Welcome everyone!

It is great to see all of you.

Before we get started:

I believe the most successful speaking engagements are when the audience is allowed to speak up about their own experiences and ask questions so, please feel free to do that. I want to ensure that everyone walks out of this room today with at least one call to action!

So, lets get started!

What About Cyber Security Compliance?

Ensures that the Technology you use is in line with the laws and regulations set forth by your governing body.

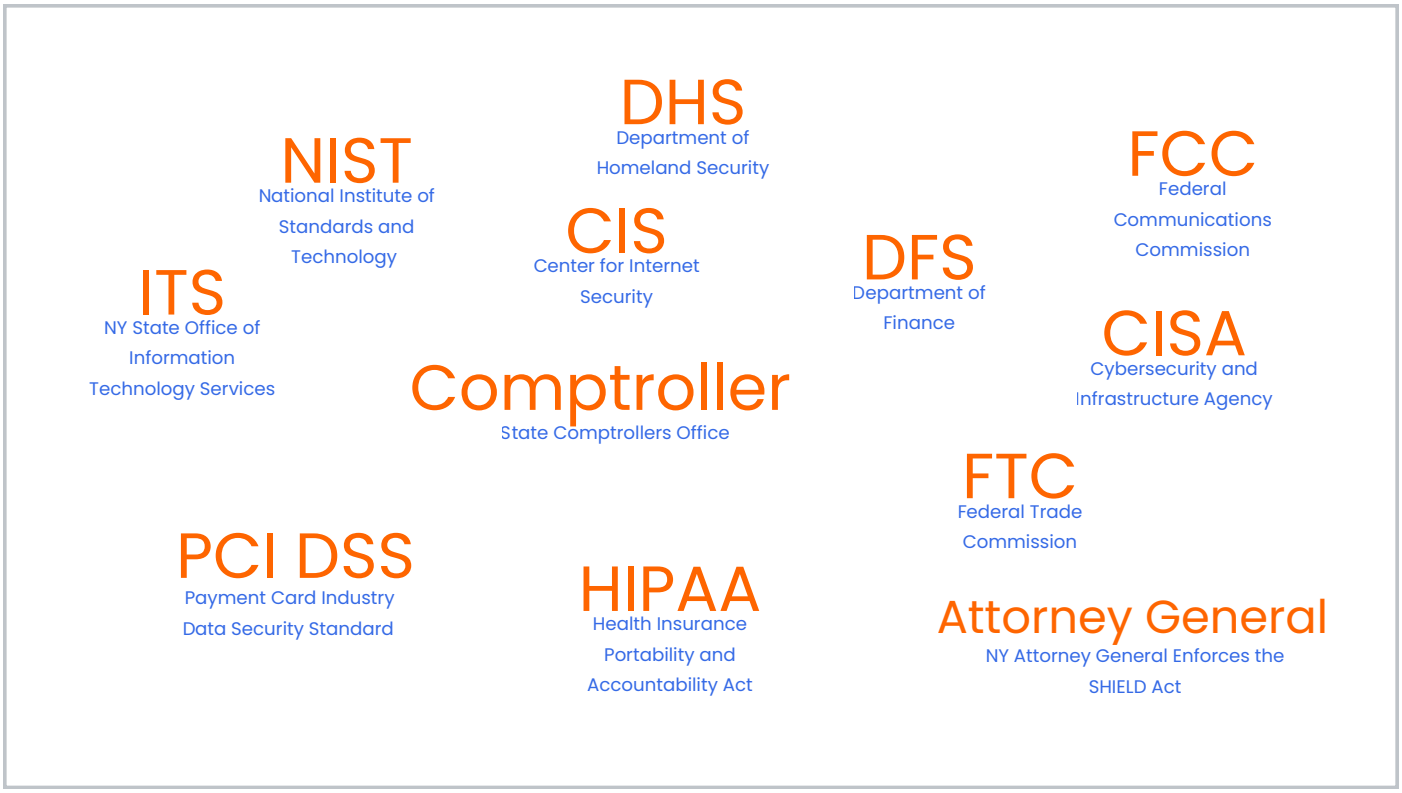
Here's what I Know....

This is probably low on your priority list...if its even on your list!

IT For Local Government assists municipalities with the compliance guidelines that are being recommended by the State and Federal Government as well as Cyber Insurance Guidelines.

Based on your Industry, the State and Federal Government has recommendations and requirements on how you secure your communities information. They are not always clear which is why having a company like CST / IT For Local Government can help with sorting it all out.

(next slide)



Here are few of those agencies. Determine which ones you should be following.

I evaluate ALL of them on my clients behalf and we pivot security measures based on it.

NIST has the Cybersecurity Framework as well as NIST 800-53 (government controls) and 800-171 (contractor requirements)

The Attorney General's office enforces the Shield Act - requires "reasonable safeguards" for data protection and Administrative, Technical and Physical Controls

What is Cybersecurity Risk?

According to the National Institute of Standards and Technology (NIST) – It is the loss of confidentiality, integrity, or availability of information, data or IT controls and reflect the potential adverse impacts to organizational operations.

(Definition based on ISO Guide 73 [6] and NIST SP 800-60 Vol. 1 Rev. 1 [7])

So before we dig in – what is Cybersecurity Risk?

According to NIST – the National Institute of Standards and Technology – it is the loss of confidentiality, integrity, or availability of information, data or IT controls and reflect the potential adverse impacts to organizational operations.

(next slide)

IT IS NOT IF YOU WILL GET ATTACKED – IT IS WHEN

It is not IF you will get attacked – it is WHEN!

The goal now is to take every precaution to minimize the RISK.

(next slide)

What is YOUR Current Risk?

You Have NO Cybersecurity in Place
.....risk is all yours

You Have Some Cybersecurity in Place
.....risk is shared

You Have All The Things in Place
.....risk is with someone else

What is YOUR Cybersecurity Risk?

Think of cybersecurity risk like the security for you and your family.

How many of you...

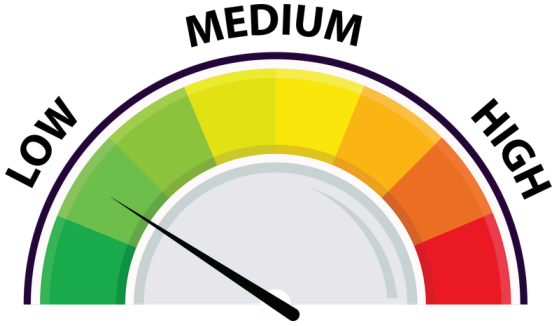
Lock your doors?
Lock your windows?
Lock your car?
Have a fence around your home/property?
Have security camera's?
Have a dog?
Have INSURANCE?

These are all layers of security. Think of your business the same way?

(next slide)

To Lower Your Risk...

Have Layers of SECURITY!



Just Like your Personal Life, You need to have LAYERS of Security in your business!

The more layers of security you have, the lower your risk.

What layers does your business or organization have in place now?

Where would the needle of this graph be for you?

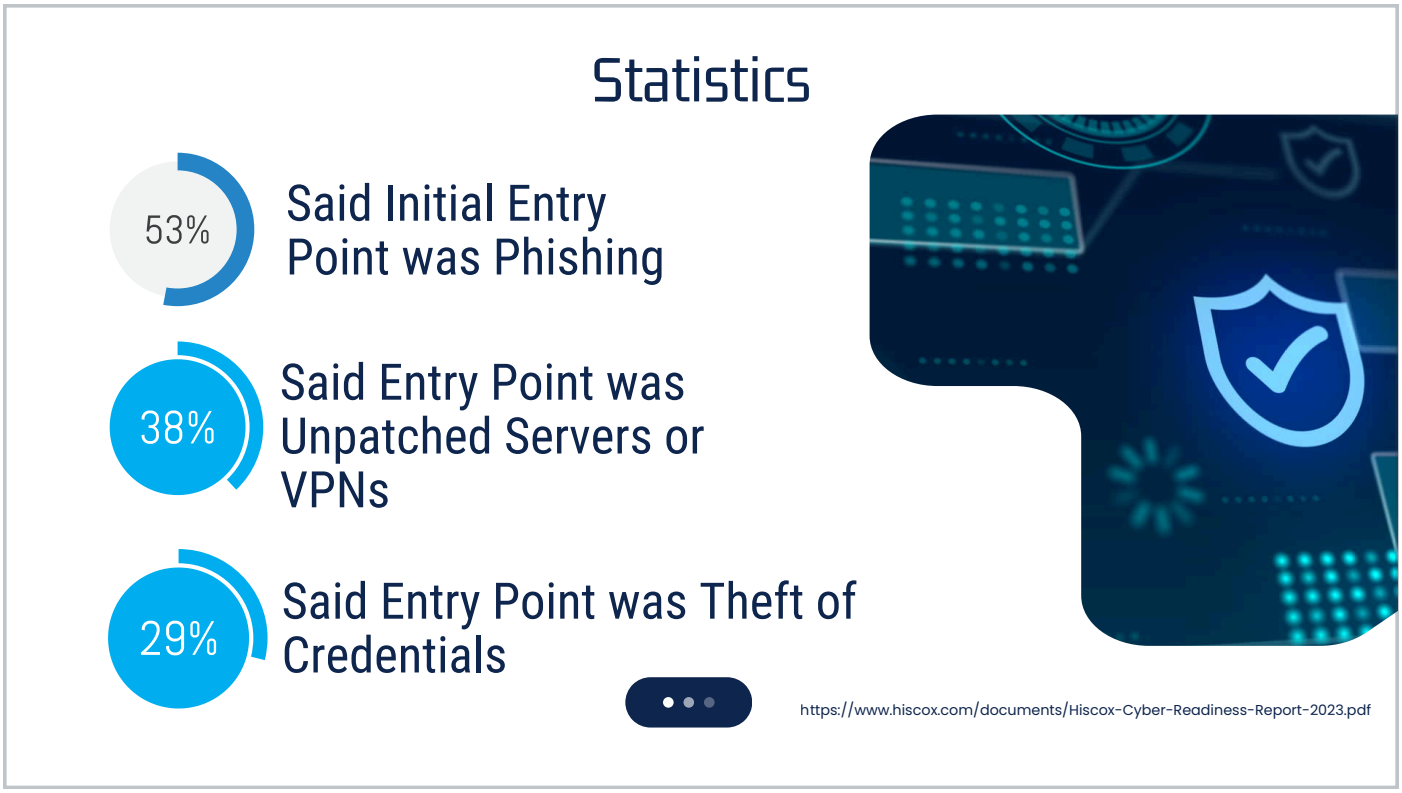
(next slide)

What are the odds of getting an attack?

73% of US Small Businesses reported a cyber attack or data breach in the past 12 months

https://www.hiscox.com/documents/Hiscox-Cyber-Readiness-Report-2023.pdf

(Next slide)



Statistics continued...

In U.S. small-business ransomware cases, reported initial entry points were phishing 53%, unpatched servers or VPN 38%, and credential theft 29%.
Hiscox

(Next slide)

Statistics continued...

Among US Small Businesses that paid a ransom, 50% did not fully recover their data.

Of those, approximately 1/3 of them were asked to pay more or attached multiple times

and....1 in 3 were attached again.

Could your business survive this?

(Next slide)

That means.....
They thought they were safe....

They may have been investing in security.....

AND.....Attackers still got in!

In Cybersecurity, what worked yesterday – does not work today!

And hackers are counting on it!

Let's be honest – every responsible company should protect and secure their data!

Let me put it another way….

How would you feel if your doctor, had ZERO precautions in place to protect your medical records? What if he/she had no firewall blocking access to your information? How would you feel about that?
What if you knew that your favorite store, had NO security in place to protect your credit card every time you swiped it?
What about your bank? How would you feel if they had no security in place?

We make pretty huge assumptions that ALL businesses are protecting YOUR information – but are they?

This topic is expanding as we work through 3rd party vendor cyber security regulations. This means that every company you do business with needs to have the same or better security protocols than you! This is happening sooner than you think and is a discussion all on its own.

(next slide)

So – knowing all of this – let me give you the FIVE TIPS that will reduce your risk!

Your BIGGEST risk is You and Your STAFF – EDUCATE THEM –OFTEN!

According to Verizon's 2025 Data Breaches Investigations Report, 60% of data breaches involved a human element.
This includes incidents in which employees expose information directly (for example, by misconfiguring databases) or by making a mistake that enables cyber criminals to access the organization's systems.

Implementing Training is more important than ever…

Do any of you remember the MGM Breach in September 2023? This breach involved the IT Help Desk where a help desk technician received a phone call from who he thought was an executive in the company. He then proceeded to reset a password for this person. Except….it wasn't the executive. It was a $100 million dollar hit to the organization. All because there was no process in place of how to verify an employee's identity before doing something like….changing a password!

(next slide)

How Do You Perform SAT?

Email Phishing Simulations?

In Person Meetings?

Webinars?

***Document** your security protocols to ALL staff, regularly.*

So how you do perform SAT?

Ideally, you should have automated phishing simulations to determine who, in your organization, is putting you at risk….

You should also do Quarterly In-Person Security Awareness Training - Annually at minimum.

However, you should always be communicating your policies and procedures and document all security protocols and then SHARE that information with your STAFF on a regular basis.

Be sure you document it all – what you are doing, when you did it, etc. This will all matter if you ever get a breach.

(next slide)

Here is a quick checklist of what you should see

Staff should be able to

1. Recognize email phishing attempts
2. Know how to secure email with encryption
3. They should know when it is appropriate to click a link in an email
4. When it is appropriate to download a file
5. They should know how to verify someone's identity
6. And finally, they should know how to identify and handle financial transactions!

(next slide)

Number TWO –
Enforce Complex Passwords!

I know, I know, everyone HATES passwords – but this is the first line of defense when accessing your information and accounts and if you make that password “password” you are inviting cyber criminals in.

How are you managing your passwords? What about your staff?

(next slide)

Passwords On Paper are NO LONGER ACCEPTABLE!

Passwords on post it notes are no longer acceptable and
Neither is a notebook in your desk drawer or paper under your keyboard.

We need to implement more sophisticated ways to track passwords!
Oh, using the same password over an over again – also a NO, NO!

Or using the same password with slight variations – also a NO!
(next slide)

How Do You Manage Passwords?

(and your employee's passwords)

How are you managing your passwords
Your staff passwords?

With so much being "cloud" based – there are more passwords than ever! It used to be just a computer passwords – one – and you had access to everything - but that is certainly not the case anymore.

It is time to take control over how your organization is managing passwords.

Let me give you an example. We had a client who fired an employee – when the employee left (on less than favorable terms), she left with ALL her credentials. Including accessing her computer, software, logins, state websites, all of it!

What would you have done?

(next slide)

Enforce Strong Passwords

Requirements:

- Never Reuse Passwords
- Strong Complexity
- 16 or more characters

I get it, everyone HATES having to manage passwords.

Everyone manages them different, and I bet if I were to take a poll right now of how many of you have at least ONE password written on a post it – I would get 100% positive response.

That protocol Is no longer acceptable. There are easier ways to manage your passwords by implementing a password manager where you create ONE complex password and the software manages the rest of them!

TIP for creating passwords - Use a phrase instead of a word to help with remembering your ONE complex password to access your password manager – something like “I L0v3 Purpl3 Sk1es!!” is 21 characters long and significantly more complicated to crack.

Password Managers

- Stores Passwords
- Sends Alerts
- Generates strong new passwords
- Automatic Fills Credentials

Encryption ensures that the password manager never "knows" what your passwords are, keeping them safe from cyber attacks.

Consider implementing a Password Manager – why?

Because it will store your passwords, alerts you of duplicates, generates strong, complex passwords and
automatically fills in when you need them and…..

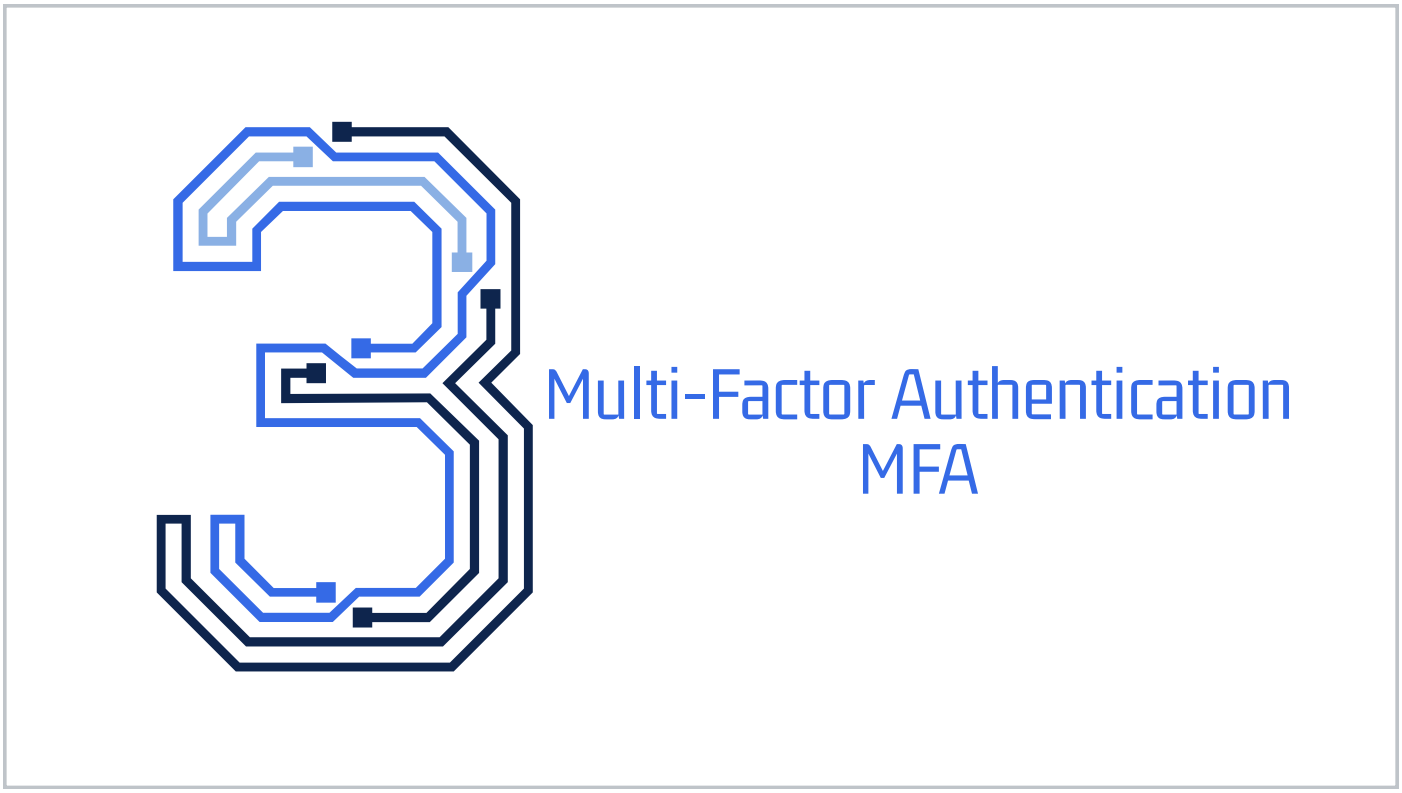
You only need to remember ONE – the ONE password to your password manager – It will remember all the others.

Passwords are secure and encrypted so not even your manager knows what they are and you should consider one that provides administrative controls so you would be able to gain access to all employee's passwords.

Options for Password Managers include –
BitWarden
NordPass
1Password

CST uses an enterprise password manager that links to our documentation process. This allows us to ensure passwords are updated as our clients and their staff update them. This keeps all your documentation in your Detailed Technology Manual.

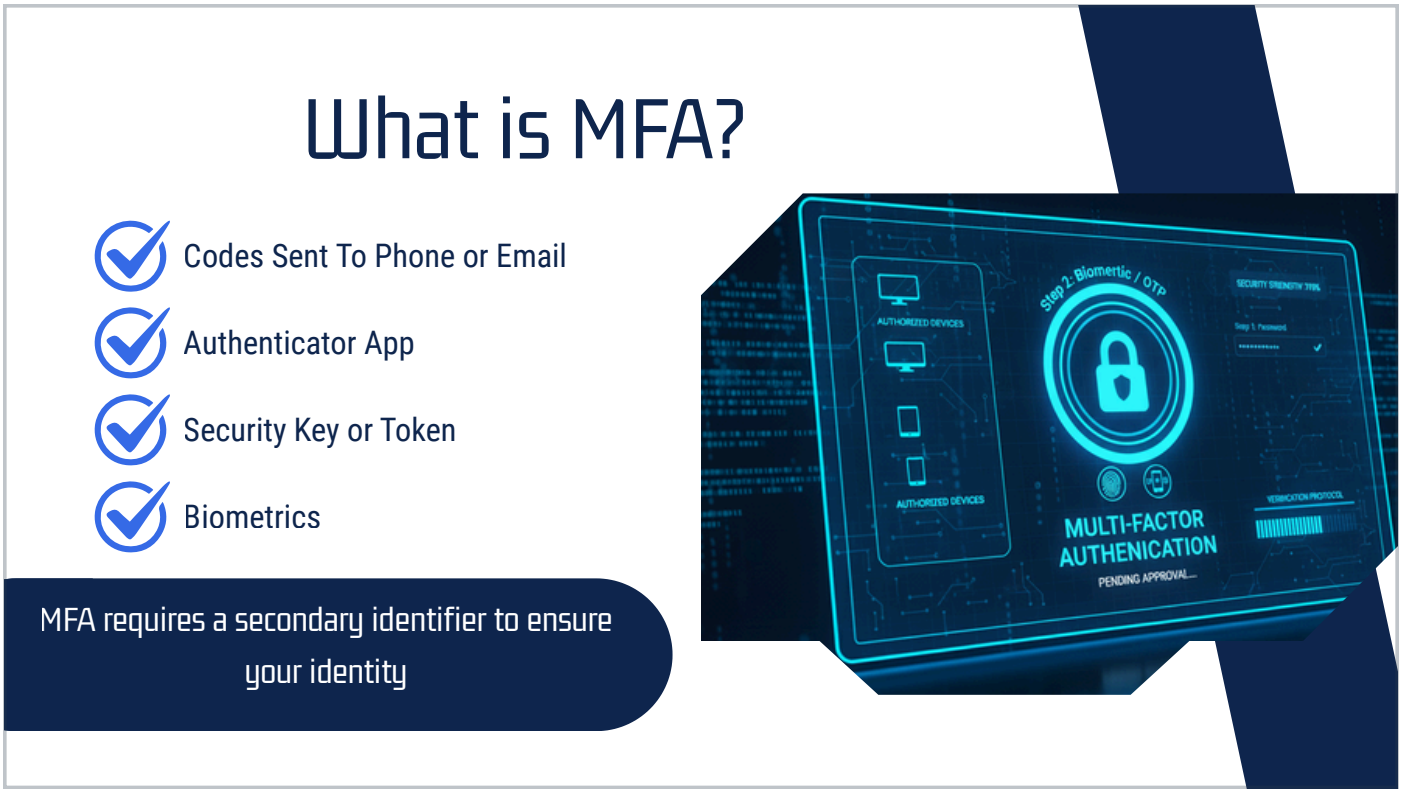
(Next Slide)



Three – Multi-factor authentication – also called two factor authentication or MFA/2FA

Honestly, we all hate this one – but it is a necessary evil when it comes to protecting your information.

(next slide)



MFA is security measure that allows the software to verify you are who you are by requiring another piece of information from you other than a password. Most software companies are now requiring this level of security.

How are you going to handle MFA requirements? Will employees be asked to download authenticator apps on personal cell phones? Receive text messages on their personal phones?

Come up with a plan so you can manage how MFA is going to work within your organization.

(next slide)

Where should you use MFA?

ON ALL ACCOUNTS – PERIOD!

NOTE: There has been some concern about HOW you manage employee MFA where an employee refuses to put work authenticator on their personal phones. This is one of those things that should be part of the hire protocol and there should be a policy in place regarding however you choose to handle it.

Some options?
Company phone – does not need a cell provider – just wifi
An authenticator device also called a security key or hardware token – like YubiKeys (if your company allows usb/usb-c devices).
Find another way like FortiToken on the Microsoft Store, Duo by Cisco Systems,
Use an email to two factor

So, what do I mean when I say Updates, patches and scans?

(next slide)

Updates – ensure your devices and applications are protected from the latest threats – you see when it comes to your Operating Systems – Microsoft opening admits that both they and hackers are finding flaws to get into your computers through a flaw within the coding. Microsoft identifies what they are and sends out updates and patches to "fix" the holes. If you do not download and apply these updates and patches, you are basically leaving the door open to your house!

Inviting the hackers in.

When we talk about updates, patches and scans, remember that it is NOT just your Operating System – It is ALL of your hardware AND software…so don't forget about network appliances, printers, and ALL the software you use.

Remember ALL software gets patched when the company realizes their may be a hole within their software that a hacker could get through – those patches are what keeps their software secure. If you are not getting them, then you are at risk by simply having your system ON and connected to the Internet.

Although you may have "auto updates" on, you still need to check them to make sure they are happening. Some updates will need your assistance, some will only download and install if they are the only one and some will require additional assistance – like a restart!

Pay attention to them!
(Next Slide)

Patches

Fixes any “holes” or known issues within your software.

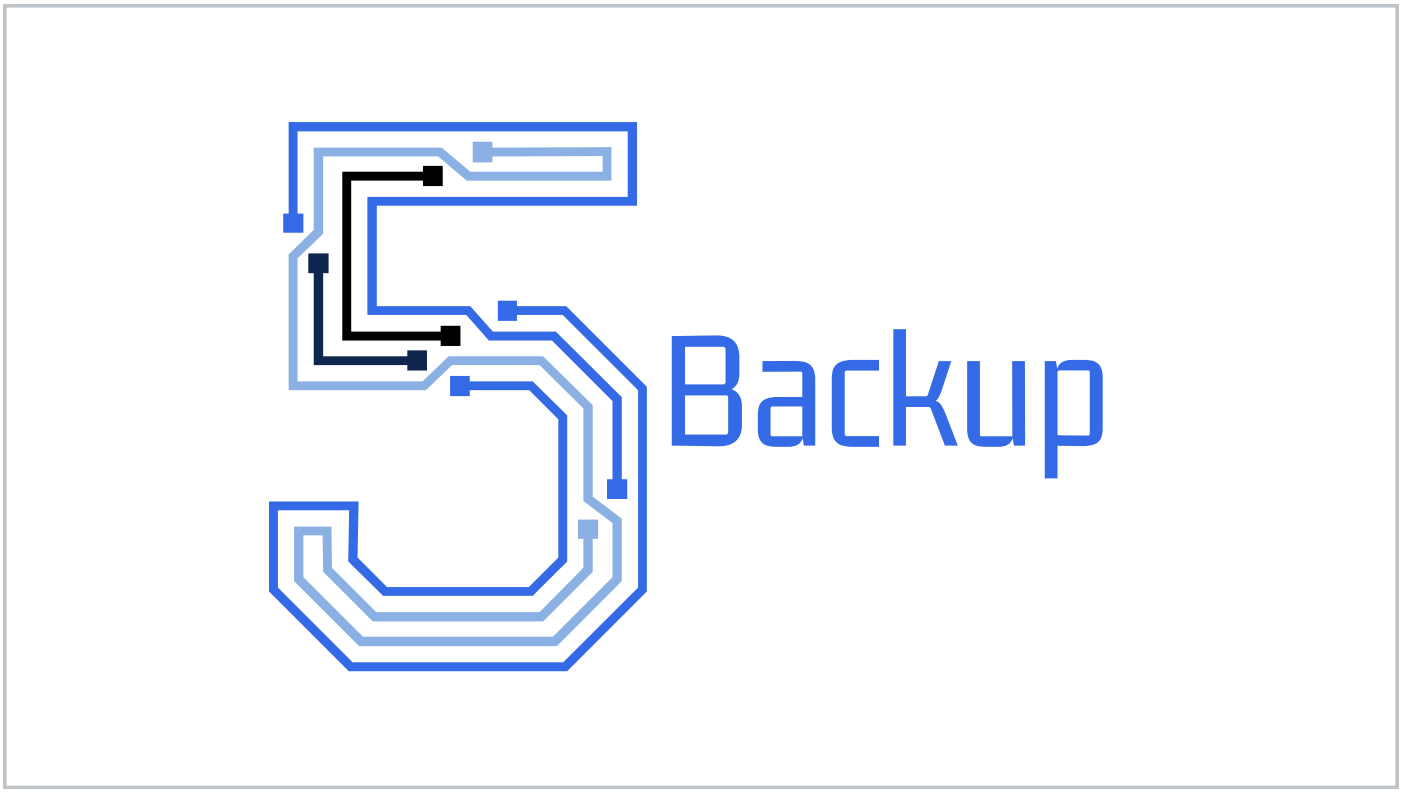
Patches fix the holes or known issues with your software.

A patch will normally come down (or be installed) along with the updates but, on occasion, patches run separately and sometimes they will be at the request of your software provider.

For example, local government clients use BAS or Williamson Law. On occasion, they will ask you to install a patch to fix a known issue.

Scans actually look for AND identify issues within your system.

These scans are important to us because it allows us to fix issues before they affect you.



This one is tough because most everyone will tell me they have a solid backup! Do you?

(next slide)

When I ask a business to identify where their data is, over 90% have no idea. Do you know where your data is located? When I ask - they usually say – "it is on a flash drive or external hard drive" or they may say "its in the "cloud"" without really understanding what that means.

Now let's talk about the Backup of that data? Where is that? Is it being tested?

Key Components of the 3-2-1 Rule

3 Total Copies: The original data, plus at least two backups.

This protects against simultaneous failure of multiple storage devices.

2 Different Media: Store backups on at least two different types of storage, such as local hard drives, USB drives, NAS devices to avoid a single point of failure.

1 Off-Site Copy: Keep one copy in a different physical location to protect against local disasters like fire, theft, flood.

REMEMBER TO VERIFY AND TEST BACKUPS REGULARLY!

We had a break/fix client a few years back who assured us they had backups in place. Until they received a Ransom Attack! When we got the call, we spoke with the owner who advised his backup was verified the previous night. Upon arrival, we realized that the backup drive (a USB

Hard Drive) was plugged into the Server. The device was hit and the backup was completely useless to us. This client paid over $60,000 to get their data back.

Disaster Recovery Plan

This will include
RTO's - Recovery Time Objective
and
RPO's - Recovery Point Objective

Both will drive your backup process!!!

Consider developing a Disaster Recovery Plan – a plan that is laid out ahead of time, discussed with stakeholders and put in to position if a disaster occurs. No stress, no doubt!

By doing this, you will create an RTO and RPO which will impact how you do your backups.

BONUS TIP - Must Haves

Hardware Firewall

Managed Detection and Response

Endpoint Detection and Response

Firewalls are now a required element! You need to have a physical device between YOU and the Internet. This device will prevent breaches through your Internet connection.

Managed Detection and Response (MDR) is a service that combines technology with human expertise to provide 24/7 security monitoring and threat hunting across an entire network, cloud, and endpoints.

Endpoint Detection and Response (EDR) is a technology that monitors and responds to threats on individual endpoints, while

The key difference is the addition of human analysts and broader network visibility in MDR, which can be a good option for organizations lacking in-house security staff or expertise. EDR is a tool for an organization's internal security team to use, while MDR is an outsourced security service.

ITFLG uses a FOUR step approach when reducing cybersecurity risk.

1. Assess Risk - we evaluate your current situation. What do you have in place and what you do NOT have in place.

2. We implement controls - using the recommendations and requirements from your governing body and insurance provider.

3. We monitor and support - 24x7x365.

4. We help train your team - education is incredibly important to keep your business secure.

100% CONFIDENTIAL RISK ASSESSMENT

SECURITY SNAPSHOT

DISCOVER WHERE YOUR BUSINESS MAY BE VULNERABLE BEFORE CYBERCRIMINALS DO.

Your Assessment Will Reveal:

- **If employee passwords and credentials are exposed on the Dark Web**
- **Whether your systems are truly protected from hackers and insider threats**
- **If your backup can survive a ransomware attack or disaster**
- **Whether your IT environment meets data protection compliance standards**

Plus You'll Receive:
A Customized Total Potential Liability Report outlining your financial exposure based on identified vulnerabilities.

Everything we discuss and uncover remains strictly confidential.

Would you like to know your current risk?

ITFLG is offering a FREE Risk Assessment/Security Snapshot of your existing network. Even if you have an IT Provider, wouldn't you like to know if there are any open doors or windows?

Scan the QR code to sign up.

Now, I want to remind you that technology changes regularly – so here is what to expect in 2026

Ready For A Raffle?

Amazon Best Selling Author, Lisa Brown presents....

"From Exposed To Secure"

The Cost of Cybersecurity and Compliance Inaction And The Best Way To Keep Your Company Safe

I am so proud to have been involved in co-authoring this Amazon #1 Best Selling Book.

If you don't win, you can purchase it on Amazon and all proceeds go to St. Jude Children's Hospital.

I wrote this e-Book specifically for Local Governments.

Limited IT resources, outdated systems, and human error make towns and villages prime targets for cyberattacks. Protecting data and community trust now requires proactive, modern cybersecurity—because one click can change everything.

It contains valuable information and I am offering it for FREE.

Scan the QR Code to grab your free eBook download today!


QUESTIONS ?
Thank You for Attending
Presented by Lisa A. Brown
www.itforlocalgovernment.com
lisa@itforlocalgovernment.com

Questions?