CST TECHNOLOGY TIMES

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

"passionate NOT pushy"

By Lisa Brown, CEO & Founder

What is the potential risk of taking NO action?

I'm not just referencing technology and cyber security, but life in general!

It is said that the average adult makes 33,000-35,000 decisions a day. Some are menial, like what you are going to wear today, while others are life changing.

I read an article in Harvard Business Review, "*A Simple Way to Make Better Decisions*" written by Amanda Reill. Ms. Reill suggested implementing something called "morning pages" based on Julia Cameron's book, *The Artist's Way*. The premise is that every morning, before coffee, checking messages or technology, you journal your thoughts. There are no rules to this, just whatever happens to be on your mind. It could be about a dream you had, tasks you want to accomplish, relationships, gratitude, or whatever else is on your mind. The premise of this exercise is to center your thoughts and clear your head before you get started for the day. My thoughts? Genius! If I'm going to be making 33,000+ decisions a day, constantly evaluating risk with each decision, then I feel I need to be at the top of my game.

As you can imagine, I get a lot of ideas first thing in the morning. I also solve a lot of problems in my dreams so you can imagine how helpful this technique is for me.

I woke up this morning with an idea for a presentation I will be doing at the end of September. I am developing content to not only inspire a few hundred women but

(continued on back page)

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.

WHAT DO YOU DO WHEN A COMPANY COMPROMISES YOUR DATA?

With the rise in cyber-attacks worldwide, you've likely received more than one notification from a company you work with informing you that your data has been compromised in a breach. While there are steps we can take as consumers to protect ourselves, sometimes we can't control when a company that promised to protect our personal data gets hacked.

In 2023, Statista reported that 52% of all global organization breaches involved customers' personal identifiable information (PII), making your personal data – addresses, numbers, names, birth dates, SSNs, etc. – the most commonly breached type of data. A recent example is ChangeHealthcare, breached in February of this year. Due to the breach, it's estimated that one-third of Americans – possibly including you – had sensitive information leaked onto the dark web.

So now what? What do you do when you receive a letter in the mail from your health care provider or favorite retail store admitting, "Whoops, we got breached." It's more than upsetting to think that your data is now in the hands of criminals. When sensitive information leaks, you'll have to do some recon to protect your

continued on page 2...

...continued from cover

accounts from suspicious activity. Follow these seven steps to stop the bleeding after a company fails to protect your data from being compromised.

What To Do After Your Data's Been Leaked

1. First, make sure the breach is legit.

One ploy that hackers use to get our data is to impersonate popular companies and send out fake e-mails or letters about an alleged breach. Whenever you get a notification like this, go to the company's website or call the company directly. Do NOT use information in the letter or e-mail because it could be fake. Verify that the company was hacked and which of your data may have been compromised. Try to get as much information as possible from the company about the breach. When did it happen? Was your data actually impacted? What support is the company offering its customers to mitigate the breach? For example, some companies offer yearlong free credit monitoring or identity fraud prevention.

2. Figure out what data was stolen.

After speaking directly with the company, determine what data was stolen. Credit cards can be easily replaced; Social Security numbers, not so much. You'll want to know what was compromised so you can take the necessary steps to monitor or update that information.

3. Change passwords and turn on MFA.

After a breach, you'll want to quickly update to a new, strong password for the breached account and any account with the same login credentials. Additionally, if you see an option to log out all devices currently logged in to your account, do that.

While you're doing that, make sure you have multifactor authentication turned on in your account or privacy settings so that even if a hacker has your login, they can't access your account without your biometric data or a separate code.

4. Monitor your accounts.

Even after changing your passwords, you should keep a close eye on any accounts linked to the breach. Watch out for any account updates or password changes you didn't authorize. They may be a sign of identity theft. If your credit card number was stolen, pay attention to your bank and financial accounts and look for unusual activity, such as unexpected purchases.

5. Report it.

If you're not sure a company knows it's been breached or you've experienced fraud due to a breach, report it to relevant authorities like local law enforcement or the Federal Trade Commission. They can provide guidance and next steps on how to protect your identity.

6. Be aware of phishing attempts.

Often, after data leaks, hackers use the information about you they stole to send you phishing e-mails or calls to trick you into giving away even more sensitive information. Be very wary of any e-mails you weren't expecting, especially those that request personal or financial information, and avoid clicking on any links or attachments.

7. Consider identity theft and data breach protection.

Consider identity theft protection after a breach, especially when highly sensitive data is stolen, like your SSN. It's a time-consuming process to replace a Social Security card. In the meantime, criminals could be using it to impersonate you. Identity theft and data breach protection help monitor your credit or other accounts, protect your identity and notify you when your data appears on the dark web.

While companies are responsible for protecting customer information, breaches can and will still occur. By following the steps above, you can minimize a breach's impact on your life. Ultimately, we must all contribute to protecting our information in an increasingly risky digital world.

UPCOMING FREE WEBINAR

Protect Your Business: Must-Know Cyber Liability Insurance Tips for Small Business and Local Government

Wednesday, August 14, 2024 at 9:00 am

Do you have cyber liability insurance? How do you know if what you have, will cover your needs?

In this webinar you will learn:

- Changes in cyber security requirements
- What you need to do to protect your company
- Understanding risk and regulations
- The importance of cyber liability questionnaire's

For complete information and registration, visit us online at:
www.cstsupport.com/webinar

CARTOON OF THE MONTH

(continued from front cover)

also weave in technology and the importance of deciding risk.

What I realized is that I am a risk taker….but only after I have evaluated ALL of the potential outcomes. I ask myself if I am willing to accept ALL outcomes no matter what. Now, I am always hoping for the best outcome but, if it doesn't go as planned, am I okay with the worst outcome?

So, let's say you take your car to the mechanic for a tire rotation. She (yes, my mechanic is female) tells you your brakes are in need of replacing. You decide, for a multitude of reasons, you are not going to replace them. You have chosen to accept this risk the potential problem could cause. The next day, you are driving your family to baseball practice, your brakes fail, and you cause an accident (you decide the severity of that accident), now how do you feel about the decision you made. You had the information, made a choice and accepted the risk.

Here's the thing, many of you are taking the risk of not implementing cyber security protocols. Some of you have no idea what they are and choose to put your head in the sand. Some of you have regulatory compliance mandates and are not meeting those requirements, but choose to accept the risk of non-compliance fines or worse, in my opinion, a breach where your data is compromised. In doing so, you are accepting the possible worse case scenarios. Are you okay with that?

Look, most of you have built a business, poured your heart and soul into it and make 33,000+ decisions a day. I get it, the cost of hiring an IT expert is more than you want to spend, but what is your business worth?

I recently produced and starred in a documentary called *Cybercrime: Fallout*. It will be released on Amazon in a few months, and it explains the fallout of cybercrime and the risks of doing nothing. I am joined by 9 other cyber security experts around the country, so you get amazing information from more than just me. I encourage everyone to watch it.

In the meantime, CST will be hosting a few Cybercrime: Fallout movie premier's locally and I would love to see you attend one of those events. This is my personal invite to each of you. They will be red-carpet events so come dressed up (or not) and ready to be inspired. More details on these events as we solidify the details.

As you navigate your daily decisions, I encourage you to consider the worst-case scenarios, assess the associated risk, and ensure you're prepared to accept the consequences should they arise.

As Always,

"passionate NOT pushy"

Lisa

DON'T MAKE THIS MISTAKE WITH YOUR HOME'S SMART TECH

Smart devices are so pervasive throughout our homes that it's hard to imagine what life was like before them. From door cams that show us when our kids get home to AI-powered devices that keep track of grocery lists and play our favorite music while we cook, we truly live in "smart" homes.

But unlike devices of the past, you can't "set and forget" smart devices. These tools are connected to the Internet, where hackers keep a close eye out for unprotected devices. When they find a device with a weak password, they can access it and carry out terrifying crimes like watching your family through a home camera. Before you plug in your smart device, follow these simple steps to make sure it's not an open door for peering eyes.

Pros And Cons Of Smart Devices

When hackers find an unprotected device – like an indoor cam that you never bothered to change the default password to – they can access sensitive information on your account, including your address, birth date, e-mail address and phone number. Criminals use this information to create a profile about you and carry out targeted attacks. A family in Mississippi even had a hacker taunt their young daughter through their Ring camera.

Thankfully, you can take a few simple security steps to avoid becoming a victim of your smart device.

Steps To Keep Your Smart Home Safe

1. Change the default login information immediately. Default passwords are low-hanging fruit for hackers, so be sure to change this to a new, stronger password right away.

2. Make sure your WiFi is secure. If your WiFi password is a few years old or you use the same password on other accounts, change it to a stronger password.

3. Enable multifactor authentication (MFA) in security settings. This way, users can only log in with a security code or authenticator app, making it nearly impossible for hackers to get in.

4. Regularly update the device. Updates fix issues or add new features that may improve your security. Don't skip these updates. If your smart device doesn't update automatically, set a reminder in your phone to check for updates periodically.

5. Consider separate networks. Many WiFi providers offer guest networks. Consider connecting smart devices to a home guest network separate from the one that your phones or laptops are on. This way, if a smart device is hacked, it's not a straight shot to devices holding more valuable information.

The biggest mistake smart-device users make is thinking they can plug in their devices and walk away. These tips go a long way toward ensuring that your device isn't an open door to creepy criminals.

ARE YOU USING THIS HELPFUL GOOGLE CALENDAR HACK?

It's a bit embarrassing when you log in to your computer at 9:00 a.m. only to realize you missed the all-team Zoom meeting at 8:30 a.m. Thankfully, Google Calendar offers a helpful hack: daily agendas. With this feature, you can send yourself a daily agenda first thing in the morning so you know everything planned for the day. To set it up, log into your Google account and go to Settings. Find "Settings for my calendars" > "Other notifications" > "Daily agenda." The default is set to "None," so click on it and change it to "Email." Now you have a daily agenda automatically sent to your inbox before you even get out of bed!

MICHAEL MICHALOWICZ

EXPLAINS HOW TO BUILD A TEAM THAT CARES ABOUT YOUR COMPANY'S SUCCESS AS MUCH AS YOU DO

Early in his career, Mike Michalowicz was eager to announce to his team a new corporate vision for the year: a $10 million revenue goal. However, what he imagined would be one of his greatest visionary moments as a leader was one of his biggest mistakes.

After revealing the vision to his team, "it was total silence," Michalowicz explained to a room of business leaders at a recent industry conference. "A colleague came over to me and said, 'Mike, if we achieve $10 million in revenue, you get the bigger house. You get the new car. That's your vision. What about our vision?'" This was a transformative learning moment for Michalowicz, who committed himself to learning what it takes to be a GREAT leader.

Today, Michalowicz is the author of several books, including *Profit First, Get Different, The Pumpkin Plan* and other small business must-reads. He's an entrepreneur and speaker teaching other leaders how to build and retain unstoppable teams who care about the company's success as much as you do, so you'll be happier, grow faster and create an environment where everyone flourishes.

How To Build An Unstoppable Team

1. Most leaders tell their team what to do. Great leaders ask their team what they could do. One of the Baltimore Museum of Art's most successful exhibits was curated by 17 museum guards. The idea came from a conversation between a curator and a guard around what the guard did day-to-day. He revealed how much he learned about the art from patrons and what interested them. Museum leaders quickly learned this wasn't unique to the one guard, and a group was assembled to create "Guarding the Art." Michalowicz explains that great leaders encourage ownership by asking, "What could we do?" rather than always telling their employees what to do.

2. Great leadership assembles and unifies. The movie *The Boys in the Boat* recounts how an inexperienced US rowing team won gold in the 1936 Olympics. The leader helped the team connect, communicate and work together to win against all odds. He fostered deep trust within the team, which Michalowicz says distinguishes great leadership in any circumstance.

3. Great leaders follow a FASO model. Michalowicz's research and experience in leadership culminate in a four-part model he calls "FASO." Leaders who want to be great can use FASO to assemble an unstoppable team.

- **F – "Fit."** When hiring a new team member, they must be an ideal fit for the organization, and the organization must be an ideal fit for them.
- **A – "Ability."** Great leaders look for people's raw potential. Do they have curiosity, desire and a thirst for the role? That's what great leaders hire and recruit for, not simply experience and innate ability.
- **S – "Safety."** Great leaders account for their team's physical, relational and financial safety. They ensure that people feel safe in how they are treated and where they work, they have a transparent financial culture and they educate their team on personal finances.
- **O – "Ownership."** "When we're forced to comply, we'll seek to defy," Michalowicz says. Great leaders encourage their team to personalize, gain intimate knowledge of and control aspects of their work.

Above all, Michalowicz says, "No one cares how you care; they care THAT you care." Show your team you care by working to incorporate these great leadership approaches in your organization.

SHINY NEW GADGET OF THE MONTH

Targus Coastline EcoSmart Backpack

With its thoughtfully engineered and comfortable design, the Targus Coastline EcoSmart Backpack is an excellent choice for professionals on the move. Its standout feature is the SafePort® Sling Protection System, which ensures that laptops up to 16" are securely cradled against the bumps and knocks of a daily commute.

Additional padded straps, front pockets and a 22L capacity leave plenty of room for everything you need on a long commute or a day away from the office. Equally impressive is the backpack's commitment to environmental responsibility. Made from 69% certified Ocean-Bound Plastic, the backpack is durable and resistant to wear and tear but also contributes to reducing plastic waste in our oceans and empowering coastal communities.

Business After Hours Event:

CST Group Inc.
and
Malone Ford
invite you to
Malone Chamber of Commerce
Business After Hours

August 15, 2024
5:30pm @ Malone Ford
3350 State Route 11, Malone, NY

Join us for an evening of food, drinks and networking. Bring your friends! Free admission.

CST Group Inc.

MALONE Ford

SUMMER HEAT

Is it just me or does this summer feel extra hot?

Summer is in full swing and the heat is coming in hot....pun intended.

August always seems to be the start of getting organized for the next few months. We have school starting back up and all the holidays are approaching. In Northern NY, we try to enjoy the warm weather while we have it, but then August hits and we suddenly remember all the projects we wanted to get done before the cold comes. Time to make that to-do list because time is running out for outside tasks!

There is still plenty of time, however, for some summer fun.

=Jessica=

Important Dates in August

8th- International Cat Day

14th - Webinar with Lisa

15th- Business After Hours with Malone Ford

Tech Humor...

QUESTION:

What is a computers favorite snack?

Q & A with Carrie

your friendly Account Manager

Dear Carrie,

My computer and printer are wireless but the connection is not great. Why am I having internet issues when my router is in the same room? How can I fix this?

Sincerely,
Poor Connection

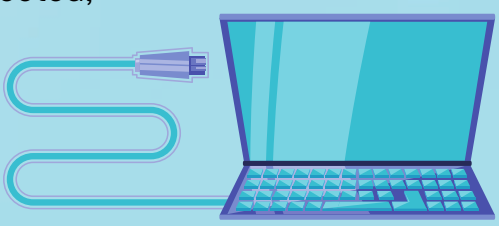
Dear Poor Connection,

A Wi-Fi connected device relies on obtaining an IP address from your router. Because the IP address can change, it will disconnect your equipment resulting in inconsistent connections. The distance of the router isn't necessarily relevant.

We always suggest the best way to ensure you are getting the best connection possible is to connect your equipment directly to the router or computer. This will ensure your connection is stable at all times.

Still having issues? Give us a call and we will work through your specific issue.

Always Connected,
Carrie



ANSWER: Microchips!

WE ARE AIMING HIGH AND NEED YOUR HELP

CST has launched a customer satisfaction rating platform where, YOU, our customers can rate our service levels.

At the bottom of our email, you will see this "How am I doing?" image, simply click the rating and fill it out.

WANT TO SEE HOW WE ARE DOING?

VISIT: HTTPS://WWW.CSTSUPPORT.COM/OUR-CLIENTS/

LIGHTS, CAMERA, CYBERSECURITY!

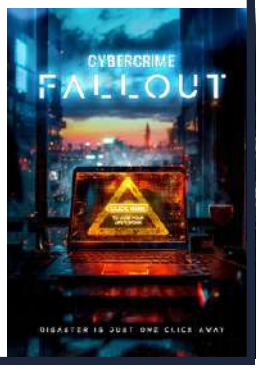
FREE MOVIE PREMIER OF

Cybercrime: FallOut

As cyber threats evolve, this movie showcases the expertise and strategies of leading cybersecurity professionals, highlighting their relentless fight against digital crime.

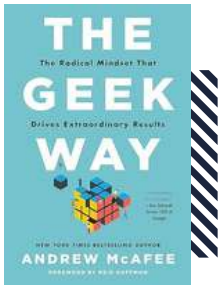
LISA CO-PRODUCED AND CO-STARS IN THIS MOVIE DESIGNED FOR SMALL BUSINESS! BEFORE IT IS RELEASED ON AMAZON, WE WILL BE HOSTING SEVERAL MOVIE PREMIERE'S.

BE WATCHING FOR UPDATED INFORMATION!



THE GEEK WAY:
The Radical Mindset That Drives Extraordinary Results

By Andrew McAfee



When we have a big problem, we like to go to experts who don't just like what they do but are downright geeky about it. Geeks are known for being intelligent and efficient problem-solvers, but what if we could all benefit from a geeky mindset to perform better in our work and lives?

In *The Geek Way: The Radical Mindset That Drives Extraordinary Results*, Andrew McAfee explores four "norms" – science, ownership, speed and openness – that define geek culture. He explains that when these norms are aligned, it taps into our human superpowers: our ability to cooperate intensely and learn quickly. This book blends science, history and real-world examples to provide insights into harnessing geek culture for innovation. The Geek Way is a compelling read for anyone interested in channeling their inner geek to improve their ideas, business or community.

Tyler's TECH TIPS

"Don't forget on Wednesdays to leave your unit on and connected to the internet. This way all neccessary updates can be installed"