CST Tech News

What's New

It's hard to believe October is upon us already. We have officially stepped in to fourth quarter so we need to prepare for end of year projects, last minute purchases (if we can get equipment) and positioning ourselves for a successful end of 2021. If you have not had a QBR (Quarterly Business Review) with me, please reach out so we can finalize end of year activities. There is certainly enough happening in our world for us to worry about so having the end of year checklist off our plate would be awesome.

As promised, I'd like to talk about password management as a segue from last month's article on email. On average, business employees must keep track of 191 passwords (LastPass, 2017). As a business owner, do you know what these are? Now multiply that by the number of employees you have. For some of you that number is staggering. What if this employee left or worse, got fired? What then?

This is exactly what happened to two of our clients in the last sixty days. One employee left on good terms, but the employer never considered asking for their credentials to all the accounts they had access to, including bank login credentials, security questions and vendor login information. Luckily, when we discovered it, the employee was more than willing to share that information with us. Whew, crisis averted. But the next scenario is not nearly as neat or tidy. An employee was fired. It was ugly and unfortunate. Once again, this employee had access to confidential company data including customer

October 2021

This monthly publication provided courtesy of Shawn & Lisa Brown, Owners

CST Group Inc.

Our Mission:

To provide outstanding technology services to our customers allowing them to focus on their business.

Want To Make Sure Your Business Is Protected From A Data Disaster?

Did you know that 93% of all businesses – that don't have a disaster recovery plan in place when they experience a data disaster – go out of business within a year of that disaster? And yet, 68% of businesses don't have a disaster recovery plan in place.

Losing access to your business's data in this day and age could very well mean losing everything. That means that as data becomes an increasingly important commodity to businesses of all types and sizes, so does having a plan for if or when your business experiences a data disaster.

The thought of protecting your business against a data disaster might be daunting, but don't worry. By following the steps listed below in this article, you can make sure that your business is ready to take on the challenge.

However, before we actually get into those steps, there is one distinction you should understand: the difference between a business continuity plan and a disaster recovery plan. A business continuity plan is primarily proactive, in that it is a strategy by which a business can continue to operate no matter what kind of disaster or setback befalls it. A disaster recovery plan is primarily reactive and has to do with how a business acts immediately following a disaster of some sort – in this case, a data disaster.

So, now that we're clear on what a disaster recovery plan is, here are the steps your business can take to create one that works for you and your employees.

Step 1: Rally The Troops And Assess Your Equipment
In the fight against data disasters,

Continued on pg.2

Continued from pg.1

everyone has to be on board. Otherwise, there will always be holes in your defense plan. That's why executive buy-in – getting everyone in the company, from the CEO to the entry-level employees – is crucial. You need everyone to collaborate cross-functionally in order to fully protect your business.

From there, you need to thoroughly analyze each of your business's systems, applications and data sets, as well as how they're physically accessed, in order to suss out any potential vulnerabilities. Then you should determine which systems are absolutely critical to the operation of your business and for getting products and services to your customers. These are the functions that will need to stay up and running, even after a data disaster.

Step 2: Create Your Disaster Recovery Strategy
Once you have everyone on board and an understanding of your equipment and assets (as well as their vulnerabilities), it's time to actually formulate your disaster recovery plan. To do this, you should take a look at your budget, resources, tools and partners in this endeavor. When you understand how long it takes your business to get back online and the cost for doing so, you'll have a good idea of how to move forward.

> **"68% of businesses don't have a disaster recovery plan in place."**

Step 3: Test Your Strategy
No great plan is complete without first testing it to see if it will work. Put your disaster recovery plan through a trial run to see how quickly your team responds to solve the problem and see if there are any improvements that need to be made to the process. Then, by the time an actual data disaster occurs, your business will know how to shut it down and keep running with no problem at all.

While the steps themselves aren't difficult to understand, preparing your business to combat data disasters takes a lot of work. In the end, though, the work is worth it if it means protecting your data. As a recap, here are the four main action steps that you need to take in formulating a disaster recovery plan:

1. Get executive buy-in for creating a disaster recovery plan.
2. Analyze and evaluate your business's systems, applications and data to understand how they could be impacted.
3. Find out which systems you need to keep running and prioritize them during the fallout of the data disaster.
4. Test your plan before you actually need to put it in action.

Follow these steps, and your business's data will be safe from any threat that comes your way. If you need guidance, please reach out and we would be happy to help.

"I DIDN'T KNOW"

Unfortunately, That Excuse Doesn't Replenish Your Bank Account, Resolve A Data Breach Or Erase Any Fines And Lawsuits.

It's coming ...

- That day a hacker steals critical data, rendering your office useless ...
- That day when your bank account or credit card is compromised …
- Or that day when your customers' private lives are uprooted …

Cybercriminals and hackers are constantly inventing NEW ways to infiltrate your company, steal your assets and disrupt your life. The ONLY way to STOP THEM is by CONSTANTLY EDUCATING yourself on how to PROTECT what's yours!

We have the perfect way to help reduce your risk and keep you safe! Simply sign up to receive our FREE "Cyber Security Tip of the Week." We'll send these byte-sized quick-read tips to your e-mail in-box. Every tip is packed with a unique and up-to-date real-world solution that keeps you one step ahead of the bad guys. And because so few people know about these security secrets, you will learn something new every week! Visit www.cstsupport.com/about-us/newsletter-techtips-signup/ to receive our FREE "Cyber Security Tip of the Week"

lists, financials and refused to give up any information on login, passwords, security questions, and the list goes on. Now what? When CST was contacted to disable this user's email, we quickly discovered no other data was obtained prior to this person leaving. They even changed their computer login password preventing the employer from gaining access. Luckily, we had an admin user on this computer, and we were able to get in, change the employees' password and gain access to what they had. Guess what we found? A document with all account and password information. Although this is not recommended, we were grateful to have found it. The employer was then able to see what they had access to and quickly contact banks and vendors to prevent access. For both clients, the result was not nearly as bad as it could have been.

My point is, I encourage all of you to be pro-active with employee credentials. CST is currently working with a password management company to establish an enterprise business account that will allow us to help you, the steward of your company, gain some control of every user and password account you have across your entire organization. We have already deployed it and are learning everything we can on its admin features, so we look forward to some discussion about getting you access to this. Look for it in upcoming discussions.

Let's be honest, we all hate passwords especially for those that force us to change them every 30/60/90 days. We all know the importance of not using the same password for everything, making them more difficult to guess and adding special characters and numbers to make it more complicated. However, knowing those rules does not make us want to implement them considering 53% of us haven't changed our passwords in over 12 months. So along with your concern as an employer, you also have the concern of the employee who gets anxiety just thinking about it. This is exactly what opens us up to risk of cyber-attack.

As you wait for information on deploying an admin account for password management, here are some things you can do to encourage healthy password management.

5 tips for improving your password security

1. **Don't reuse passwords**.
2. **Update your passwords**.
3. **Use strong passwords**.
4. **Take advantage of MFA and biometrics**.
5. **Monitor your data**.

I will have much more on password management in the coming months so be watching for that. Have a beautiful October and Happy Halloween.

Don't Give Up On You No Matter What Anyone Says

At the office, in our shipping area for our books, there's a little shelf on the wall, displaying a copy of each of the six books I've written. However, technically, there is one book missing from the display: my book *Profit First*.

Now, there is a copy of *Profit First* on the shelf. However, it's not the first copy that I published – it's self-published, actually. *Profit First* was the third book that I wrote, the first two being *The Toilet Paper Entrepreneur* and *The Pumpkin Plan*, both through Penguin Random House Publishing. When I pitched *Profit First* to them, however, their exact words to me were as follows: "No one needs another accounting book."

And they declined to publish it – at least at first. Not too long after facing that rejection, I spoke with someone who was mentoring me at the time about my frustrations at not getting *Profit First* into the hands of business owners everywhere just because my publisher didn't have faith in it. After I finished explaining all of that, my mentor left me with the words that I would actually follow: "Make them regret it."

I had to make them see that in refusing to publish *Profit First*, they were making a huge mistake. I had faith in my book. I knew it could help so many business owners out there. All I had to do was prove it.

So, that's why I initially had to self-publish *Profit First*. And guess what? It sold so many copies that Penguin Random House eventually came back to me and said that they wanted to buy the book and republish it in a revised and expanded edition. *Profit Firs*t is by far my most popular book, and it's helped more than 600,000 business owners apply the profit first method and mentality to their business.

It's my hope that sharing this story leads to a wake-up call for you. Don't let the few naysayers who are scrunching their noses at your big ideas dictate the direction you take in your business and in your life. If they don't share your vision (at least at first), that doesn't mean you have the wrong vision – it just means you have to double down and press forward. You have to believe in your idea even more than you already did.

If I hadn't stuck to my guns and published *Profit First*, regardless of what my publisher said, there would be thousands of business owners out there who would not be nearly as successful as they are now. They've grown, curated their clients and automated their business in ways that wouldn't have been possible otherwise.

What's your next big idea? Does the thought of how it could help people fire you up? Are there people in your life, even people who care about you, who tell you that your idea won't work? Don't give in. Don't give up on your dreams. Keep pushing forward, and I promise you that eventually, you'll see the success that you already know is possible.

Mike Michalowicz is a very successful author, entrepreneur and lecturer. He has written several successful books, including his latest, Get Different. *He is currently the host of the* Business Rescue *segment on MSNBC's* Your Business, *and he previously worked as a small-business columnist for* The Wall Street Journal.

WE ARE MOVING!

CST is excited to announce we are moving our NY headquarters! We have outgrown our building and need more office space for our incredible staff.

Our new physical address affective November 1, 2021 will be

14923 State Route 30
Malone, NY 12953

Our mailing address as always will remain

PO Box 848
Malone, NY 12953

Be sure to change the address in your accounting system. To keep updates on our move, check out our social media accounts. @CSTGroupInc #CSTisMovinOnUp

A Massive Threat To Windows 10 Users?

Security researchers discovered a vulnerability in Windows Hello's facial recognition programming that could potentially impact Windows 10 users, but does it warrant much fear? Experts say no – at least, not to the average user.

The vulnerability has to do with Windows Hello's camera system. It uses a camera with an infrared sensor and an RGB sensor. However, only the infrared image is processed during facial recognition. This theoretically means that if someone were to get a hold of an infrared image of your face, they could use it to access your computer – and that's where the threat starts to fall apart. Whenever a hacker needs physical access to the computer and the computer's user, they won't waste their time unless you're hiding some pretty juicy data. So, don't worry, Windows 10 users – you can sleep easy knowing that no one is trying to steal your face.

CALLING ALL CREEPS

SOME PEOPLE LOVE SUMMERS WARM WEATHER, BEACHES, AND LAZY DAYS. BUT EVERY YEAR AT THIS TIME, THE NORTH COUNTRY IS INCREASINGLY POPULATED WITH A DIFFERENT TYPE OF PERSON. THE ONE WHO CAN'T WAIT FOR PUMPKIN SPICE TO BE BACK AT THE COFFEE SHOPS, THEY DEFIANTLY PULL OUT THEIR SWEATSHIRTS WHEN TEMPS ARE STILL TOO HIGH AND START THE COUNTDOWN TO HALLOWEEN.

HALLOWEEN IS THE MOST EXCITING AND FREAKIEST OF ALL HOLIDAYS OUT THERE, AM I RIGHT?

HALLOWEEN CELEBRATORS AMP UP THE HOLIDAY SPIRIT BY PUTTING UP DECORATIONS WITH PUMPKINS, SPOOKY ELEMENTS AND LET'S NOT FORGET THE COSTUMES.

WE ARE WEEKS AWAY FROM HALLOWEEN AND BETWEEN THE DECORATING HERE AT THE OFFICE AND OUR LOVEABLE FRED GOING ONSITE, WE HAVE BEEN BUSY. DO YOU DECORATE THE OFFICE? DO YOU GO FOR SCARY DECORATIONS, OR DO YOU OPT FOR A FUN THEME?

WE WOULD LOVE TO SEE WHAT YOU HAVE GOING ON SO TAG US IN ALL YOUR HALLOWEEN FUN. DO NOT FORGET TO CHECK OUR FACEBOOK, AS ALWAYS, FOR ALL OUR OFFICE SHENANIGANS.

AND AS ALWAYS
#STAYCYBERSAFE
JESSICA