Meeting Tree COMPUTER

Deeply Rooted - Providing You With Secure Hassle-Free IT Solutions

HIPAA SEAL OF COMPLIANCE COMPLIANCY GROUP HIPAA VERIFIED

February 2020

The New York Shield Act Takes Effect In Less Than 60 Days!

Just when you think your worst IT projects are finally completed, all your computers now run on Windows 10, and life is good. Right?

Unfortunately, no. Wrong. There is a new challenge in town, going by the name of SHIELD Act. This past summer Gov. Cuomo introduced new cybersecurity regulations. Phase 1 of this new law took effect in October and covers new notification requirements; who do you need to notify if you fall victim to a data breach, what should these notices look like and what is a reasonable timeframe in which this is all supposed to happen.

We have been given until March 21st to implement phase 2. All businesses maintaining, collecting and using private information on New York State residents must implement what the law calls "reasonable safeguards." Reasonable in the sense that, depending on the size and nature of your business and the type of private information that you collect you will be required by law to implement different security measures to satisfy compliance requirements. Even business verticals already subjected to cybersecurity regulations will have to take a second look at the data they hold and how they are protecting it.

Over the next few months, we're going to be talking to you about some of these changes. Together we will decide what is reasonable for your business. As your IT provider we have a pretty good idea of what will be needed, but it is going to be up to you to decide how you want to proceed with implementation. It will be a great opportunity to mature a critical part of your business though, i.e. your information security processes. As, at this point, we're all well aware of the risks if we don't.

Call us if you'd like to get a head start. We're here to help.

If You Think Your Business Is Too Small To Be Hacked... You're A Cybercriminal's #1 Target

Many cybercriminals look at small businesses like blank checks. More often than not, small businesses just don't put money into their cyber security, and hackers and cybercriminals love those odds. They can target small businesses at random, and they are all but guaranteed to find a business that has no IT security – or the business does have some security but it isn't set up correctly.

At the same time, cybercriminals send e-mails to businesses (and all the employees) with links to phishing websites (websites designed to look like familiar and legitimate websites) or links to malware. They hope employees will click on the links and give the criminals the information they want. All it takes is ONE employee to make the click.

Or, if the business doesn't have any security in place, a cybercriminal may be able to steal all the data they want. If you have computers connected to the Internet and those computers house sensitive business or customer data – and you have NO security – cybercriminals have tools to access these computers and walk away with sensitive data.

It gets worse! There are cybercriminals who have the capability to lock you out of your computer system and hold your data hostage. They may send along a link to ransomware, and if you or an employee clicks the link or downloads a file, your business could be in big trouble. The criminal may request a sum of money in exchange for restoring your PCs or data.

However, as some businesses have learned, it's not always that simple. There are businesses that have paid the ransom only for the cybercriminal to delete all of their

data anyway. The criminal walks away with the money and the business is left to die.

And that's not an understatement! Once cybercriminals have your data and money, or both, they don't care what happens to you. Cybercriminals can do more than just major damage to small businesses; their actions can literally destroy a business! We're talking about the costs of repairing the damage and the cost of losing customers who no longer want to do business with you. You're looking at a public relations nightmare!

> **"The reality is that cyber security should be a normal, everyday part of any business."**

This goes to show just how critical good IT security really is, but business owners still don't take it seriously. Even as we enter 2020, there are business owners who don't consider cyber security a high priority — or a priority at all. It's a mindset that comes from before the age of the Internet, when businesses didn't face these kinds of threats. And many business owners fall into the habit of complacency. In other words, "It hasn't happened yet, so it probably isn't going to happen." Or "My business isn't worth attacking."

Cybercriminals don't think like this. It's a numbers game and only a matter of time. Business owners need to adapt to today's online landscape where just about everything is connected to the Internet. And if something is connected to the Internet, there is always going to be some level of vulnerability.

But you can control your level of vulnerability! You can be cheap or complacent and do the bare minimum, which will put your business and customers at risk. Or you can take it seriously and put IT security measures in place – firewalls, malware protection, secure modems and routers, cyber security insurance and working with a dedicated IT security company. There are so many options available to secure your business.

The reality is that cyber security should be a normal, everyday part of any business. And anyone thinking about starting a business should be having the cyber security talk right from the very beginning: "What are we going to do to protect our business and our customers from outside cyberthreats?"

When it comes down to it, not only do you need good cyber security, but you also need a good cyber security policy to go along with it. It's something you share with your team, customers, vendors, investors and anyone else who puts their trust in your business. Transparency about your cyber security is a great way to build and maintain trust with these people. If you don't have IT security in place, why should anyone trust you?

Think about that question and think about the security you have in place right now. How can you make it better? If you need to reach out to an IT security firm, do it! It will only make your business better and prepare you for the threats that are looming right now. No business is too small or too obscure to be hacked.

Can We Bribe You To Do Us A Favor?

We love having you as a customer and quite honestly, wish we had more like you! So instead of just wishing, we've decided to hold a special "refer-a-friend" Valentine's Day month special for the clients we love the most – YOU!

Simply refer someone you know needs our help and we'll send you a special Valentine's Day box of **DELICIOUS TRIPLE FUDGE BROWNIES** plus we'll give the person you refer a FREE Technology Tune-Up to make their systems run faster, cleaner and with fewer problems (that's a $397 service…absolutely FREE!)

You can refer someone by simply sending us an e-mail at mduci@meetingtreecomputer.com with the name of a friend (or two) that you'd like to refer to us, or call us at **(845) 237-2117** and just tell us who you'd like to refer.

We promise to be extremely respectful to the people you send our way and will treat them with 'kid gloves.' That means we won't put any heavy sales pressure on them, and we promise to deliver the same top-notch service to them that you've come to expect from us. After all, we don't want to harm our relationship with you in any way.

3-2-1 Backup!

Quarterback, linebackers, cornerback, running backs and back up players – who is ready for the Superbowl? Having an effective backup strategy in place is essential in any endeavor, whether it's in sports or in your business. How, where and what you back up makes a major difference in your ability to recover should disaster strike.

There is a well-documented industry best practice standard for backing up your critical data. It is known as the 3-2-1 Backup rule: Have at least t**hree copies of your data**, Store the copies on **two different media,** Keep **one backup copy offsite**.

Sounds pretty good, right? It is, but there is more to consider than just backing up your data, i.e. your files. Let's suppose you could back up all the personal items you have in your house—your clothes, furniture, valuables, etc., and somehow maintain a copy of everything in a warehouse 1,000 miles away from your current residence. Now let's suppose (and God forbid) your house burns down, destroying everything with it. You'd be relieved that you had a copy of everything somewhere else.

But here's the problem: If your house burned down, you might have a copy of everything you own, but you no longer have a place to put it. So, for starters, you have to rebuild the house. Next, you have the project of getting everything out of that storage unit into your NEW house. Then you have to rearrange everything. This is exactly how most backup systems work UNLESS you are running "image" backups. An image will allow you to restore your server, PC, device, etc., FAST because you're not backing up single items but, instead, the ENTIRE HOUSE.

Call us at **845-237-2117** to see how a solid disaster recovery strategy can help you safeguard your business in the event disaster strikes.

3 Reasons Why Recessions Are Awesome For Great Companies

It may be jarring to read the words "recession" and "awesome" in the same sentence. Recessions are bad for most people. I will not make light of how horrible recessions are for the vast majority of companies and their employees, (as well as for not-for-profit organizations and governments).

For most companies, recessions mean increased stress at work, stalled career progression or even layoffs, uncertainty, increased board and shareholder pressure, increased financial strain and a feeling of looming danger in the pit of your stomach, which is no fun to wake up to every day! But for great companies, recessions can be awesome.

What are great companies?

Great companies make great products or deliver great services to customers. They provide a wonderful work culture that attracts and retains talented people. And because they take great care of customers and employees, great companies don't have a dangerous debt burden. They are profitable and able to pay their bills to suppliers while delivering an attractive return to investors in dividends and equity appreciation.

How are recessions awesome for great companies?

<u>Recessions allow great companies an opportunity to do the following:</u>

1 Shake loose the cobwebs of complacency.
"Success breeds complacency," said Andy Grove, the legendary CEO of Intel. And while I'm not here to suggest everybody embrace full-on "paranoia" in the workplace (Only The Paranoid Survive), I am here to suggest that great companies have to keep hustling to stay great. A recession provides an opportunity for a

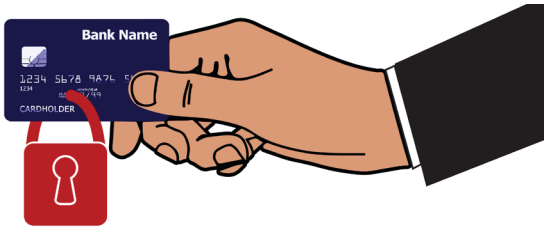
wake-up call to great companies that may start to coast on past greatness and help them get back on track.

2 Take customers and colleagues away from lesser companies that don't deserve them.
As lesser companies stumble during recession (e.g., shutting locations, letting service and quality drop, highlighting dysfunction in the culture, etc.), it's the perfect time for great companies to pick up more customers and talented people. I remember when a successful business services company with 70 locations around North America entered the '08 recession. Lesser competitors were closing branches and laying off people, and service was slipping. But the CEO of the successful company was not fearful about the recession. Instead, he sensed the opportunity to win more customers with better service and poach some top talent away from the struggling competitors. The recession allowed this great company to gain market share and build a stronger leadership talent pipeline.

3 Increase the rate of learning of your leaders.
Time seems to move more quickly for me during harder times than during easy times. This can improve the learning curve of your up-and-coming leaders. Just remember to not make too many decisions for them; that will stunt their growth. Allow your leaders to come to you with problems and solutions, and coach and support them. Let them test and learn various approaches to leading through uncertain times.

Geoff Smart is chairman and founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the New York Times best-selling book, Who: A Method For Hiring, and the author of the No. 1 Wall Street Journal best seller Leadocracy: Hiring More Great Leaders (Like You) Into Government. Geoff co-created the Topgrading brand of talent management. He is the founder of two 501(c)(3) not-for-profit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring, and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a BA in Economics with honors from Northwestern University, and an MA and PhD in Psychology from Claremont Graduate University.

7 Things To Do So You DON'T Get Hacked When Shopping Online



1. Verify the URL is safe.
Many browsers have a little padlock in the URL bar. If the padlock is closed, the URL is safe. If it's open, you may want to avoid the site.

2. Verify the URL is accurate.
Many scammers register fake websites using misspelled URLs or extra numbers to look like the real deal. If the URL looks odd, it's probably a scam.

3. Use a secure web browser.
Firefox and Chrome, for example, always navigate to HTTPS (Hypertext Transfer Protocol Secure) websites. These websites are more secure than their HTTP counterparts.

4. Don't click suspicious links or attachments.
Never click a link if you can't verify it first. In fact, it's better to delete any e-mail you don't recognize.

5. Always bookmark authentic websites.
When you bookmark real websites, you never have to worry about mistyping or clicking scam links.

6. Rely on a password manager.
It's hard to remember strong passwords, but with a password manager, you don't have to. Never use a bad password again!

7. Use the official mobile apps for online stores.
If you download the official app of your favorite online stores, such as Amazon or eBay, you don't have to worry about accidentally navigating to a scam website. Just make sure the app is verified by Google or Apple. *Lifehacker, Nov. 19, 2019.*

Top 2 Tips For Scaling Security For Your Small Business

Put a greater emphasis on passwords. The more passwords employees have to remember, the less likely they are to have strong passwords and the more likely they are to use the same password for everything. Another problem is password sharing. A team of people may share a single license for a piece of software, which means they share a single password. Password managers like LastPass can save a lot of hassle while still protecting your accounts, and many password managers are scalable.

Rely on multi-factor authentication (MFA).
MFA adds another layer of security on top of firewalls and malware protection. It's like adding an extra password on top of your existing password, though only you can enter it. However, some employees skip MFA because it adds extra steps to the login process. But an extra 15 seconds to log in is worth it for the security.

This Month We Would Like To Welcome To Our Family:

Advance Testing Co. Inc. and the Law Offices of Adam Singer, PLLC.

Thank you for your trust and your business!

We look forward to supporting you for a long time to come.

Follow Us On Social Media!

http://bit.ly/MeetingTreeComp-Facebook

http://bit.ly/MTC-LinkedIn

A referral from a friend, Client, or colleague is the highest compliment we can receive.

www.MeetingTreeComputer.com
Phone: (845) 237-2117