TechConnect

WILD FROG CONSULTING

People-First IT Services For Central Ohio / July 2023

What Compliance Standards Does Your Business Need To Maintain?

Compliance standards are some of the most important things a business needs to maintain to be profitable and well-respected while staying out of legal trouble. Failure to meet these standards will make your business susceptible to fines and legal action. You'll also take a hit on your reputation as customers, vendors and competitors may find your business to be untrustworthy. By enforcing compliance, you're working to promote ethical behavior while protecting the rights of your employees, customers and other stakeholders.

But it's not always obvious which compliance standards apply to your industry or specific business. While most businesses need to ensure they're following Occupational Safety and Health Administration standards for workplace safety, they must also meet Environmental Protection Agency regulations for protecting the environment. There are also compliance requirements that have to do with the information you store and share. Here are three other compliance standards that you should know about if you're a business owner or leader.

Health Insurance Portability And Accountability Act (HIPAA)

You probably already know about HIPAA if you've been to any doctor's appointment in the past two decades. This law was enacted in 1996 to protect the privacy of individuals' personal health information and to ensure the security of that information. HIPAA only applies to "covered entities," which include health care providers, health plans and health care clearinghouses. These entities must comply with the rules set forth by HIPAA when handling protected health information. They must have the necessary administrative, technical and physical safeguards in place to ensure the confidentiality, integrity and availability of the information.

There's been confusion in the past relating to HIPAA, especially during the Covid-19 pandemic. When employers requested vaccination status from their employees, many claimed that this violated HIPAA, which is false. HIPAA only applies to covered entities. It's essential that you know the ins and outs of HIPAA if you work in the health care industry. Noncompliance can lead to fines, legal trouble and, in some cases, the loss of your license to practice medicine.

National Institute Of Standards And Technology (NIST)

The NIST is a non-regulatory agency of the United States Department of Commerce that develops and promotes standards, guidelines and best practices for ensuring the security and privacy of information systems. NIST compliance is vital for any organization that handles sensitive information, such as personal data, financial information or intellectual property. It becomes even more important for heavily regulated industries like health care, finance and government. NIST compliance can help organizations protect against

>> CONT. PAGE TWO

Compliance Standards

>> CONT. FROM PAGE ONE

cyberthreats, data breaches and other security incidents. It also helps organizations meet regulatory requirements set by HIPAA.

When you adhere to NIST standards, you'll easily identify vulnerabilities, improve incident response plans and prioritize security measures. The NIST has created a helpful framework and various publications that provide guidelines for various systems and scenarios. If you're looking for a specific publication or are interested in other NIST resources, head to their website, NIST.gov, for more information.

Cybersecurity Maturity Model Certification (CMMC)

The CMMC is a framework developed by the U.S. Department of Defense to assess and certify the cyber security practices of organizations that work with the DoD. This framework includes a set of controls and processes that organizations must implement to protect sensitive information and systems from cyberthreats. The CMMC framework applies to all organizations that work with the DoD and handle Controlled Unclassified Information. This often includes defense contractors, suppliers, subcontractors and organizations that provide services to the DoD, such as IT, logistics and engineering. Businesses that support the defense supply chain, including manufacturers, technology firms and professional service providers, also need to adhere to CMMC guidelines. Failure to achieve CMMC certification can result in being unable to bid on or win DoD contracts.

Compliance is something every business needs to be aware of, regardless of industry. Start by investigating HIPAA, NIST, and CMMC to see if their rules and regulations are applicable to your business, then look to other organizations. Doing so will help set your business up for success.

NOT PATCHING SOFTWARE COULD COST YOU!

Back in September we wrote about why it's so important to keep your software up to date. It's how security holes get fixed. It's how vendors roll out new features & functionality. Cyber insurance questionnaires have become a lot more detailed and more particular in the last several years.

For a while now, carriers have wanted to know that you have a documented process for ensuring that updates are applied to your technology estate in a timely fashion. That means monitoring and verification. Back when desktop computers ruled the landscape and everybody worked at desks, this was relatively easy. Leave computers on overnight, software was updated. Then just walk around to be sure. This isn't the case anymore. As companies started moving to laptops - and then to WFH - you may not even have a central office anymore. Then on top of it all, Apple has now officially said that they will only guarantee security fixes for the most current version of macOS. It's made what was already an extremely challenging task nearly impossible.

But, you know what? Your cyber insurance provider doesn't care. They're expecting you to keep your systems patched and up to date because they know it's one step that reduces the chances of your having a cyber incident - necessitating a claim you'd expect them to pay.

Well. . .insurance carriers are starting to back that up. Chubb, a national insurance carrier, has started implementing a 45-day grace period for patching. That is, when there's a software patch/update that addresses a known vulnerability (known as a CVE) they expect you to apply that patch within 45 days. If the update is not applied after the 45 day grace period the carrier will incrementally reduce the amount of a claim they're willing to pay out. And it makes sense. We tell people all the time that security isn't a 'thing' - it's a collection of choices. Insurance carriers are now saying that allowing your software to become out of date is a risky choice. And they'd rather not continue to pay for their customers' risky choices. I fully expect other carriers to follow Chubb's lead on this.

So What To Do?

You need to have a plan in place to ensure these updates happen in a timely fashion. And trusting your employees to just take care of this on their own isn't a plan. And paying for a low-cost IT provider who only shows up when something breaks isn't a plan either. A competent IT provider should be able to explain in plain English their process for keeping your fleet up to date. They should also be able to show you how they monitor your fleet to ensure it gets done. Patching is one of the most basic functions of an IT provider. So if they can't do these things run away fast!

If you're concerned that your fleet may not be kept as up to date as it should be, drop us a line at help@wildfrog.net and we'll be glad to help.

TEN SIMPLE STEPS TO HELP PROTECT YOUR BUSINESS

Small businesses are particularly susceptible to cyber attacks for a number of reasons. But here are ten things you can do to help protect your business.

1 - Keep your software and operating systems up to date. To protect against known vulnerabilities, make sure to apply security updates and patches for both operating system and apps within a week of their becoming available.

2 - Use strong passwords. Our recommendation is passwords should be at least 16 characters and contain at least 3 of the following 4 criteria -

- Upper case
- Lower case
- Number
- Symbol (such as @, #, $, %, & or !

Each password should be unique and not re-used for any other login. Think of it more like a passphrase than a password. We strongly recommend a password manager such as 1Password or Keeper.

3 - Be cautious of email and social media. Be wary of clicking on links or downloading attachments from unknown senders. Scammers often use phishing emails and social media to trick you into giving away personal information. Additionally, do not click links or attachments from email on your phone. It's virtually impossible to look for the signs of malicious intent in your phone's email app.

4 - Use anti-malware software. Contrary to popular belief, Macs can and do get malware! Advanced anti-malware software not only looks for viruses but dodgy behavior like an app requesting permissions it shouldn't have.

5 - Use encryption to prevent bad guys from seeing the contents of your hard drives. FileVault for macOS and Bitlocker for Windows make this easy, but things like backups should be encrypted as well.

6 - Back up your data and regularly test restoring data. We recommend backing up all workstations, because while folks know they're supposed to keep everything on the server they are human and forget sometimes. Additionally there are some things like Word/Pages templates that only exit on the user's computer. While we think a cloud backup is usually sufficient for workstations and laptops, we feel servers should be backed up to a local drive in addition to the cloud. And let's face it, you don't care about backup. What you really care about is the ability to restore the data in the event of a problem. This is why you have to periodically test restoring data.

7 - Create sound policies around technology and communicate to your entire team what's acceptable and what isn't. Integrate it into your culture. Make it part of employee onboarding. Because the last thing you want is to call someone into your office after an issue and they reply "Was that wrong?".

8 - Train your employees. Bad guys know the humans are the weakest link in cyber security. As such, your staff is your front line of cyber defense. You need to educate them on how to make good security choices and keep from getting tricked into giving up valuable information. Security awareness training must be ongoing. Bad guys are constantly evolving their tactics in real time. So talking about security once a year just won't do. What's more, your cyber insurance carrier almost certainly insists on regular cyber training in order to provide coverage.

9 - Multifactor authentication for all the things. MFA adds a layer of security beyond just your username and password. While MFA isn't fool-proof, it's darned good. The idea is that even if the bad guys get your password, they can't get into your account without this extra layer. But like we covered last month, all MFA is not created equal. Whenever possible you want to use a rotating one-time password handled by an authenticator app on your phone.

10 - Have an incident response plan - and practice what-if scenarios. What happens if you get hit with ransomware or other malicious attack? How long will it take your business to become functional? How long to be fully operational? Think of your incident plan as the map that takes you from a cyber incident to recovery.

WHY HACKERS ❤️ MFA FATIGUE

Imagine. . .your organization just went through a huge campaign of encouraging your staff to use multifactor authentication (MFA) whenever possible. CONGRATULATIONS! That's a really huge lift - and one that can greatly help secure your company. After all, just having someone's username and password aren't enough now. But when you planned your MFA implementation, how much did you consider human nature? A while back, we wrote about some of the different options for multifactor authentication and how they are most definitely not created equal. In that article we touched on "MFA Fatigue" but it's been such a successful mechanism for short-circuiting the protections of MFA I feel it deserves to be covered with more depth.

What is "MFA Fatigue"?

One of the more common ways of setting up multifactor authentication utilizes "push" notifications. That is, when logging into your account, you enter your username and password. Then a signal is sent to your phone and a box appears, prompting you to approve or deny the sign-in request. Sometimes, the notification will even show the location where the login attempt is being performed. Unfortunately, getting usernames and passwords is something bad guys have gotten extremely good at. It seems like they have an unlimited arsenal of tricks to try to get people to divulge things they shouldn't. From phishing to social engineering to just buying credentials on the dark web. MFA Fatigue is when bad guys get a username and password and cause what seems like an endless stream of notifications to approve a sign-in request. They're counting on human nature! They're betting that after you've been bombarded with sign-in requests for a while you'll click Approve just to make the notifications stop. This type of social engineering tactic for bypassing MFA has been extremely successful and was used to breach large and well-known organizations such as Microsoft, Cisco, and, most recently, Uber.

How to fight MFA Fatigue?

The first step we suggest for avoiding MFA fatigue is to avoid utilizing MFA based on notifications. We recommend using one-time passcodes - a 6-digit number stored in an authenticator app that rotates every 30 seconds. If you must use notification-based MFA, the newest methods will present a notification on your phone that requires you to enter the number presented on your computer when logging in. This is much more secure than a notification with merely a simple yes/no option. Additionally, as we mention on page 3, you should be getting ongoing cyber security awareness training. Pay attention and take it seriously!

I'm getting bombarded with notifications!
What do I do?!?

The first step is to stay calm and breathe! Seriously. The bad guys are counting on panic and urgency in the hopes you'll make a bad choice. After that, here is a list of Do's and Don'ts. . .

Don't - click to approve any sign-in request you didn't initiate or know about. It sounds simple, right? But in 20+ years of supporting Macs in small businesses, I've found that when a dialog box pops up people's first reaction is to click the first thing that makes it go away. Oftentimes, without even reading it. Read every dialog box that pops up and be intentional about your response.

Don't - engage with unknown people claiming to be from your organization or from your IT provider. You need to be 100% certain the person at the other end is who you think they are.

Do - Immediately(!) contact your IT staff or outsourced IT provider - through your known channels/processes so they can reset the affected password or walk you through doing so yourself. Resetting your password will make the overload of notifications stop.

Do - request your IT staff or IT provider help you to move to one of the more secure - and less intrusive - forms of MFA.

With the right combination of planning and training, you and your staff don't have to be the next victims of MFA Fatigue!