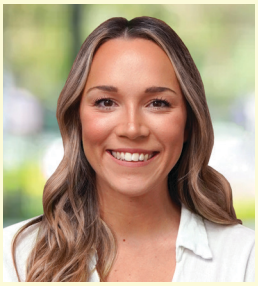
Central Texas Technology Solutions
Your Business Partner

Technology Monthly Newsletter
November 2020

Welcome Madison!



We are excited to announce we have a new Team member, Madison Melser!

As our Inside Sales Account Executive, Madison will help CTTS maintain our excellent customer service by making sure our Clients are always taken care of and that they have all the IT products and services needed to successfully and efficiently run their business.

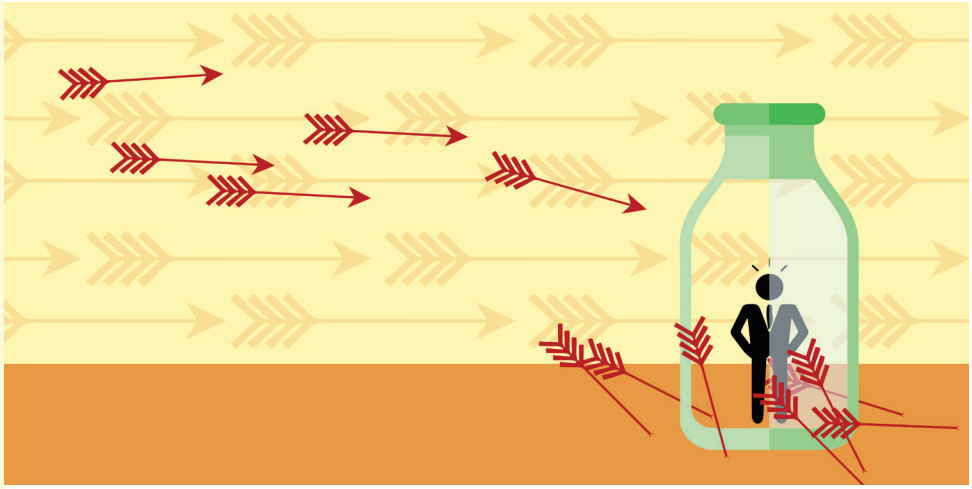
Madison studied at Texas State University and Champions School of Real Estate where she obtained her Real Estate License.

Along with being a Real Estate Agent, she has also worked as a Sales Development Representative for a software company helping to drive sales and provide their software to those who needed it.

In her free time, Madison enjoys spending time with her fiancé and their fur baby Dixie, watching football on Sundays, and game nights with friends.

Madison looks forward to getting to know our Clients and their individual needs as we work together toward the growth and development of your business.

This monthly publication provided courtesy of CTTS, Inc.



4 Questions Your IT Services Company Should Say "Yes" To

Out with the old and in with the new! For far too long, small and midsized businesses have taken an old-school approach to IT services and security. In other words, they wait until something goes wrong before they call an IT services company and request help.

Back in the day (think 1990s and 2000s), this approach worked, more or less. External threats, such as hackers and viruses, were still few and far between. A data breach wasn't on anyone's mind. So, it made sense to wait until something went wrong before taking action.

In IT circles, this is known as the "break-fix" approach. Something breaks, so someone has to come in to fix it. And they charge for their services accordingly. If something small breaks and it takes a short time to fix, you could expect a smaller bill. If something big breaks, well, you can expect a pretty hefty bill.

The break-fix approach is 100% reactive. As many businesses have learned, especially in more recent years, as the number of threats have skyrocketed, it can get very expensive. IT specialists are an in-demand field. With just about every business relying on the Internet and Internet-connected devices in order to operate, there's a lot of opportunity for something to go wrong.

This is exactly why you can't rely on the reactive break-fix model anymore. If you do, you could be putting your business at serious risk. In some cases, the mounting costs and damages done could put you out of business.

If you're hit by a data breach or if a hacker infiltrates your network (which is a common occurrence), what's next? You call your IT services partner – if you have a partner – and tell them you need help. They might be able to restore lost or stolen data. That is, if you routinely backed up that data. You

don't want to find yourself in this position.

And you don't have to.

Instead, take a proactive approach to your IT support and security. This is the new way of doing things! It's also known as managed services – and it's a far cry from the break-fix approach.

If you work with an IT services company that only comes out when something breaks, it's time to get them on the phone to ask them these four big questions.

1. Can you monitor our network and devices for threats 24/7?
2. Can you access my network remotely to provide on-the-spot IT support to my team?
3. Can you make sure all our data is backed up AND secure?
4. Can you keep our network protected with up-to-date malware solutions, firewalls and web filtering?

If your IT services partner says "no" to any or all of these questions, it might be time to look for a new IT services partner.

> **"When things go wrong, and these days, things will go wrong, you'll be left with the bill – and wishing you had been more proactive!"**

If they say "yes" (or, even better, give you an emphatic "yes"), it's time to reevaluate your relationship with this company. You want to tell them you're ready to take a proactive approach to your IT support and you'll be happy to have them onboard.

Far too many small businesses don't bother with proactive support because they don't like the ongoing cost (think of it as a subscription for ongoing support and security). They would rather pay for things as they break, but these break-fix services are more expensive than ever before. When things go wrong, and these days, things will go wrong, you'll be left with the bill – and wishing you had been more proactive!

Don't be that person. Make the call and tell your IT services provider you want proactive protection for your business. Ask them how they can help and how you can work together to avoid disaster!

Or give CTTS a call at (512) 388-5559 and we'll give your business a free IT Assessment to see where technology is getting in the way of your daily operations and how we can alleviate those computer headaches.

Honoring All Who Served

Liberty comes at a price, and the men and women who serve our country are willing to pay that price for our freedom and for peace.

We thank you, we salute you, and we honor you, Veterans!

We would like to show our appreciation and gratitude to those who have served in the US military by offering all Veterans a FREE Computer Clean-up and Optimization (a $197 Value).

Simply call us today at (512) 388-5559
or e-mail Josh.Wilmoth@CTTSonline.com

12 Cyber Readiness Strategies To Move From Defense To Offense

"Everyone has a plan until they get punched in the mouth." – Mike Tyson

As business leaders, we've all been punched in the mouth recently. What's your new game plan? Since COVID-19, the annual or quarterly one you had is now likely irrelevant.

You have two options:

1. Sit and wait for the world to go back to the way it was...
2. Create and act upon a new game plan.

Option 2 is the correct answer! AND, you're in luck, because at CTTS, we are here to help you and your organization move from defense to offense. Get started today with our top **12 Cyber Readiness Strategies:**

1. **Have A Cyber Readiness Plan**
The success and survival of your business will be determined by your ability to overcome security threats or breaches. You need a cyber readiness plan that includes elements of prevention, continuity and recovery strategies.

2 Establish Strict Policies and Procedures
Policies and procedures regulate business operations and are essential for defining the standards and expectations of employee behavior and actions in the workplace. While establishing strict, security-focused protocols is essential, a system of validation and enforcement is equally important. After all, rules without consequences are merely suggestions.

3. Keep Updates -- Up to Date
While updates often introduce new or enhanced features into your apps, programs and systems, they also install security and performance fixes known as patches. Undiscovered defects or flaws can leave your systems exposed. Hackers will exploit any vulnerability or security gap they find. Keeping your systems updated is vital for keeping your business cyber ready.

4. Force Authentication
One-level security is no longer enough. Even the strongest passwords are vulnerable to theft or exposure. Requiring more than one method to authenticate user identity or access permissions can reduce or eliminate the risk of stolen or unauthorized credentials being utilized.

5. Back Up Everything!
Data is the lifeblood of every business. Unfortunately, the risks and threats to the protection, privacy and usability of that data are endless. Follow the 3-2-1 method for backups; a minimum of three unique copies of your data, two available locally and one off-site or in the cloud. Make sure to test your backups often for functionality and integrity.

6. Don't Neglect Compliance
Maintaining regulatory compliance is mandatory for many organizations. While navigating and satisfying the obligations can be complicated and stressful, achieving compliance is a critical component of having a cyber ready business. Security and privacy are integral elements of compliance.

7. Continuous Network Intelligence
A critical component of cyber readiness is having on-demand insight of anomalous activities, suspicious changes, potentially harmful misconfigurations or any other malicious activities occurring internally on your network. Promptly detect and remove threats before they cause damage.

8. Security Awareness Training
Users are the weakest link in security, given a lack of education and experience. Instituting a security awareness training program for every member of your staff will significantly reduce the probability of user-related errors and exposures.

9. Combat the Password Crisis
With over 80% of hacking-related breaches linked to weak, reused or stolen passwords, user credentials are emerging as the top vulnerability for businesses. Balance convenience and security by monitoring the dark web for exposed credentials, implementing multi-factor authentication, and streamlining control of password management.

10. Don't Skip the Insurance
Increasing risks and threats of data breaches and ransomware, regardless of size or industry, have prompted many businesses to adopt Cyber Risk Insurance to protect themselves from catastrophic loss. Investing in a cyber insurance policy could save your business should you be the next victim.

11. Reduce Supply Chain Vulnerabilities
Nearly two-thirds of firms (65%) have experienced cyber-related issues in their supply chain in the past year. Regularly evaluate and monitor the security of your supplier networks and third-party vendors.

12. Deploy a Multi-Layer Security Strategy
Protect your data and your business by deploying multiple security strategies together as one.

Ensure that your data is protected and secure from all cyber threats because the right safeguards act as the backbone of your company, giving you a foundation you can count on and grow from.

Is Working From An Office More Secure Than Working Remotely?

It may come as a surprise, but working remotely can be just as (or more) secure than working in the office, **if done right.**

Those are the three operating words: if done right. This takes effort on the part of both the business and the remote employee. Here are a few MUST-HAVES for a secure work-from-home experience:

1 **Secure networks.** This is nonnegotiable. Every remote employee should be connecting to a secure network (at home, it should be WPA2 encrypted), and they should be doing so with a VPN.

2 **Secure devices.** All devices used for work should be equipped with endpoint security – antivirus, anti-malware, anti-ransomware and firewall protection. Employees should also only use employee-provided or approved devices for work-related activity.

3 **Secure passwords.** If employees need to log into employer-issued programs, strong passwords that are routinely updated should be required. Of course, strong passwords should be the norm across the board.
Small Entrepreneur, June 17, 2020

Top Tips On How To Prevent Your Smart Cameras From Being Hacked

Smart cameras have been under attack from hackers for years. In fact, one popular smart camera system (the Amazon Ring) had a security flaw that allowed hackers to get into homeowners' networks. That issue has since been patched, but the risk of being hacked still exists. Here are three ways to keep your camera (and your network) safe from hackers:

1 **Regularly update your passwords.** Yes, passwords. This includes your smart camera password, your WiFi network password, your Amazon password – you name it. Changing your passwords every three months is an excellent way to stay secure. Every password should be long and complicated.

2 **Say no to sharing.** Never share your smart camera's login info with anybody. If you need to share access with someone (such as a family member or roommate), many smart camera systems let you add a "shared user." This will let them access the camera, without the ability to access the camera's configuration or network tools.

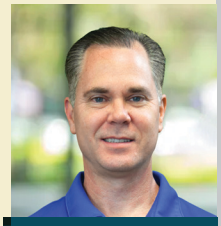
3 **Connect the camera to a SECURE network.** Your smart camera should only be connected to a secure WPA2 encrypted, firewalled WiFi network. The more protection you put between the camera and the rest of the digital world, the better. *Digital Trends, 2020*

Tech Tip of the Month:

Optimize Your Access Point

Is there anything more frustrating than a bad Internet connection? There are many factors that can influence the performance of your WiFi signal.

Here are 3 simple steps to improve your Wi-Fi coverage and your productivity.



Read it Here: http://bit.ly/Tech-Tip-195