APRIL 2024

CST TECHNOLOGY TIMES

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

"passionate NOT pushy"

By Lisa Brown, CEO & Founder

It starts with the sale – or at least with the salesperson. Time and time again, I encounter mediocre vendors. And guess what, it is NOT their fault! Remember, it starts at the top!

You know who I'm talking about? Company's you work with who don't answer their phones, take days, sometimes weeks, to respond and blow you off every chance they get?

Part of what CST does for our clients involves coordination of effort on ensuring the software and or hardware they purchase from another vendor works and performs as it should. If you have a problem with your accounting software, we will coordinate the solution. If you have a problem with a printer, we will take care of it for you. Have a problem with your Internet connectivity, yup, we will solve that problem as well.

There are a couple of things I have learned about this type of vendor management offering.

1. The person that sold this solution – made promises they, in no way, had the authority to keep and….
2. Communicating with these vendors is HARD and TIME-CONSUMING as they rarely take responsibility for the problem and will often-times try to blame someone else – usually YOU! Which is why we prefer to do it for you.

(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 that specializes in helping compliance-driven industries to SECURE, PROTECT and MANAGE their technology.

3 CYBER SECURITY MYTHS THAT WILL HURT YOUR BUSINESS THIS YEAR

Working amid the ever-changing currents of technology and cyber security, businesses often find themselves entangled in a web of misinformation and outdated ideas. But failing to distinguish between myth and fact can put your business's security at serious risk.

Based on expert research in the field, including CompTIA's 2024 global State Of Cybersecurity report, we will debunk three common misconceptions that threaten to derail your success in 2024.

Myth 1: My Cyber Security Is Good Enough!

Fact: Modern cyber security is about continuous improvement.

Respondents to CompTIA's survey indicated that one of the most significant challenges to cyber security initiatives today is the belief that "current security is good enough" (39%).

One of the reasons businesses may be misled by the state of their security is the inherent complexity of cyber security. In particular, it's incredibly challenging to track and measure security effectiveness and stay current on trends. Thus, an incomplete understanding of security leads executives to think all is well.

Over 40% of executives express complete satisfaction with their organization's cyber security, according to CompTIA's report. In contrast, only 25% of IT staff and 21% of business staff are satisfied. This could also be accounted for by executives often having more tech freedom for added convenience while frontline staff deal with less visible cyber security details.

continued on page 2...

...continued from cover

"Either way, the gap in satisfaction points to a need for improved communication on the topic," CompTIA writes.

Get your IT and business teams together and figure out what risks you face right now and what needs to change. Because cyber security is constantly changing, your security should never be stagnant. "Good enough" is never good enough for your business; vigilance and a continuous improvement mindset are the only ways to approach cyber security.

Myth 2: Cyber Security Keeping Threats Out

Fact: Cyber security protects against threats both inside and outside your organization.

One of the most publicized breaches of the last decade was when BBC reported that a Heathrow Airport employee lost a USB stick with sensitive data on it. Although the stick was recovered with no harm done, it still cost Heathrow £120,000 (US$150,000) in fines.

Yes, cyber security is about protection. However, protection extends to both external and internal threats such as employee error.

Because security threats are diverse and wide-ranging, there are risks that have little to do with your IT team. For example, how do your employees use social media? "In an era of social engineering, there must be precise guidelines around the content being shared since it could eventually lead to a breach," CompTIA states. Attacks are increasingly focused on human social engineering, like phishing, and criminals bank on your staff making mistakes.

Additionally, managing relationships with third-party vendors and partners often involves some form of data sharing. "The chain of operations is only as strong as its weakest link," CompTIA points out. "When that chain involves outside parties, finding the weakest link requires detailed planning."

Everyone in your organization is responsible for being vigilant and aware of security best practices and safety as it relates to their jobs. Make sure your cyber security strategy puts equal emphasis on internal threats as much as external ones.

Myth 3: IT Handles My Cyber Security

Fact: Cyber security is not solely the responsibility of the IT department.

While IT professionals are crucial in implementing security measures comprehensive cyber security involves a multidisciplinary approach. It encompasses not only technical aspects but also policy, development, employee training, risk management and a deep understanding of the organization's unique security landscape.

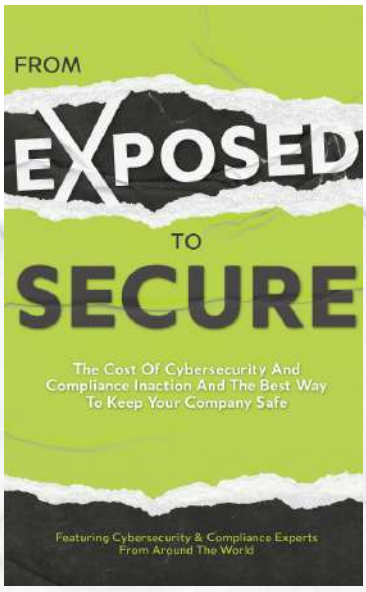
Because each department within your organization involves unique risks, people from various roles must be included in security conversations. But many companies are not doing this. CompTIA's report shows that while 40% of respondents say that technical staff is leading those conversations, only 36% indicate that the CEO is participating, and just 25% say that business staff is involved.

"More companies should consider including a wide range of business professionals, from executives to mid-level management to staff positions, in risk management discussions," CompTIA writes. "These individuals are becoming more involved in technology decisions for their departments, and without a proper view into the associated risks, their decisions may have harmful consequences."

Business leaders and employees at all levels must actively engage in cyber security efforts, as they are all potential gatekeepers against evolving threats.

Don't Listen To Myths

By embracing a mindset of continuous improvement, recognizing the wide range of threats and understanding the collective responsibility of cyber security, your business will remain safe, resilient and thriving, no matter what the future holds.



Lisa's NEW Book is an Amazon #1 Best Seller...

Cybercrime has developed into a billion-dollar industry. And as long as it's profitable to be a hacker or a scammer, these criminals *aren't* going away.

Featuring **TOP** cybersecurity and compliance professionals with **DECADES** of experience, *From Exposed To Secure* reveals the everyday threats that are putting your company in danger and where to focus your resources to eliminate exposure and minimize risk.

These experts share their experience in utilizing data protection regulations and **COMPLETE** security measures to protect your company from fines, lawsuits, loss of revenue, intellectual property theft, *and* reputational damage.

From Exposed To Secure delivers the crucial, smart steps every business must take to protect itself against teh increasingly prevalent and sophisticated cyberthreats that can destroy your company - including phishing, the Internet of Things, insider threats, ransomeware, supply chain, and zero day.

Consider this book the secret weapon that hackers never saw coming!

Find Out Where Your Business Could Be At Risk For A Cyber-Attack By Scheduling A Call: 877-954-4100 or visit www.cstsupport.com/discoverycall

Book is available on Amazon and online retailers like Walmart, Target and Barnes and Noble!

Most business leaders strive for one thing: to be a strong and competent leader of a high-performing team. To do this, they'll try just about anything, from free lunches to daylong team-building retreats. Although these are helpful, high-performing teams don't begin with external motivators. They begin when leaders embrace a culture of extreme ownership.

"Extreme ownership is pretty straightforward," Jocko Willink says. "You're not going to make any excuses. You're not going to blame anybody else. When something goes wrong, you're going to take ownership of those problems and get them solved."

Willink is the author of the New York Times bestseller Extreme Ownership: How U.S. Navy SEALs Lead And Win. He explains that the same leadership concepts that enable SEAL teams to succeed in the most intense circumstances can also help businesses win again and again.

As a young SEAL, Willink noticed that a culture of finger-pointing grew when blame was directed toward a person or a team. When that happens, "no one solves the problem," he says. However, when leaders owned issues and responsibility for finding a solution, the team reflected that ownership. "It actually made the other people inside the platoon have the same attitude. They'd say, 'It was my fault; let me fix it,'" Willink explains.

Eventually, Willink went on to fill leadership roles within the SEALs, learning to embrace personal accountability and team empowerment. Now a retired SEAL officer and co-founder of the leadership consulting firm Echelon, he's worked with hundreds of civilian companies on extreme ownership, finding the same results: when leaders take ownership of problems, the entire team is more likely to be high-performing and successful.

How To Create An Extreme Ownership Culture

"The biggest thing you've got to overcome is your ego," Willink explains. Pointing out that someone didn't do their job right or that the marketing plan wasn't carried out correctly doesn't solve the problem. "You're the boss. You own it," Willink says. When one person takes ownership, it spreads. "That's what develops the culture."

Although extreme ownership starts with the boss, the key to a high-performing team is to empower individuals to take responsibility for projects and tasks too.

"If you want people to take ownership, you have to give them ownership," Willink says. This way, you empower your team to make decisions while you serve as a reliable guide and offer direction when needed. "Put them in positions where they make decisions, make mistakes and learn to be honest with you," he says. If you're not getting the behaviors you need, you can study it and start to correct it by figuring out what support you can provide.

Willink points out that there will always be team members who don't embrace ownership. But when extreme ownership is a culture, they'll naturally get weeded out.

Those who are ready to step up, however, will rise to the top. "There's something more important to many people than how much money they make," he says. "That is control over their destiny, autonomy and freedom."

SHINY NEW GADGET OF THE MONTH

JSAUX USB Data Blocker

Last year, the FBI warned consumers not to use public charging stations because hackers were installing malware into USB ports and stealing data. If you forget your charger, the JSAUX USB-A Data Blocker is a game-changer for secure charging when you're on the go.

Designed exclusively for charging with no data-sync function, it's perfect for public charging stations in airports, hotel lobbies and coffee shops, eliminating hacking risks. It offers a rapid 2.4A charge and works with a wide range of devices. Compact, portable and cheap, the USB Data Blocker is the no-brainer companion you need in your travel backpack right now!

FREE EDUCATIONAL REPORT DOWNLOAD:

16 Questions You **MUST** ask before Hiring any I.T. Company

You'll Discover:

- The single most expensive mistake most small business owners make when hiring an I.T. consultant.
- The surprising reason most small businesses fall victim to sub-standard support
- How to avoid expensive computer repair bills and get all the computer support you need for a low, fixed monthly rate.

Claim your FREE copy today at
https://www.cstsupport.com/16questions/

(continued from front cover)

As you may have figured out by now, I am NOT a salesperson – I actually prefer not to "SELL" but rather to educate (our motto for 2024). Now this does not mean I do not come across as a salesperson. I LOVE what I do…. I'm actually pretty passionate about it…..and I LOVE that CST's customer service levels are one of the highest in the industry. If that comes across as "selling", I'm okay with that. Your IT Firm should love what they do.

What's even more important is that you have a number to call! We want you to make great decisions when it comes to your technology so just call us. We will offer expert advice to any business who needs it. It's that simple.

As we step into 2nd quarter of 2024, CST is busy doing third party risk assessments and penetration testing. As part of the Federal Trade Commission's (FTC) compliance requirements, businesses are required to run these assessments to ensure consumer information is protected. If you collect financial data such as a credit application, you fall under this scrutiny. This third-party assessment is crucial to find the gaps, if there are any, before a hacker does. Reach out if you would like more information.

I want to thank everyone who reached out about our VOIP solution. We are confident it will either save you money or provide you with added features you need but do not currently have...or both! Michelle and I are working on getting quotes out so please be patient as we have a pretty substantial list to get through.

Finally, I am hosting a "Client's ONLY" webinar on April 10th at 10am. This is specifically designed for our clients and I will be sharing IMPORTANT information. PLEASE PLAN ON ATTENDING and register as soon as you get the invite in your email. If you are NOT getting those invites, please call my office and talk to Sara. She will make sure your email is correct. As a reminder, please do NOT "opt-out" of receiving emails from me. If you feel we are bombarding you with emails, call and talk to Sara or Michelle. They will limit the number of emails we send to you.

Thanks everyone - Happy Spring and get those 2nd quarter goals written down and implemented.

As Always,

"passionate NOT pushy"

Lisa

CHECK FRAUD CRIMES ARE "WASHING" AWAY BANK ACCOUNTS

Headlines are usually flush with the latest digital breaches out to get businesses. Weak passwords, complex social engineering and business e-mail compromise are often the culprits we hear about. But while our eyes and ears were honed in on digital threats, old-fashioned paper-and-pen crimes were sneaking into our bank accounts.

According to the Financial Crimes Enforcement Network, fraudulent-check crimes rose 201.2% between 2018 and 2022. Experts say that the rise of check fraud began in 2020 when criminals started stealing stimulus checks. Once those ended, they needed a new source of income. In 2023, S&P Global noted that check fraud made up one-third of all bank fraud, excluding mortgage fraud.

It's a cheap and relatively simple crime happening under our noses, and that's why they're getting away with it.

How Criminals "Wash" Checks

AARP says that most check fraud involves check "washing." This is when criminals use bleach or acetone to wash away the ink used to write the payee and check amount after stealing it from your mailbox or fishing it from a drop box. Once washed, the check dries, is filled out with new information and deposited at banks or cash-checking shops.

According to AARP, a 60-year-old man had a check for $235 stolen and cashed for $9,001.20 – all within 24 hours. It's not just the US either. An Ontario business owner sent a check for $10,800 to the Canada Revenue Agency to make tax payments for his maple syrup company. Days later, it had been stolen and deposited into another account.

It's a low-budget, fast-cash reward for criminals. Even worse, some banks have deadlines for reporting this kind of crime and won't reimburse you if you alert them too late.

Prevent Check Fraud With These 6 Tips

Thankfully, there are a few simple steps you can take to significantly reduce your risk of check fraud.

1. Pay Online: Pay bills online using a private Wi-Fi connection and a secure portal, like through your bank or vendor website.

2. Mail Safely: Use the post office for mailing checks; avoid leaving them in personal or outdoor mailboxes.

3. Use Gel Ink: Use non-erasable gel ink in blue or black for writing checks; these are harder to erase than ballpoint pen ink.

4. Collect Mail Daily: Pick up your mail daily. If away, arrange for collection.

5. Monitor Your Accounts: Regularly check your bank account online – a few times a week is best.

6. Report Incidents Immediately: Report fraud quickly to your bank and Postal Inspection Service. Most institutions are required to reimburse stolen funds if the theft is reported within 30 days.

It might be a digital world, but criminals will use every tactic to get hold of your hard-earned cash. Add these simple tips to your routine to significantly reduce your risk of check fraud.

THE GENERATION MOST PRONE TO PHONE-RELATED ACCIDENTS WILL SURPRISE YOU

It's time millennials stop making fun of their elders for butt dials, weird FaceTime angles and other tech snafus. According to data from the National Electronic Injury Surveillance System, millennials are more prone to embarrassing tech-related accidents than any other generation. Since 2020, injuries across the board have shot up 20%, likely due to people being home more during the pandemic. The biggest culprit: people lifting televisions, resulting in strains and sprains (lift with your legs, people!). This accounts for 30% of injuries in the US. Unsurprisingly, walking and using a cellphone is runner-up, causing 23% of tech-related boo-boos. Eyes up, friends!

SPRING HAS SPRUNG

We have been eagerly awaiting blooming flowers and the warm weather. Winter is always hard in Northern NY, so when we get a hint of nicer weather, we start a silent argument with Mother Nature to hurry it up already!

Spring gives us the sense of renewal and fresh beginnings. A little spring cleaning and home or office refresh can really go a long way. So while you're starting your garden seeds and rearranging the furniture remember to take a few minutes to enjoy the change in season.

While you are doing that, be sure to reach out to Tyler if your technology is running a little slow. We will do a little spring cleaning there as well.

=Jessica=

Important Dates in April

1st – April Fools
8th – Solar Eclipse
11th – National Pet Day
15th – Tax Deadline
24th – Administrative Professionals Day

Tech Humor...

QUESTION:
What happened when the computer hit the floor?

"FREE UP COMING WEBINAR"

CLIENTS ONLY
A MUST WATCH - NEED TO KNOW Webinar

Join Lisa for a 30-minute LIVE webinar on:

Wednesday
April 10, 2024
at 10:00 am

- Some Critical Information Our Clients MUST Know NOW!
- Updates From YOUR Tech Team
- Security Protocol Highlight
- We Need Your Cooperation….

For The Full Details And To Register, Go Online To:
www.cstsupport.com/webinar

Q & A with Carrie

your friendly Account Manager

Dear Carrie,
Why do I need to add Multi Factor Authentication to my emails? Isn't my password enough?

Signed,
No More Apps

Dear No More Apps,

That is a great question. While you may have a strong password for your email, that password is still able to be hacked and once they get it, hackers can wreak havoc on your emails including sending them on your behalf. When you add 2fa (Multi Factor Authentication) to your email accounts, no matter if your password is stolen anyone who tries to login to your email will need a code that is specific to YOUR phone. Without that code, they can't do anything. With the level of hacking that we see happen on a daily basis, it is good to add Multi Factor Authentication to any online accounts that you have (emails, Facebook, Banking, etc.).

TURNING DOWN THE VOLUME ON STRESS:

Why Leaders Are Choosing Mindfulness Over Hustle

Meditation and mindfulness practices have been studied in a range of contexts – from college students to hardened marines (who showed faster stress recovery with mindfulness-based mind fitness training). Leaders who meditate think more clearly, stay calm in chaos and make smarter decisions. You don't need a mountain retreat to channel the Zen; meditation apps like Headspace, Calm and Insight Timer provide pocket-sized guided sessions to ease into this practice anywhere, anytime.

Want to meditate without interruptions? Just hit "Do Not Disturb" on your phone. On Android, swipe down and tap "Do Not Disturb." Apple folks, find it under "Settings" > "Focus" > "Do Not Disturb." Customize it to keep those calls and notifications quiet. This way, you can meditate peacefully and stay sharp for those big business moves.

ANSWER: It slipped a disk

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

Lisa Brown's #1 Amazon Best Selling BRAND NEW BOOK!

Cybercrime has developed into a billion-dollar industry. And as long as it's profitable to be a hacker or a scammer, these criminals *aren't* going away.

Featuring cybersecurity and compliance professionals with of experience, ***From Exposed To Secure*** reveals the everyday threats that are putting your company in danger and where to focus your resources to eliminate exposure and minimize risk.

These experts share their experience in utilizing data protection regulations and C security measures to protect your company from fines, lawsuits, loss of revenue, intellectual property theft, *and* reputational damage.

Find Out Where Your Business Could Be At Risk For A Cyber-Attack By Scheduling A Call:

https://www.cstsupport.com/discoverycall/

AMAZON 1# BEST SELLER

https://www.cstsupport.com/from-exposed-to-secure/