CST TECHNOLOGY TIMES

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

"passionate NOT pushy"

By Lisa Brown, CEO & Founder

Shawn and I were recently asked what our "exit" strategy was for CST. Honestly, neither of us had given it much thought. Well, that isn't totally true, I have given it thought…. DEATH! That was my exit strategy. Now that I think about it with more intent, the dying part would certainly not have been fair for either our employees or our family. I know that may sound strange, maybe even a little harsh to some of you looking to "get out" of your business at some point, but here's the thing….I do not want to retire. Both Shawn and I LOVE what we do! It is not "work" for us – it is a mission and believe it or not, we are positioning it to fit in to our lifestyle. Yes, we are going to slow down, take more vacations, spend more time with family, but if we do it right, this company, our team, will continue to thrive.

I bring this up because we celebrate Mother's Day this month which gives me the perfect opportunity to brag about my mom. You see, she is 92 years old, lives independently, drives and YES, still works! She and my dad were founders of H & C Robinson Contractors. After my dad passed away in 1993, my brother Scott took over, but my mom still goes to work every morning. It is what motivates her to get out of bed knowing she has tasks to complete and employees to take care of. Although my brother is hugely successful and has grown the company, I am pretty sure this was not his dream.

(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.

WHY 60% OF DATA BACKUPS FAIL BUSINESSES WHEN THEY NEED THEM MOST

From natural disasters and cyber-attacks to accidental deletion, there are many reasons a business needs to back up its data. However, Avast's latest findings on disaster recovery highlight an alarming issue for small and medium-sized businesses (SMBs): 60% of data backups are not fully successful, and half of the attempts to recover data from these backups don't work. This leads to businesses being offline for an average of 79 minutes, costing them roughly $84,650 for every hour of downtime.

Still, not all backups are created equal. It's important you're aware of backup best practices, so you're confident your backup solution will work when you need it most.

Why Backups Are Failing

There are a few common reasons backups are incomplete or a restoration fails:

- **Backup products are unreliable:** When it comes to backups, you get what you pay for. Free or cheap solutions may not offer the robust features of more expensive products. This can result in backups that are not as secure or reliable.
- **Backup times are not optimal.** If backups are scheduled during high-traffic periods or when data is being heavily modified, there's a risk that not all data will be captured.
- Compatibility issues. **As your business e**volves, so do your systems and software. However, new systems may not always be fully compatible with existing backup solutions. This can lead to situations where data is not properly saved or, even if it is, cannot be restored correctly because the formats or systems are no longer aligned.
- **Human error.** Mistakes such as incorrectly configuring backup parameters, accidentally deleting crucial files or ignoring backup schedules and alerts can lead to backup failures.

continued on page 2...

...continued from cover

Cyber-attacks and other disasters are a constant threat. If your backup fails and you get hacked, you might lose data permanently. Additionally, health care and finance organizations have strict compliance regulations around data handling, and failed backups can result in fines, legal challenges and a damaged reputation.

Best Practices For Successful Data Backup And Restoration

Reliable data backups and successful restoration are your lifeline in times of crisis. From choosing the right backup solution to regular testing and daily monitoring, these best practices protect your data from surprise disruptions, ensuring your business doesn't miss a beat, no matter what comes your way.

1. Pick a solid backup solution.

Don't just go for the big names in backup software; some might not deliver what they promise. Digging deep and finding a solution that suits your needs is essential. For example, immutable backups are a must-have for anyone needing to meet strict compliance rules, as they can't be changed or deleted, even by a ransomware attack. Talk with your IT provider about the backup technologies they're using for you, how quickly you can expect to recover data, what kind of downtime you might face and whether your backups are on the cloud, local or a mix of both. Make sure your backup ticks all the boxes for compliance, especially if you're in a sensitive field like health care.

2.Use the 3-2-1 rule.

Once you have a reliable backup solution, consider using the 3-2-1 backup rule, a standard set of best practices for data recovery. The rule recommends storing three copies of your data in two different formats, with one copy stored off-site. This significantly reduces your risk of total data loss.

3. Make sure a backup status report is being generated daily.

Ensure someone – either you or someone on your IT team – is checking the backup status every day. Incomplete backups should be followed up on immediately. Even if your IT team receives a daily report, ask to have a weekly or monthly report delivered to you too, so you can verify that your backups are successful.

4. Do regular restore tests.

Like a fire drill for your data, do a trial run and restore some files or even the whole server every few months to ensure everything works as it should. It's one thing to have backups, but another to ensure they are in good condition and the data can be retrieved as expected.

Don't Ignore Your Data Backups!

Backups might seem like one of those "set and forget" tasks, but when disaster strikes – be it a flood, fire or cyber-attack – your backup could be what saves your business. If you haven't already, start a conversation with your IT provider and make sure your backup strategy is solid and reliable.

"FREE UP COMING WEBINAR"

Join Lisa for a 30-minute LIVE webinar on:

"Essential Documentation for Small Business Owners: What You Need to Have to Cover Your A$$"

Wednesday, March 8, 2024 at 9:00 am

- Streamlining Account Management: Easy Strategies for Organizing Your Accounts and Passwords
- Securing Your Sensitive Data: Best Practices for Protecting Your Information
- Choosing the Right Storage: Exploring Secure Options for Storing Vital Information
- Centralizing and Safeguarding: Strategies for Efficiently Managing, Protecting, and Sharing Critical Information

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

July 20, 1969, just eight years after President Kennedy made one of history's most ambitious declarations – the US would send a man to the moon and back – Neil Armstrong and Edwin "Buzz" Aldrin became the first people to set foot on the moon.

Today, Buzz is a philanthropist, author and renowned speaker who shares what being a space pioneer taught him about life on Earth: no mission is completed alone, failure is a crucial milestone of success and to never stop envisioning your next impossible dream .

Lessons From "The Moonman"

Dream The Impossible

Aldrin remembers President Kennedy's announcement in 1961, and although he wasn't sure how they'd do it, he said, "We did have a leader with that determination, the courage and the confidence that we can get there." Without a leader brave enough to share an impossible vision, ideas never get off the ground. In business, it's crucial to give your team a meaningful vision to rally around, something they want to be a part of.

Behind Every Successful Mission Is A TEAM

The "backroomers" – software engineers, secretaries and even the tailors who manufactured spacesuits – were all necessary to Apollo's safe launch and return to Earth. When Apollo 11 landed, the world cheered. "People were not just cheering for three guys but for what we represented," Buzz recalled in a speech. "That by the nation and the world coming together, we had accomplished the impossible, and the true value of it is the amazing story of innovation and teamwork that overcame many obstacles to reach the moon."

Success is rarely the story of one person. Rather, it's often the story of many people working together. "There are a lot of people out there in the universe who wish you well and want to be your friend. Let them help you," Buzz said. "You don't have to carry it all on your own."

Failure Is A Mark Of Growth

In the book *No Dream Is Too High*, Buzz explains how everyone at NASA knew the risks involved in their mission. Only by planning for failure and testing every system, component and spacesuit zipper could they improve design and functionality – failure was part of the process.

"Some people don't like to admit that they have failed or that they have not yet achieved their goals or lived up to their own expectations," Buzz wrote. "But failure is not a sign of weakness. It is a sign that you are alive and growing."

Know What's Next

What happens when you accomplish what you set out to do after all the cheers and high-fives? After Apollo, Buzz wrote in the book Magnificent Desolation, "There was no goal, no sense of calling, no project worth pouring myself into."

He sunk into severe depression for years, finally realizing, "I needed to realign my direction and find a new runway."

Today, he's a speaker, author and philanthropist for STEAM-based education to help get the next generation of heroes to the moon – and beyond. Perhaps the key to lifelong fulfillment is never to "land" for too long – to keep learning, growing and achieving impossible things.

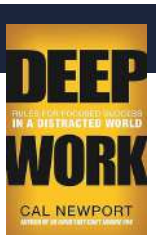
SHINY NEW GADGET OF THE MONTH

Amazon Basics 8-Sheet High Security Micro-Cut Shredder

Your recycling and garbage bins are a jackpot for identity thieves. Even if you don't handle CIA-level classified documents, criminals can use your recycled mail – like bank or credit card statements – to steal personal information. A shredder like the Amazon Basics 8-Sheet High Security Micro-Cut Shredder is an easy and affordable way to secure your information. You can shred up to eight pieces of paper simultaneously, with a five-minute continuous run time. Recycle the shreds, use it as packaging material or add it to your cat's litter box. Either way, a shredder keeps your information out of the hands of criminals.

By Cal Newport

DEEP WORK



It's undeniable: we're more distracted than ever. From text messages and e-mail pings to social media and our own disruptive thoughts, the relentless influx of distractions is sabotaging our productivity and even our ability to be present in our lives. *Deep Work*, by Cal Newport, is a compelling guide to help us take back our focus and cultivate more fulfillment in our work. Newport introduces readers to four "rules" to transform our minds and habits into a hyper-focused superpower: work deeply, embrace boredom, quit social media and drain the shallows. Through engaging stories and practical advice, the book outlines a framework for cultivating a deep work ethic, promising professional growth and a more profound sense of personal fulfillment. *Deep Work* is an essential read for those looking to navigate a distracted world with grace and achieve focused success.

(continued from front cover)

My question is, was this my parents "exit" strategy? In talking to my mom, she doesn't remember it ever being a topic of discussion which means they didn't have one. I dare say the company would have just organically slowed down for them until they were no longer able to work and then it would have either closed or another family member might have taken over? Who knows?

Which brings me back to an exit strategy being more of a succession plan. Shawn and I have been talking to our kids lately. They are all adults with hugely successful careers however, they see value in what their parents are doing and want that legacy to continue. Man, if you want to see two people excited about their kids showing interest in what they do – you should have seen the joy on my face. My two kids grew up with this company, went on plenty of service calls with me and have watched, with a keen eye, on how we are growing it.

Let me just say, it is incredible that we went from having death be our exit plan to now a generational business….it makes this mom a very happy woman.

So, what is your "exit" plan? If you haven't been thinking about it, maybe now is the perfect time.

On a separate note, all clients should have received an email from me regarding our new payment portal. This portal will allow our clients to view and pay their invoices - all with ease and transparency. Please be sure login, save your credentials and setup auto pay to make our lives a little easier. If you have any questions, or did not receive the email, please contact Jessica at the office. She will be happy to help.

Have a beautiful month. For those that lost a loved one while serving this country in the United States military, we honor and mourn your loss. To all the mom's reading - Happy Mother's Day!

As Always,
"passionate NOT pushy"
Lisa

DEEPFAKES ARE COMING TO THE WORKPLACE

Deepfakes result from people using AI and machine-learning technology to make it seem like someone is saying something they never actually said. Like every other tech on the market, it can be used with good and bad intentions. For example, David Beckham appeared in a malaria awareness campaign, and AI enabled him to appear to speak nine different languages. On the other hand, pornographic deepfakes of Taylor Swift went viral on X (to the horror of Swifties worldwide), and audio deepfakes of Biden encouraging New Hampshire voters not to cast ballots caused concern among experts.

However, deepfakes aren't happening only to high-profile politicians and celebrities – they are quickly making their way into the workplace. In April 2023, forensics research company Regula reported that one-third of businesses worldwide had already been attacked by deepfake audio (37%) and video (29%) fraud. Regula also noted that the average cost of identity fraud, including deepfakes, costs global SMBs $200,000 on average.

How Deepfakes Are Impacting The Workplace

While deepfake technology is used to commit a variety of crimes, there are two ways deepfakes currently cause harm to businesses like yours:

1. Impersonation/Identity Fraud Schemes
2. Harm To Company Reputation

One of the most common deepfake attacks is when AI impersonates an executive's voice to steal credentials or request money transfers from employees. Other attacks include deepfake videos or audio of a CEO or employee used to disseminate false information online that could negatively affect a brand. More than 40% of businesses have already experienced a deepfake attack, according to authentication experts at ID R&D.

What To Do About It

There are a few simple things you can do to prevent deepfakes from having damaging consequences on your business.

1. Review policies around technology and communication

Ensure you have transparent communication practices and that your team knows how communications are used internally. Would a company executive ever call an employee to place an official request for money or information? If not, employees should be suspicious. Also, encourage employees to verify any e-mail or phone request they aren't sure about.

2. Include deepfake spotting in cyber security awareness training

Double-check that your cyber security awareness training covers how to spot deepfakes. Things to look for include unnatural eye blinking, blurry face borders, artificial-looking skin, slow speech and unusual intonation.

3. Have a response plan

Deepfake attacks are in their infancy, and you can expect to see more attacks like this in the future. Be sure your company's leadership talks about how to respond if a deepfake attack impacts your company. Even though there's no perfect solution to the problem yet, the worst thing that can happen is to be caught unprepared.

SHOULD YOU VERIFY YOUR PROFILE ON LINKEDIN?

In 2022, LinkedIn launched verification options where most users can submit a personal ID, employer e-mail or workplace ID to prove they're a real person amid an increasing number of fake accounts. In the second half of 2021 alone, Microsoft (LinkedIn's parent company) removed over 15 million fake accounts. If you feel weird about sharing your biometric or ID information online, that makes sense. But verification isn't a bad idea because of the number of fake accounts on LinkedIn. Although LinkedIn reports using the highest security protections, consider using the employee e-mail option if it's available (employers must have a LinkedIn page and turn on this feature) because it's the least risky.

IT IS OUR YEAR

At CST we have announced that 2024 is our year to shine. We feel big things are coming our way and it has already started! With the launch of Lisa's #1 Amazon Best Seller Book to kick off this year right we are excited to see what else comes our way.

Don't worry though, we are not leaving our best year up to fate alone. We have planned and prepped some amazing things and are excited to have all of you along for the journey. Follow us on our socials so you can get all the details as we release them.

=Jessica=

Important Dates in May

4th- May the 4th Be With You
7th- Teacher Appreciation Day
8th – FREE Webinar with Lisa
9th – Resource & Job Fair with the Saranac Lake Chamber
12th – Mother's Day
27th – Memorial Day (OFFICE CLOSED)

Tech Humor...

QUESTION:
What did the baby supercomputer call their father?

"FREE UP COMING WEBINAR"

A MUST WATCH!
Essential Documentation for Small Business Owners: What You Need to Have to Cover Your A$$

Join Lisa for a 30-minute LIVE webinar on:

Wednesday
MAY 8th, 2024
at 9:00 am

- Streamlining Account Management: Easy Strategies for Organizing Your Accounts and Passwords
- Securing Your Sensitive Data: Best Practices for Protecting Your Information
- Choosing the Right Storage: Exploring Secure Options for Storing Vital Information
- Centralizing and Safeguarding: Strategies for Efficiently Managing, Protecting, and Sharing Critical Information

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

Q & A with Carrie

your friendly Account Manager

Dear Carrie,

I typically send emails with account information to clients and vendors. I have a company email that I use for this. But why am I being told I also need encryption if I am the only person using my email?

Sincerely,
Make This Make Sense

Dear Make This Make Sense,

If you are sending emails with ANY type of sensitive data (personal info, banking, credit card, birthdates etc) there is a chance that information can be intercepted on its way to the destination. Once you hit send, any information in emails is exposed to all of the cyber criminals out there on the internet. When emails are encrypted, the information is jumbled before being sent out into the internet world and the recipient gets notified that they have an encrypted email that they will have to login to an account to view.

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: Data

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/

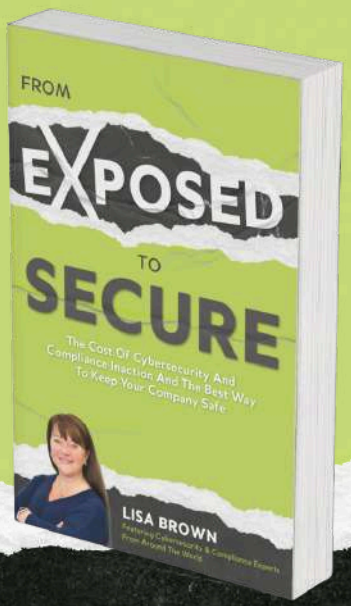
or call us at 1-877-954-4100

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/