www.cstsupport.com

JUNE 2025

CST TECHNOLOGY TIMES

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

"passionate NOT pushy"

Embracing Change: A Constant Journey

Change is an inevitable part of life. It happens every second of the day, often without us realizing it. From the subtle shifts in our environment to the monumental changes in our personal and professional lives, change is a constant companion. Yet, despite its ubiquity, many of us struggle with embracing it. The uncertainty it brings can be daunting, and the comfort of the familiar often keeps us anchored in the status quo.

This past month, I was bombarded with change both positive and negative.

An update on the positive; we officially moved into our home in Florida. As most of you know, our children and grandchildren live in Punta Gorda and we have been travelling back and forth for over 16 years. Our accommodations were a 36' camper on our daughter's property and although it was everything it needed to be, it certainly was not ideal for work. Last November, we took the plunge and hired a contractor to build our home. We officially moved in on April 30th. This entire task was daunting but worth the wait as it is everything we need it to be all while being manageable as a second home. For those of you questioning our residency,

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

SHADOW IT:

How Employees Using Unauthorized Apps Could Be Putting Your Business At Risk

Your employees might be the biggest cybersecurity risk in your business – and not just because they're prone to click phishing e-mails or reuse passwords. It's because they're using apps your IT team doesn't even know about.

This is called Shadow IT, and it's one of the fastest-growing security risks for businesses today. Employees download and use unauthorized apps, software and cloud services – often with good intentions – but in reality they're creating massive security vulnerabilities without even realizing it.

What Is Shadow IT?

Shadow IT refers to any technology used within a business that hasn't been approved, vetted or secured by the IT department. It can include things like:

- Employees using **personal Google**
- **Drives or Dropbox accounts** to store and share work documents.
- Teams signing up for **unapproved project management tools** like Trello, Asana or Slack without IT oversight.
- Workers installing **messaging apps like WhatsApp or Telegram** on company devices to communicate outside of official channels.
- Marketing teams using **AI content generators** or automation tools without verifying their security.

Why Is Shadow IT So Dangerous?

Because IT teams have no visibility or control over these tools, they can't secure them – which means businesses are exposed to all kinds of threats.

- **Unsecured Data-Sharing** – Employees using personal cloud storage, e-mail accounts or messaging apps can accidentally leak sensitive company information, making it easier for cybercriminals to intercept.
- **No Security Updates** – IT departments regularly update approved software to patch vulnerabilities, but unauthorized apps often go unchecked, leaving systems open to hackers.
- **Compliance Violations** – If your business falls under regulations like HIPAA, GDPR or PCI-DSS, using unapproved apps can lead to noncompliance, fines and legal trouble.
- **Increased Phishing And Malware Risks** – Employees might unknowingly download malicious apps that appear legitimate but contain malware or ransomware.

continued on page 2…

...continued from cover

- **Account Hijacking –** Using unauthorized tools without multifactor authentication (MFA) can expose employee credentials, allowing hackers to gain access to company systems.

Why Do Employees Use Shadow IT?

Most of the time, it's not malicious. Take, for example, the "Vapor" app scandal, an extensive ad fraud scheme recently uncovered by security researchers IAS Threat Labs.

In March, over 300 malicious applications were discovered on the Google Play Store, collectively downloaded more than 60 million times. These apps disguised themselves as utilities and health and lifestyle tools but were designed to display intrusive ads and, in some cases, phish for user credentials and credit card information. Once installed, they hid their icons and bombarded users with full-screen ads, rendering devices nearly inoperative. This incident highlights how easily unauthorized apps can infiltrate devices and compromise security.

But employees can also use unauthorized apps because:

- They find company-approved tools frustrating or outdated.
- They want to work faster and more efficiently.
- They don't realize the security risks involved.
- They think IT approval takes too long – so they take shortcuts.

Unfortunately, these shortcuts can cost your business BIG when a data breach happens.

How To Stop Shadow IT Before It Hurts Your Business

You can't stop what you can't see, so tackling Shadow IT requires a proactive approach.

Here's how to get started:

1. Create An Approved Software List

Work with your IT team to establish a list of trusted, secure applications employees can use. Make sure this list is regularly updated with new, approved tools.

2. Restrict Unauthorized App Downloads

Set up device policies that prevent employees from installing unapproved software on company devices. If they need a tool, they should request IT approval first.

3. Educate Employees About The Risks

Employees need to understand that Shadow IT isn't just a productivity shortcut – it's a security risk. Regularly train your team on why unauthorized apps can put the business at risk.

4. Monitor Network Traffic For Unapproved Apps

IT teams should use network-monitoring tools to detect unauthorized software use and flag potential security threats before they become a problem.

5. Implement Strong Endpoint Security

Use endpoint detection and response (EDR) solutions to track software usage, prevent unauthorized access and detect any suspicious activity in real time.

Don't Let Shadow IT Become A Security Nightmare

The best way to fight Shadow IT is to get ahead of it before it leads to a data breach or compliance disaster.

Want to know what unauthorized apps your employees are using right now? Start with a Network Security Assessment to identify vulnerabilities, flag security risks and help you lock down your business before it's too late.

FREE REPORT:

What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This report will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

PROTECT YOUR NETWORK

"What Every Business Owner Must Know About Protecting and Preserving Their Network"

Don't Trust Your Company's Critical Data And Operations To Just Anyone!

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

CARTOON OF THE MONTH

"I understand your concerns, but there's a chain of command. Have you spoken to the sheepdog?"

CULTURE AND TRUST:

A $1M GROWTH FORMULA

When it comes to entrepreneurship, sometimes your biggest obstacle is you—and getting out of your own way and empowering employees is the recipe for success. Here are a few tried-and-true entrepreneurial mindset shifts from other business owners that pushed them closer to success.

The Biggest Entrepreneurial Challenge: Delegation

Learning how to step away—and get out of your own way—is one of the biggest lessons many entrepreneurs must learn. When you start a business, you're running everything. You're wearing all the hats. However, in order to grow, you have to face the fact that there's only so much time in a day. You simply don't have time to work in the trenches and scale the business.

Hiring good, capable people and trusting them enough to take tasks off your plate is critical to your business' success. After all, as the company's leader, it's important to strategically spend your time—not just stay busy. Delegate what you can, and focus on setting the vision and strategies that will keep your business moving forward.

Shaping The Culture With A Family Dynamic

There are a few factors that are key to a healthy company culture. An open line of communication is one of the biggest. Listening to what your team needs—even if it's unconventional—and giving it a fair shot can make all the difference. Just be sure to clarify up front that if productivity or the quality of your deliverables slips, it'll be straight back to the way things were before.

If it works, your business has a thriving new dynamic, potentially increasing productivity and workplace satisfaction. But even if it doesn't, your team will feel heard, respected and like you've got their backs. And that makes all the difference when it comes to creating a strong, trust-based company culture.

If you're not sure where to go next, don't underestimate the value of picking up some books on creating a strong culture. Take advice from entrepreneurs who have been there, done that and begin incorporating the ideas you like best into your own business. After all, if it worked for them, it might just work for you.

Focus On "Done", Not "Perfect"

From creating processes to marketing, things are better done than perfect. Perfectionism can seriously hold you back. Instead, come up with a plan and implement something. It doesn't have to be exactly right. You can always make tweaks along the way, but if you never take the leap and execute, you'll never get anywhere. So put the planning notebook down, and get implementing!

Entrepreneurship will never be the easy road, but with some essential shifts to your mindset and a great team around you, many challenges don't seem quite so insurmountable.

...Continued from cover

we are NOT moving to Florida - it will simply be our second home and a great place to enjoy family and be able to grow our business there.

I was also presented with a medical challenge that was definitely not expected but after going through surgery, all is well. I continue to be amazed at the medical advances and am thankful I was in the right place at the right time for quick action and expert care.

Now, in today's fast-paced world, technology is at the forefront of driving change, whether you like it or not. Innovations emerge at a dizzying pace, reshaping industries, and altering the way we interact with the world. Have you considered how your organization is utilizing to use AI? The digital revolution has permeated every aspect of our lives, making change even more prevalent and noticeable. I think the struggle comes as a double-edged sword – while technology brings convenience and efficiency, it also demands adaptation and learning.

At CST, we understand the challenges that come with technological advancement and the rapid pace of change. We are committed to ensuring that security remains a priority amidst this evolving landscape. Please know that as we adopt new technologies and implement innovative solutions, we are acutely aware of the risks and vulnerabilities that arise. Our dedicated team works tirelessly to safeguard your systems and data, employing the latest security measures to protect against threats.

Embracing change means being open to learning, being resilient in the face of challenges, and being proactive in finding solutions. This is where we hope you consider CST your partner in growth. We have a unique perspective and incredible resources to facilitate most technological changes so, as you consider new processes and procedures and new software and hardware, we hope you will loop us in to guide you in making really great decisions when it comes to growing your business. Transparency and collaboration are cornerstones of our approach, helping us to build trust and to create a supportive environment where change is seen as a shared journey.

As we close out second quarter, here are a few items I want you to ensure are on your radar:

1. Windows 10 computers – upgraded or replaced – deadline on this is October 14th.
2. Training Opportunities – we love to educate and have a full spectrum of courses to guide you and your staff. Email Jessica for details – jessica@cstsupport.com

Remember, change is a powerful force that shapes our world every second of the day. While it can be challenging to embrace, it also brings opportunities for growth and innovation. We strive to turn the challenge of change into a pathway for success.

Have a beautiful June and to all the Dad's - Happy Father's Day!
As Always,
"passionate NOT pushy"
Lisa

IS YOUR PRINTER THE BIGGEST SECURITY THREAT IN YOUR OFFICE?

If I asked you to name the biggest cybersecurity threats in your office, you'd probably say phishing e-mails, malware or weak passwords. But what if I told you that your office printer – yes, the one quietly humming in the corner – could be one of the biggest vulnerabilities in your entire network?

It sounds ridiculous, but hackers love printers. And most businesses don't realize just how much of a security risk they pose – until it's too late. In 2020, Cybernews ran what they called the "Printer Hack Experiment." Out of a sample of 50,000 devices, they successfully compromised 56% of the printers, directing them to print out a sheet on printer security. That's nearly 28,000 compromised devices – all because businesses overlooked this "harmless" piece of office equipment.

Wait, WHY Target Printers?

Because printers are a goldmine of sensitive data. They process everything from payroll documents and contracts to confidential client information. And yet, most businesses leave them wide-open to attack.

Here's what can happen when a hacker gains access to your printer:

- **Printers store sensitive data** – Every time you print, scan or copy a document, your printer keeps a digital copy. Many printers have built-in hard drives that store years' worth of documents, including payroll files, contracts and employee records. If a hacker gains access, they can steal or even reprint those files without your knowledge.
- **Default passwords are a hacker's dream** – Most printers come with default admin logins like "admin/admin" or "123456." Many businesses never change them, making it easy for cybercriminals to take control.
- **They're an open door to your network** – Printers are connected to your WiFi and company network. If compromised, they can be used as an entry point to install malware or ransomware, or steal data from other devices.
- **Print jobs can be intercepted** – If your print jobs aren't encrypted, hackers can intercept documents before they even reach the printer. That means confidential contracts, legal documents and even medical records could be exposed.
- **They can spy on your business** – Many modern printers have built-in storage and even scan-to-e-mail features. If a hacker compromises your device, they can remotely access scanned documents, e-mails and stored files.
- **Outdated firmware leaves the door wide-open** – Like any device, printers need security updates. But most businesses never update their printers' firmware, leaving them vulnerable to known exploitations.
- **Data mining from discarded printers** – Printers that were improperly disposed of can be a goldmine for cybercriminals. Residual data stored on discarded printers can be mined for sensitive information! This can result in potential security breaches. Printers need to have their storage wiped clean to avoid being vulnerable to data breaches and legal liabilities.

How To Protect Your Printers From Hackers

Now that you know printers can be hacked, here's what you need to do immediately:

1. Change The Default Password – If your printer still has the default login credentials, change them immediately. Use a strong, unique password like you would for your e-mail or bank account.

2. Update Your Printer's Firmware – Manufacturers release security patches for a reason. Log into your printer settings and check for updates or have your IT team do this for you. 3. Encrypt Print Jobs – Enable Secure Print and end-to-end encryption to prevent hackers from intercepting print jobs.

4. Restrict Who Can Print – Use access controls so only authorized employees can send print jobs. If your printer supports PIN codes, require them for sensitive print jobs. You can also add a guest option.

5. Regularly Clear Stored Data – Some printers let you manually delete stored print jobs. If yours has a hard drive, make sure it's encrypted, and if you replace a printer, wipe or destroy the hard drive before disposal.

6. Put Your Printer Behind A Firewall – Just like computers, printers should be protected by a firewall to prevent unauthorized access.

7. Monitor Printer Activity – If your IT team isn't already tracking printer logs, now is the time to start. Unusual print activity, remote access attempts or unauthorized users printing sensitive documents should be red flags.

Printers Aren't Just Office Equipment – They're Security Risks

Most businesses don't take printer security seriously because, well, it's a printer. But cybercriminals know that businesses overlook these devices, making them an easy target.

If you're protecting your computers but ignoring your printers, you're leaving a huge hole in your cybersecurity defenses.

SCHOOL IS OUT, SCREENS ARE ON

The school year is coming to an end, and kids will be home and using their electronics more. With an increase in online gaming, social media, and streaming it is important to keep an eye on their activity.

I think its easy to say that kids these days grew up with phones and computers. Most of the time they know more about technology than some adults. This is why it is important to be aware of the risks that come with internet access.

Key Risks to Be Aware Of:

- Inappropriate content (YouTube, TikTok, games)
- Online predators (chatrooms, games, social media)
- Cyberbullying (more social interaction online)
- Privacy leaks (oversharing personal info)
- Scams targeting kids (fake contests, free game codes, phishing)

Don't worry parents! There are things you can do to help your child enjoy their screen time safely. Here are some tips for a safe digital summer…

- Set screen time boundaries – balance online and offline play.
- Use parental controls – on devices, apps, browsers.
- Create a tech agreement – outline rules for online behavior.
- Teach personal info protection – don't share full names, locations, school names.
- Keep devices in common areas – especially for younger children.

We understand that screen time is inevitable when the kids are home all summer. Just keep in mind that kids are not the only ones on the internet. Teaching our kids about location-sharing, strangers online and cyberbullying will set them up for success. A safe digital summer means peace of mind for parents and healthy online habits for kids that last all year. =Jessica=

Important Dates in June

Happy Internet Safety Month

6th- National Donut Day

15th- Fathers Day

19th- Juneteenth

21st- Summer Solstice

27th - National Sunglasses Day

Passionate NOT Pushy WITH LISA BROWN

Introducing "Passionate Not Pushy" – A Podcast for Bold Thinkers!

I'm thrilled to introduce my new podcast, Passionate Not Pushy—where bold ideas meet authentic conversations!

In business and life, passion is a powerful force—but there's a fine line between being driven and being pushy. This podcast is for entrepreneurs, creators, and anyone who wants to lead with heart, build meaningful connections, and make an impact—without the pressure.

Each episode, we'll explore real stories, strategies, and insights that help you stay true to who you are while turning passion into success.

SUBSCRIBE

Don't Forget To Subscribe!

ATTENTION

Windows 10 Support Is Ending And Your Office Will Be Vulnerable To Data Breaches

Find Out What This Means For YOU!

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

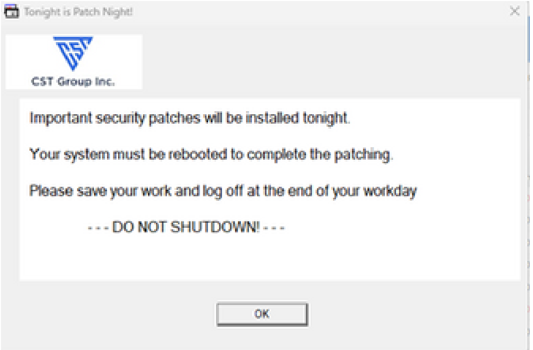
If you've been following the latest news in cybersecurity, you know that attacks have only continued to grow in both size and sophistication. However, you might not be aware that small and mid-sized businesses like yours are the most targeted by Dark Web criminals. Would you be among the 60% of SMBs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

Shawn's Security Corner

Part of CST's security protocol is our management of Windows security patches. We are hoping to clarify how the process works and what your part in this security process is and how necessary it is to ensure we keep you up-to-date and secure.

Wednesday morning everyone will see a white notification box on your screen (see below screenshot).



Important security patches will be installed tonight.

Your system must be rebooted to complete the patching.

Please save your work and log off at the end of your workday

- - - DO NOT SHUTDOWN! - - -

As the notification states, you need to, at the end of your workday Wednesday, save your work, LOG OUT and leave your computer on and connected to internet. The simplest way to achieve this is to just restart your computer at the end of your workday and walk away. This will accomplish the log out and your computer will be ready to do patches - we take care of the rest Wednesday evening after hours.

If your computer user does NOT have a password, please add one to enhance security measures.

If you follow these simple steps, you will not encounter any issues when you log into your computer on Thursday.

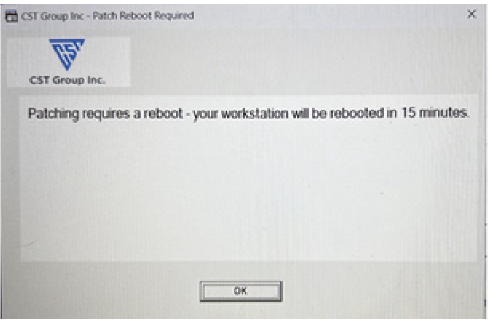
*****NOTE*** If your system is not on and connected to the internet so this process can complete on Wednesday evening, then you are going to experience the following.**

When your system is turned back on and connected to the internet, our software is going to run the updates AND FORCE a restart of your system with a notification giving you 15 minutes to save your work. Then it restarts!

This can be very disruptive to those who do not follow the process and ignore the warning. All work they/you have done that was not saved will be lost!

We understand the struggles, but our job as your security team is to ensure every computer is updated, patched and scanned. We need your cooperation in this. Please simply restart your system Wednesday at end of day!

Dedicated to your Security,
The CST Tech Team



Patching requires a reboot - your workstation will be rebooted in 15 minutes.

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.

WHO MAKES AN IDEAL REFERRAL?

- **Any business with 10 or more computers**
- **Needs help with security, compliance, backup, support or network**
- **Wants 24/7/365 peace of mind**

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

Important Backup Information

Keep Your System Online for Scheduled Backups

To ensure the security and integrity of your business data, it's essential that your computers remain powered on and connected to the internet during scheduled backup times.

Here's why:

1. Uninterrupted Backup Execution – Your system must be online for scheduled backups to run. If a device is turned off, the backup cannot initiate, leaving your data unprotected.
2. Cloud Backup Synchronization – If your backups are stored in the cloud, a stable internet connection is required to upload files securely and ensure data is up to date.
3. Security & Compliance – Regular, completed backups help meet compliance requirements and protect against potential data loss from cyber threats, hardware failures, or accidental deletions.
4. Automatic Updates & Maintenance – Keeping your system online allows our team to apply necessary updates and monitor backup health, ensuring optimal performance and security.

To avoid any disruptions in your data protection plan, please make sure your devices remain powered on and connected during backup windows