VOLUME 5, ISSUE 10 OCTOBER 2022

MTC TECH TALK

For Humans Not Geeks!

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

Did You Know Your MSP Can Help Lower Your Cyber Insurance Premiums?

What's In This Issue?

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, often resulting in significant financial losses caused by operational downtime, reduced revenues, costs resulting from investigations, remedies, and other fees or penalties.

As an MSP, it is our job to work with our clients to prevent attacks from happening, but, unfortunately, no security offers 100% protection, making incident response strategies ever more important.

A proper recovery strategy includes not only data back up and business continuity strategies, but cyber liability insurance should be of equal importance.

Cyber insurance helps recover the cost resulting from data loss, cyber theft, encryption, a network outage, or other IT interruptions caused by ransomware, malware, and other cyber variants targeting your business. And in today's business climate, it is an indispensable part of any risk management framework. Unfortunately, as cyber-attacks continue to increase, so have the payouts from insurance companies. They are not happy about barely breaking even and are passing on the high costs to their customers. If your policy is up for renewal this year, you are likely to see a steep increase in annual premium. And if you're new to the game: get ready to be unpleasantly surprised at the quote you'll receive.

These policies are not cheap. They are, however, increasingly necessary, and your General Liability policy will not cover potential 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 gets attacked and

data gets lost or stolen, a data recovery service will try to salvage it from the damaged, corrupted, failed, or inaccessible storage media when standard methods of accessing the data are not offering the necessary results.
- Legal expenses and fees: Fines and lawsuits resulting from cyber incidents can escalate quickly
- Compliance/notification fees: More and more states (NY state included) are mandating that data breach notifications are 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 scams like these.

In an attempt to protect themselves against high data breach payouts, insurance carriers are raising premiums and are adding new demands. The application questionnaire that used to be a page or two of basic questions will now feel like a probing you weren't ready for.

Some of the most common topics covered on the new applications include:
- Multi-Factor Authentication/2FA
- Endpoint detection and response tool (EDR)
- AV and malware detection
- Full data back-up
- Regular software updates and patching
- Encryption
- Security Awareness Training

This list is limited, and requirements tend to vary per insurance carrier. Most carrier applications are long and ask detailed and complicated questions. Questions that probably only your IT provider knows the answer to.

Having an IT security partner in your corner, who has experience with these policies and applications, will ensure that your network security is appropriate for your business and satisfies all policy requirements.

How can they help?
- A proper MSP can help simplify the research process. Although they cannot provide you with the right policy for your business, they often know people who can and can make suggestions regarding the most appropriate policy for your business. Not all insurance agents are equally well versed in cyber liability insurance. It is in your best interest to do your due diligence to find the right policy and agent; an experienced MSP can help.
- Ongoing IT security support lowers the cost of cyber insurance. Insurance providers understand that attacks occur at all hours of the day and night. 24/7/365 IT support service monitors and secures your infrastructure and can take immediate action should an attack be detected. 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 protecting your insurance company from having to cover higher than necessary claims.

Doing the research, going through the application process, and implementing the requirements might seem overwhelming, but with the right help, it is manageable. A well-versed MSP will implement cyber defenses appropriate for your business and bring them to a level acceptable to your insurance carrier. The annual premiums might still shock you, but they will be much more affordable. And you can rest assured that your risk management framework includes everything it needs to protect your business from unwanted downtime and expenses.

Cybersecurity is a team effort, always.
Let's talk: 845-237-2117

Technology Update:

Thanks to a new feature Microsoft has added to the platform making sure you're fully engaged with your MS Teams call just got a lot simpler.

If you use Microsoft Teams on desktop, you can now use a Bluetooth headset or speakerphone to answer or end a Microsoft Teams call, rather than fumbling about for the on-screen button.

An end to awkward pauses? Sign us up!

Would You Pay??

Ransomware is scary. If it happened to you, would you pay the fee?

Despite what the criminals promise, they don't always unlock data when the ransom fee is paid: at times they ask for a second fee, or they unlock it as promised, but then sell it on the dark web anyway.

Many large companies are now refusing to pay, finding other ways to get their data back. And ransomware groups are increasingly looking at small, financially stable businesses as their new targets.

This means you and your team need to be vigilant about cyber security. Continue to take the necessary precautions such as using a password manager, checking that emails are from who they say they're from, and making sure your network is being monitored and protected.

It's also vital that you have a working backup of all data. Check it regularly.

Even without paying the ransom demand, your business stands to lose a lot of money if hit by ransomware. Recovery can take long time and it can cost a ton to get back on your feet

If you want us to audit your business and check its ransomware resilience, get in touch.

Your Business Could Be More Productive with One Simple Change

Most businesses simply wouldn't survive without technology. That's a fact.

When you have the right tools, devices, and network in place, your work is made easier; your team is more productive; and that leads to a more profitable business.

And yet, many businesses are working with an IT infrastructure that simply doesn't meet their needs.

Sure, they have a network that they can access, and they're using tools that help get the job done. But when you look at their plans for the future, or you speak to their team, you'll realize they could be doing so much more.

Does this apply to your business to any degree?

Ask yourself: When did you last create a formal business IT growth strategy?

If your answer is more than a year or two ago – or worse, never – then you have some work to do. And with a new year just a few months away, there is no better time than now.

You see, an IT strategy is the foundation to moving your business forward. Improving productivity and profit. If you're just winging it, you're almost certainly wasting money and holding your business back.

This is why we're now offering you a FREE IT strategy review to discuss your plans and goals for next 12 months to 3 years, and to see if your current system is up to the task.

If you're open to a frank, no obligation, discussion about your plans for the future, book a (video) call now: Visit https://calendly.com/meetingtreecomputer and choose the time and date that suits you best.

Do You Know Exactly What Services Your Staff Are Signing Up For?

Whatever problem, need or want you have... there's a cloud application out there that can help you.

We've never lived in a such a rich time for problem solving. Every day, hundreds of new services launch to make our lives easier and help us be more productive.

These applications all live in the cloud. They're known as Software as a Service – or SaaS – because you don't load any software onto your device. You use them in your browser.

We would argue this SaaS revolution over the last 15 to 20 years has played a critical part in shaping the way we work today.

However, there's an issue. Many businesses aren't 100% aware what new services their staff have signed up to. And this problem isn't a financial one, it's a security one.

Let's give you a scenario. Suppose a member of your team, Shanice, is trying to do something creative, but just can't with her existing software. She Googles it and finds a cool application.

Shanice signs up for an account, and as she's in a rush uses the same email address and password as her Microsoft 365 account. Yes, reusing passwords is very bad practice. But this gets worse.

She uses the application for half an hour to achieve what she needs to do... and then forgets it. She's got no intention of upgrading to a premium subscription, so just abandons her account.

That's not an issue... until 6 years later. When that SaaS application is hacked by cyber criminals, and all its login credentials are stolen.

It's well-known that cyber criminals will try stolen details on other sites, especially on big wins sites like Microsoft 365.

Can you see the issue here? Shanice's 365 account would be compromised, and she'd have no idea how it happened. She won't remember an app she used for half an hour years before.

The answer is to have a solid policy in place about who can sign up for what kind of service. Also ask us about dark web monitoring and ways to track what apps are being used across your business.

And definitely get a password manager for your staff... this will generate a new long, random password for each application, remember it and autofill login boxes. Password managers encourage good password practice because they make it easy.

The Business Owner's Complete Guide to Phishing

Chances are you know about phishing.

It's where someone sends you a fake email pretending to be someone else. They're hoping you'll click a bad link or download a dangerous attachment.

It's one of the biggest kinds of cybercrime.

But do you know what the red flags are?

Here's our top advice on how to stay a step ahead of cyber criminals: https://www.meetingtreecomputer.com/files/2022/09/Complete-Guide-to-Phishing-Meeting-Tree-Computer.pdf

Q&A

Should I let my team have work apps on their personal phones?

It's personal preference. But if you do, make sure their phones are protected by the same security measures they'd have on work devices.

I've received an email that looks genuine, but hasn't addressed me by name. Should I click the link?

If you ever have cause for doubt, don't click links or download files. Phone the sender to check if they really sent the email. It may take a few minutes but it's worth it.

Should I be monitoring my remote staff?

Software exists to do this, but what message does it send to your team? It can be highly counterproductive in many cases. Take the time for regular catchups over Teams instead, or try a productivity tracker if you have concerns.

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