Most businesses do not have a revenue problem. They have a profitability problem.

As we continue to move faster with tools like AI, this message becomes even more important.

Speed is only valuable if your numbers are solid.

## Do It Scared: The Real Work of Growing Your Business

I have spent the last couple of months in Florida, where Shawn and I are enjoying time with family, connecting with clients, and working to grow the business in a new market.

Growth in a new place requires something very real. You have to put yourself out there. And if I am being honest, that can be uncomfortable.

Walking into rooms where you know very few people is not easy. It takes effort, intention, and a willingness to feel out of place for a while. But that is what growth looks like. You put yourself in uncomfortable situations until they become part of your normal.

We have joined several Chamber associations here and I have been attending events, ribbon cuttings, open houses, and business networking breakfasts. My goal is simple. Build relationships and connect with companies that could benefit from what we do.

If I am being candid, the experience has been mixed. While I know not every organization operates the same way, I have found that many are not as proactive in helping new members get connected as you might expect. You are welcomed but not always integrated.

That means you have to take ownership.

You have to introduce yourself. Start conversations. Follow up and show up again and again.

And yes, sometimes that means doing it before you feel ready. What I would love to see is more intentional support for new members. Imagine joining an organization and being paired with a mentor. Someone who attends events with you makes introductions and helps you navigate the community. That kind of experience would create stronger connections and better outcomes for everyone involved. Until then, the responsibility is ours.

If you are growing your business, do not wait until you feel comfortable. Put yourself out there. Join the groups that align with your goals. Take the steps to be seen and known. Do it even when it feels uncomfortable. Because in the end, that is where real growth happens.

You do not have to be the loudest person in the room to grow your business. You just must be present, consistent, and genuine.

That is what being Passionate Not Pushy, looks like. It is showing up, building real relationships, and letting your work and your character speak for you.

So, keep putting yourself out there. The right connections will come.

Lisa

## Subscribe Here





Leadership doesn't have to be loud to make an impact. In this Month's Passionate NOT Pushy Podcast, I sat down with Billie Jo Decker, co-owner of Decker Plumbing & Drains, to talk about:

- Building a business rooted in trust & professionalism
- Leading with family and community at the center
- Staying confident and passionate without being pushy

From family-first values to giving back to the community, Billie Jo shows us what true leadership looks like.

Listen now on Spotify.



Billie Jo Decker



Family Owned & Operated Plumbing Service  
Serving South West Florida

**941-979-0896**

service@deckersquad.com

## Are You & Your Town Attending The NYS Tug Hill Commission Conference COME & VISIT US!!

Our team is excited to be attending the upcoming NYS Tug Hill Commission Conference. This event brings together local government leaders, municipal staff, and service providers from across the region. Representing our company I.T. for Local Government, Sara, our Sales Development Representative, and Mary, our Marketing Assistant, are heading out to connect, learn, and share how we support municipalities with reliable, secure, and efficient technology solutions.

During the conference, our focus is on building relationships with local government officials and gaining a deeper understanding of the evolving technology needs facing municipalities today. From cybersecurity concerns to infrastructure improvements and digital transformation, we are looking forward to engaging in meaningful conversations about how dependable IT support plays a critical role in public sector operations.

Events like the Tug Hill Commission Conference are an important part of our ongoing commitment to local governments. We're proud to be part of these conversations and look forward to the connections and insights this event will bring.

