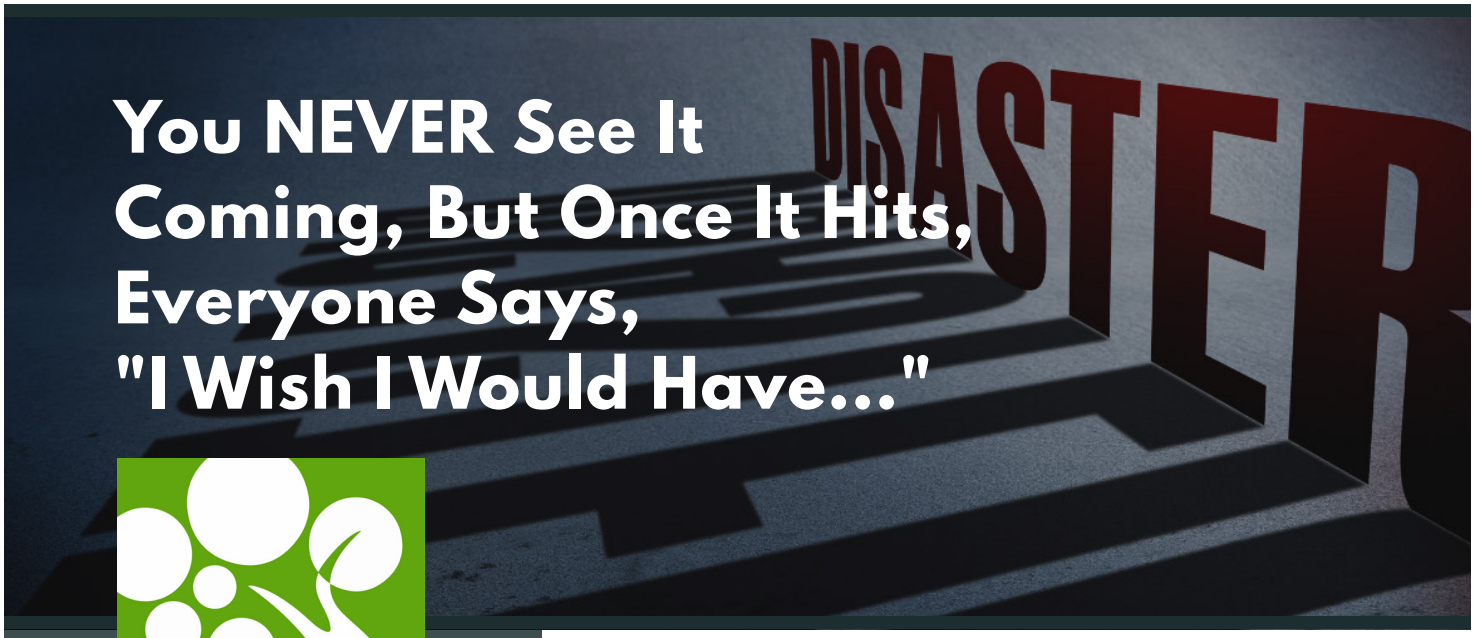
VOLUME 5, ISSUE 9 SEPTEMBER 2022

MTC TECH TALK

For Humans Not Geeks!

Your resource for the latest technology updates and opportunities for your success.



You NEVER See It Coming, But Once It Hits, Everyone Says, "I Wish I Would Have..."

What's In This Issue?

Meeting Tree Computer
☎ (845) 237-2117

Two years ago, no one could have predicted that countless businesses would shift to a remote work model. But, when the pandemic hit, small businesses had to think on their toes hard and fast. Many had only a few days or weeks to adapt. It was stressful and highly challenging.

Looking back on it, many people wish they'd had a plan in place. Unfortunately, not only were some of the changes incrementally more costly, but they also took a lot of impromptu coordination and on-the-fly planning. This meant that some things slipped through the cracks, including cyber security.

It is time to put that lesson into practice; you never know when disaster will strike, but you CAN prepare for it, whether that disaster is a pandemic, flood, fire, network failure, or cyber-attack.

Let's look at some steps you can implement today that will put you in a better place tomorrow. Here's how to get started.

Put Your Plan into Writing.
As they say, hindsight is 20/20. If you were just like a vast majority of SMBs, you might wish you had had a plan in place or had been given more time to close your buildings, but the reality is that, in early 2020, many SMBs didn't have a remote work plan, let alone a WFH security plan in place. So, they had to make one up as they went along.

A business continuity plan is a comprehensive strategy that, when enacted, will allow your business operations to continue in spite of some detrimental circumstances that would otherwise have derailed them. Without a business continuity plan in place, your business is vulnerable to chance --a risk that no business owner should take if they can help it.

The first step to preparing for the unexpected is to establish what that plan needs to address:

- Identify where your most significant losses would be if disaster struck your business.
- What would the costs be if you were to suddenly lose all or most business functions?

- How would the added expenses of a disaster affect your cash flow?
- How long would it take you to recover?

Once your plan is developed and documented, with responsibilities appropriately distributed, you need to train your staff and test the procedures that were laid out.

The plan should outline in as much detail as possible what needs to happen when disaster strikes. Pandemic? Here's how we operate. Fire? Here's what you need to know. Network failure? Call this number immediately. Ransomware attack? These are the steps to take to limit the damage.

The list goes on, and it can be extensive. Working with an MSP is incredibly valuable in any of these cases. They've already put together plans for other SMBs and know where to start when they help you customize a plan for your business.

Invest In Security, Backups, and VoIP Now
While every business should have network security already in place, the reality is that many organizations don't. There are many reasons why (cost concerns, lack of time, lack of resources, etc.), but those reasons aren't going to stop a cyber-attack. Hackers don't care that you didn't have time to put proper protection on your PCs; they just want money.

When you have IT security in place, including firewall protection, malware software, strong passwords, and company-wide IT security policies, you put your business in a much better place. All of this should be in place for both on-site employees and remote workers. With more people working from home, having reliable IT security, including proper onboarding and offboarding procedures, in place is more critical than ever. Taking care of this now will protect you from many (more) sleepless nights later.

In addition to having a flexible security strategy, you should be able to rely on secure backups. Investing in cloud storage is an excellent way to go. That way, if anything happens to your primary on-site data storage, you have backups elsewhere that will help you restore data quickly and limit downtime. Plus, implementing solid cloud options now will give your remote employees ready access to any data they might need while at home or on the go.

Something else to consider, if you haven't already, is investing in a VoIP phone system. Not only could it save you money, but your VoIP system will allow you to bring home your IP phone from your office and page co-workers, dial extensions, transfer and receive calls – all without ever missing a beat. So whatever the reason why you might be locked out of your offices, VoIP will allow you to simply pick up your work phone and plug it into any location with power and internet, giving you the opportunity to continue business as usual.

Where To Begin?
Some SMBs have the money and resources to invest in on-site IT personnel to help implement IT strategies and plan for the unexpected, but many don't. It is a significant investment. Your single best alternative is to research partnering with an experienced MSP so that next time you're not on your own when events happen that are beyond your control.

Pro-active IT support helps everyone in your organization, whether they work in the building or remote. A proper MSP is not just there to offer tech support but is a true partner in business: someone who helps you plan for growth and the good times and prepares for situations when damage control and immediate business continuity matter most.

No company is immune, so don't wish upon the stars that yours will survive; prepare now and ask for help if you need it. Contact us today if you want our help to start building your plan for the future.

Technology Update:

Home and small office routers are being targeted by cyber criminals in an attempt to steal sensitive data.

This is a smart move by the bad guys, as these routers exist outside of your business's usual security protection, and as they often have additional weaknesses to exploit; they are easy target.

What can you, as a business owner, do to protect your data when members of your staff are working from home?

If you have remote or hybrid workers, you need to make sure they have the right firewalls installed. Insist they use company devices for business work (or institute a BYOD policy as best practice) and give them encrypted connections to your office network.

Get in touch if you need help implementing any of these strategies.

Is Your Business Data Encrypted?

Encryption can be a confusing subject.

Is it a good thing, or a bad thing?

We understand the confusion. Thanks to the surge in ransomware, you could be forgiven for thinking that encrypting data is definitely a bad thing. After all, if it's encrypted, how on earth will it be usable?

However, when you're the one to encrypt your own data, you're adding a level of protection to it. It means that should it be stolen; it'll be unusable to anyone else.

Unfortunately, less than 50% of companies have standardized end-to-end encryption set up. While they have some level of encryption, they don't have a documented standard that covers every area of their business.

And it's not only hackers and other cyber criminals

that could benefit from a business' lack of data encryption. Lost or stolen devices are put that data at risk too.

When you consider that a laptop is stolen every 53 seconds, it's leaving businesses more vulnerable than they should be.

Microsoft 365 automatically encrypts business data by default. But if you have no other encryption set up across your applications and files, it's time to speak to your IT support partner.

If we can help you, please don't hesitate to get in touch.

Here's Why You Need To Automate More, Now

Most people love automation.

Because it's about creating a set of rules that software can follow

automatically, so humans don't need to do boring and repetitive tasks.

Who in your business would be against that?!

As well as saving you and your employees valuable time, automation has lots of other benefits for a business.

You should see a productivity boost as people can get more done in the same amount of time. It can also produce a leap in motivation and job satisfaction as people are spending more time enjoying the work they do.

They'll feel more listened to as you've made their jobs better and will reward that with increased loyalty. Recruitment might be easier as your reputation gets a boost.

Another benefit of automating tasks is for your customers. Perhaps they can get a response to a question a lot faster. Or maybe have a smoother experience when they deal directly with you.

Consider which tasks in your business could be automated. Even the simplest automations can have a really big impact on the way your business works.

Read more about what digital transformation could do for your business: https://meetingtreecomputer.com/files/2022/05/Digital-Transformation-Guide-Letter-Meeting-Tree-Computer.pdf

Who's To Blame For A Cyber Security Breach?

We all know what a huge danger a cyber security breach can be for a business and just how many businesses are being breached right now.

In truth, we hate having to write this. We don't want to feel like we're scaring you or being all doom and gloom! But it's really important that you're fully aware of the risk to your business.

Last year, the number of reported data breaches rose 68% compared to 2020.

And while it's a good idea to implement the right cyber security tools to help reduce the risk of a successful attack, it's practically impossible (or definitely unworkable) to give your business 100% protection, by just using software tools.

Why? Because, according to research, 85% of data breaches are caused by human error.

If that happens, who's to blame for your cyber security breach? Your employee? Or you, the business owner /manager?

It's a difficult question. Sure, your employee is likely the one to have clicked the link or downloaded a bad file that turned out to be malware. They may even have disabled security features to try to speed up their work.

However, as the business owner or manager, it should be your responsibility to reduce the risk of that happening in the first place.

A good security posture starts with training your people regularly to make sure they understand the risks and how to avoid them. But you should also have the right policies in place to remind your employees of best practices, and what happens if they fail to comply.

Employees are your first line of defence against security breaches. They can only ever be as good as your cyber security strategy though. Get that in place and everyone knows:

- What's expected of them
- How to avoid risk
- What to do if things go wrong.

We say, don't worry about who's to blame – just get your ducks in a row, starting with your cyber security strategy. If we can help, get in touch.

Free Email Comes at a Price

We've all been told that there is no such thing as a free lunch, yet it's hard to resist the siren's call of "FREE." It's one of the reasons why so many people have free e-mail accounts through Hotmail, MSN, Yahoo, and AOL.

The thing is that, while you might not be paying out of pocket for these services, there IS a cost. Here's the price you pay when you use a free e-mail account:

1. You will freely receive extra helpings of Spam (Yum! ..?)
2. Your emails aren't guaranteed delivery
3. Question or concerns? Customer Service is often non-existent
4. Moving, forwarding, or downloading messages can be difficult (if not downright impossible), and
5. In the mood to archive old messages for sentimental reasons? There is a cost for that...

To continue reading and to learn more: https://www.meetingtreecomputer.com/5-reasons-to-reconsider-your-free-email-accounts/

Q&A

I just closed an Office file without saving it. Please tell me I can get it back?

With a bit of luck you should be able to recover your file. If you saved the document once, autosave may have done its job. Otherwise, try using "AutoRecover" or check your temporary files.

I can't open an email attachment.

First, make sure this is a genuine file – call the sender to check. Then, it's possible you don't have the software that the file was created with. Right click the document and select 'Open With' to see if there's another option.

I've had an email telling me an account needs updating. Is it genuine?

Don't click any links in the email. If you're even slightly unsure, the safest thing is to visit the website by typing the URL (or copy /pasting it) into your web browser. Still unsure? Call your IT provider (us), they will know what to look for.

Submit Your Questions Here:
mduci@meetingtreecomputer.com

This is how you can get in touch with us:

call: 845-237-2117 | email: info@meetingtreecomputer.com
website: www.meetingtreecomputer.com

Follow Us