

MTC TECH TALK

*For Humans
Not Geeks!*

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




What's In This Issue?

Your Monthly
Technology Update

Does Your Business Have
a Guardian Angel?

Travel Smart – Security
for Travelers

Which Ransomware Payment
Option Is Best? (Hint: None)

Meeting Tree Computer
 (845) 237-2117

It shouldn't come as a big surprise when I say that cyberattacks on small and midsize organizations are getting worse. These attacks often result in significant financial losses caused by operational downtime, reduced revenues, costs resulting from investigations, remedies, and other fees or penalties.

As an MSP, we must shield our clients from cyber threats. Unfortunately, even the most robust security measures can't guarantee 100% protection. We wish it would. We'd be putting hackers out of a job forever. This is why it's crucial to have a solid incident response strategy in place: a plan that encompasses data backup, business continuity, AND cyber liability insurance. This policy is your safety net against the extreme costs of data loss, theft, network outages, and other cyber disruptions.

In today's volatile business landscape, cyber insurance isn't just a luxury—it's an absolute necessity. As cyberattacks surge and costs skyrocket, the need for comprehensive coverage is more urgent than ever. If your renewal is looming, brace yourself for a steep increase. And if you're new to the game, prepare for sticker shock when you receive your quote.

Yes, cyber insurance isn't cheap. However, it's a vital investment, especially considering your General Liability policy won't cover cyber-related claims. There are many horror stories of business owners who thought they were protected against cyber breaches under their GL coverage, but that is hardly ever the case. The scope of general liability coverage is often too narrow to cover the vast technicalities associated with cyber incidents.

Some examples of costs not covered under your General Liability insurance are:

- **Data recovery services:** If your network is attacked and data is lost or stolen, a data recovery service will try to salvage it from the damaged, corrupted, failed, or inaccessible storage media. This is a time-consuming and costly endeavour.
- **Legal expenses and fees:** Fines and lawsuits resulting from cyber incidents can escalate quickly.
- **Compliance/notification fees:** More and more states (NY state included) mandate that data breach notifications be sent to all entities affected by the incident. Not only is this time-consuming, but as these notifications must be sent out by direct mail and email and include messaging on websites and other publicly available platforms, they can also become costly.
- **Repairing IT assets:** Many cyberattacks result from damaged applications, computers, and other equipment. After an attack, you must repair these vulnerabilities to prevent a repeat incident. Replacing assets and paying an IT expert to fix what's broken can come at a significant expense.
- **Fraudulent wire transfers:** A simple phishing email can trick any employee into sending money to a fake recipient. Unfortunately, general liability insurance typically does not cover financial losses associated with such scams.

To cover the increasing number of claims and expenses insurance carriers are raising premiums and adding an increasing number of demands to protect themselves against high data breach payouts. The application questionnaire, which used to be a page or two of basic questions, now feels like a probing you weren't ready for. It may ask about your current security measures, past incidents, and future plans, among other things, to assess your risk and determine your premium.

Insurance carriers are tightening their grip, demanding stringent security measures like multi-factor authentication, endpoint detection and response tools, regular software updates, and more. The once-simple

application process now feels like an interrogation. Having an IT security partner in your corner with experience with these policies and applications greatly simplifies the maze of cyber insurance.

How we can help:

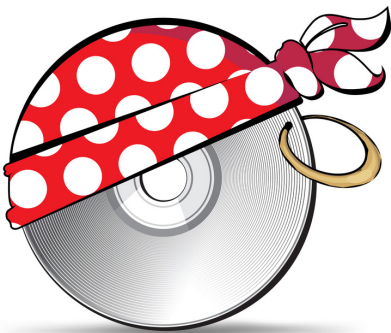
- By upgrading your cyber security protections, we can protect your business from the increasing number of nefarious actors. This includes implementing advanced threat detection systems, conducting regular security audits, and providing employee training. These measures not only significantly lower your risk but also lead to potential reductions in your cyber insurance premiums, offering a promising return on your investment.
- Although we cannot provide you with an insurance policy for your business, we can guide you through the application process. We have established relationships with reputable insurance providers who can suggest the most appropriate policy for your needs.

Knowing that your network is in expert hands lowers the risk of extensive damage in case of a data breach, protecting you from extended downtime and your insurance company from having to cover higher-than-necessary claims.

So, here's the deal: We're rewarding the first five proactive individuals who call and ask us to reevaluate their cyber posture. As a token of our appreciation, we're offering a \$50 gift card in return. This is your opportunity to fortify your defences, take control of your cyber risk, and potentially save on insurance costs. It's a gift that keeps on giving. Contact us at 845-237-2117 to secure your spot and claim your gift card.

Remember, cybersecurity is a team effort. Your active participation is crucial in protecting your business and your bottom line. Let's join forces to fortify your defences and mitigate cyber risk.

Technology Update



This Is Why You Should Never Use Cracked Software

Software can be expensive. It might be tempting to use 'cracked' or pirated versions to save a few pennies, but in reality, the cost to your business could be even higher.

That's because cyber criminals are using cracked software to install malware on devices and networks. Once installed, they have access to all your data, and even your finances.

Macs are particularly at risk right now, thanks to a campaign targeting macOS software. Be careful and always use legitimate software!

Does Your Business Have a Guardian Angel?

Let's talk about Alex, who owns a thriving business in a busy town. This business is filled with loyal customers, happy employees, and a treasure trove of valuable data.

Fortunately, Alex has a good tech team behind him, so he knows the importance of encryption – the process that turns your data into unintelligible streams of characters so it can't be understood by anyone that steals it.

But for a moment, let's imagine he didn't.

In this alternate reality, Alex's treasure trove was left wide open. And let me tell you, things quickly took a dark turn.

One sunny morning, a group of cyber criminals broke into Alex's systems. They easily infiltrated his digital vault, swiping customer data, financial records, and employee information. Alex had no idea his precious data was slipping through his fingers.

Soon, the chaos erupted. Alex's



customers started receiving strange emails, and his employees noticed fraudulent transactions in their bank accounts. The trust that had taken years to build crumbled in an instant. Alex was left with a tarnished reputation and a sinking feeling of despair.

Back to the real world where Alex has his guardian angel – encryption. It's like an invisible shield that wraps around his treasure trove of data.

Here's what would happen:

The cyber criminals still got into Alex's business and took data but couldn't make sense of what they'd stolen. It was random looking characters. Total nonsense to them.

Alex's data remained safe and sound, and so did his reputation. His customers continued to trust him, knowing that their information was secure. His employees went about their work without worry, knowing their personal details were in good hands.

The moral of the story is crystal clear. Encryption is the guardian angel your business needs. It shields your data from prying eyes, keeps your customers' trust intact, and saves you from a world of trouble.

If you want to be more like Alex, and let encryption be the hero in your business's tale, we can help. Get in touch.

Travel Smart – Security For Travelers

One of the worst things that can happen in the age of cell phone addiction that we live in is being out of town and losing your phone, iPad or laptop. If your luck is like most people's, it will probably happen about four hours before you are supposed to board the plane to come home.



Some common-sense security tips can reduce the sting when (usually not if) it happens to you:

1. Before you leave, make sure you back your phone up to iCloud, to your computer or whatever method your particular phone supports.
2. Everyone's phone typically has a passcode today – if yours doesn't, set one right away. You can usually change the options within your settings to allow a passcode that permits letters and numbers, which is even better.
3. If you travel with your laptop, it's a good idea to encrypt the hard drive. This is not a hard process with modern operating systems, and it's not invasive to you – typically, it just requires you to enter a password immediately when booting the computer.

An ounce of prevention and forethought will ease the pain (and problems!) if this ever happens to you. And if we can help, you know where to find us!

Which Ransomware Payment Option Is Best? (Hint: None)



Picture this: Your business gets hit by a ransomware attack, and your valuable data is locked away by cyber criminals demanding a huge ransom fee.

You can't afford to pay it. But there's a twist – just like those “buy now, pay later” schemes, some ransomware gangs are offering victims payment extension options.

Recent research reveals that ransomware groups are getting creative with their extortion strategies. One group is even offering victims various choices when it comes to their ransom demands.

These “choices” include: Paying to delay the publication of their stolen data, with a standard fee of \$10,000... or paying to have their stolen data deleted before it's made public.

The exact amounts charged are often negotiated with victims, adding a chilling dimension to the whole ordeal.

To increase the pressure on victims, these ransomware groups have added some terrifying features to their web sites. These include countdown timers displaying how much time businesses have before their data is released, view counters, and even tags revealing the victim's identity and description.

It's all designed to make victims feel cornered and more likely to give in to the demands.

You might be tempted to pay that ransom to protect your business data.

Not so fast.

Paying is always a bad idea and here's why:

- Paying doesn't guarantee that you'll get your data back or that the cyber criminals won't demand more money later.
- By paying, you're essentially funding criminal activities, encouraging them to continue their attacks on others.
- Paying a ransom might even get you into legal trouble, as some governments have made it illegal to pay cyber criminals.

So, what can you do to safeguard your business from falling victim to ransomware?

- Ensure you have regular, secure backups of your data. This way, you won't be at the mercy of cyber criminals.
- Educate your staff about the risks of ransomware and train them to recognize phishing emails and suspicious links.
- Invest in robust cyber security software and keep it up to date.
- Keep your systems and software updated with the latest security patches.
- Segment your network to limit the spread of ransomware if one device gets infected.
- Develop a clear incident response plan, so you know exactly what to do if you're ever hit by a ransomware attack.

Paying cyber criminals rarely makes things better, and we're seeing businesses that do pay become targets time and time again. Instead, invest in the proactive measures above to help you stay secure. And if we can help you with that, get in touch.



Is it ok to connect to Wi-Fi in a coffee shop?

It's a good idea to use a VPN (Virtual Private Network) when using any public Wi-Fi to make sure no one is snooping on what you're doing online.

Should we use VoIP phones or mobile phones in the office?

While it's tempting to switch to mobiles, VoIP phones have more features, are more scalable, and cost less than mobiles. Get in touch for more info.

Do I need to worry about staff stealing data?

Hopefully not, but don't take any chances. Make sure people can only access the files they need to do their job, and make sure you remove all access as soon as someone leaves the business.

Submit Your Questions Here:
info@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

