CHARLES HENSON

PRESENTS

FREE REPORT:

THE 5 BIGGEST MISTAKES COMPANIES ARE MAKING WITH THE FTC SAFEGUARDS RULES AND WHAT YOU CAN DO TO AVOID THEM

2022-2023 // PREPARED BY CHARLES HENSON, CEO OF NASHVILLE COMPUTER, AUTHOR, ENREPRENEUR, INVESTOR

ABOUT THE AUTHOR, CHARLES HENSON

Charles Henson is currently serving as President of Nashville Computer and worked there since 1991. He has been in the IT industry for over 30 years. He got his first "computer" around 1984 from a school friend, which made him think that if computers break, someone will need to fix them. This simple idea drove Charles to receive his degree in Electrical Engineering from ITT Technical Institute.

Charles was a featured cast member in the documentary movie CyberCrime available on Amazon Prime. He previously earned the title "Technology Marketing Toolkit 2017 Spokesperson" and "Ambassador To The IT Industry" and awarded a Tesla Model S for his business growth and marketing achievements. He is an international best-selling author of MSSP Playbook and is an international award winning speaker. Leading IT Channel Vendors, such as ID Agent, Huntress, Kaseya, and Rapid Fire Tools, seek him out for their podcasts and webinars and he's been featured on the cover of and featured within ChannelPro Magazine and in Redmond magazine. Having spoken before thousands of fellow business owners and influencers across the US and in Dubai, he was invited to Google Headquarters for his personal feedback on Google products.

Nashville Computer, Inc., established in 1988, is a full service technology solutions provider dedicated to providing fast and professional services to Businesses, Professionals and Non-Profits. We have assembled a highly skilled and experienced team who can provide expert solutions and solve the most difficult IT problems.

I've known Charles for a few years now. He's an absolute inspiration. He has gone out of his way to help me and many other peers. He is the best in the business!

Jennifer Fields
President, ASTEK Marketing Group

The 5 Biggest Mistakes Companies Are Making with the FTC Safeguards Rule and **What You Can Do to Avoid Them**

Your identity has been stolen. They applied for a credit card *in your name*.
They've already gotten a new driver's license and changed your primary address to a P.O. box in a different state.
With just your Social Security Number, they were able to easily get approved for a loan
and two shiny new credit cards within 24 hours of submitting the applications.
Over the course of the next three months, they max out the cards and default on the loans.
You are still blissfully ignorant that there is even a problem.
Until one day, you decide to refinance your mortgage, and to your surprise,
your refinance was denied.
Months later, when you file your taxes, your accountant reports that
someone has falsely filed and received a huge tax return in your name.
Now, creditors are coming out of the woodwork with their hands out, expecting to get paid. They are relentless. Phone calls day and night. Some of them are *threatening legal action*. You have no idea
what to do or how to clear your name. Your credit is so damaged, you can't finance a sandwich.
Oh, and the IRS wants to *audit you* because
of the fraudulent tax return they filed.
Can you imagine? You did everything right.
How could that story have such a bleak ending?
People who you trusted with your information weren't prepared, and when the title company you picked while buying your house *was hacked*, **you suffered the consequences.** It turns out your title company didn't do much to protect your data.
They were focused on the deal going through but weren't really thinking about the security of your personal information.
They didn't even let you know it happened.
You found out well after the event, after the damage was done. By the time you were able to trace the problem back to the title company, your personal information has traveled across every corner of the dark web, and your financial reputation is in shambles.
It will take years, *at the very least,* to get everything back to where you started.
It's an uphill battle, draining your focus and energy.
What happened to you is happening **all too often**. Organizations are cutting corners with people's personal information, and hackers are getting their hands on and abusing this sensitive information.
This is bad for consumers, bad for business, and bad for the economy.

You might be asking, why isn't the government doing something about this? They are, but regulation lags behind technology.

40 years ago: If this were a bank robbery, the robbers would be sent to jail, and you would have your money back. Today, your financial identity is much harder to pin down.

30 years ago: Congress attempted to do something with the Gramm-Leach-Bliley Act (GLBA). However, technology is constantly changing—think about your cell phone 20 years ago—you probably could text and call. Now you could run your entire life—calendar, bank accounts, email, you name it—right on your mobile phone.

The laws simply aren't keeping up and businesses are left in the Wild West, no order and no accountability, so you—the consumer—are the one having to foot the bill.

Is that fair?

Hold onto that feeling of dread when thinking about this happening to you personally. Now multiply it by 100. The weight is suddenly unimaginable. What about 100,000? If you were the source of the leak we discussed above, that many people could easily have been compromised, and many of them would experience that gut churning scenario you imagined above.

Does your perception of events change if you run the company that was hacked?

You didn't mean to share the information, and you certainly didn't believe this could happen to you. BUT, your business didn't address the risk.

This is the problem. When businesses fail to address their risks, they leave their **customers**, their **employees** and the long-term health of their **relationships** at risk.

Would you trust the title company which leaked your data with your next big purchase?

Recommend them a new client?

When sharing the story, would you call them irresponsible with your data? You likely recognize that they were a victim of cybercrime, but as a consumer, in your eyes, they screwed up.

Luckily, The FTC—Federal Trade Commission—put together new guidelines to help address the growing gap in data security. They revamped their security requirements to **include more businesses who directly interface with consumers**.

If you work with money and keep personal information about customers on file, there's a good chance you'll fall within the new FTC Safeguards guidelines.

Imagine your business was targeted with an attack—just like that title company—and word got out that you weren't doing ***the bare minimum***—what these new standards are requiring—to protect your clients' data. These new regulations are daunting and being on the right side of them is exceptionally important. How do you make sure your company is doing what it needs to do?

The 5 biggest mistakes we see when it comes to FTC safeguards are problems with:

- Briefing senior leadership
- Oversight/Implementation
- Training programs
- Incident response plan

- Control validation

Did you know: *Getting a third-party assessment will show you if there are any holes in your security.*
Let's take a closer look at the new rules and the mistakes people are making that could put **your data** at risk.
The FTC Safeguards Rule is designed to protect the information of financial institutions' customers. Noncompliance leads to heavy fines and disruptive oversight.

The big picture:
In 1999, Congress passed a **financial reform act** (the Gramm-Leach-Bliley Act) which was supposed to modernize the financial sector. It was a huge step forward as the last major financial regulation legislation was in **1933** (the Glass-Steagall Act) to address the Great Depression. The GLBA did make some **big improvements**. It defined security protections which were necessary and appropriate for the time as well as codifying disclosure requirements.
The GLBA was a thoughtful and well-intentioned piece of legislation which, because of a combination of clarity issues and rapidly evolving technology, had **no teeth on the enforcement front**. From 1999 to 2021, over a billion sensitive records were leaked, hacked, or stolen. Clearly, something had to give.
Thus, in 2021, the FTC passed and released their new FTC Safeguards rule. One of the biggest **problems** with the GLBA was scope. In the final 2002 version of the legislation, they said:
"This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission ("FTC" or "Commission") has jurisdiction. This part refers to entities such as 'you.'"
The biggest problem here is that GLBA assumed that everyone had the same definition of "financial institution" which was the Achilles heel of the entire act. Instead of arguing whether or not an institution was complying with the law, companies could argue that they didn't fit the definition of a financial institution. This made it really difficult to impose penalties (which made it a lower order priority for companies). Compare that to the 2021 version of the FTCSR:
*"**Scope. This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission ("FTC" or "Commission") has jurisdiction. Namely, this part applies to those "financial institutions" over which the Commission has rulemaking authority pursuant to section 501(b) of the Gramm-Leach-Bliley Act.** An entity is a "financial institution" if its business is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k), which incorporates activities enumerated by the Federal Reserve Board in 12 CFR 225.28 and 225.86. The "financial institutions" subject to the Commission's enforcement authority are those that are not otherwise subject to the enforcement authority of another regulator under section 505 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6805. **More specifically, those entities include, but are not limited to, mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies,**

credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register with the Securities and Exchange Commission, and entities acting as finders. *They are referred to in this part as 'You.'"*
They open with GLBA's language and then expand heavily on exactly what they mean by "financial institution" including classifying significantly more types of business as "covered entities."

So, who is considered a covered entity?

- Mortgage lenders
- "Pay day" lenders
- Finance companies
- Mortgage brokers
- Account servicers
- Check cashers
- Wire transferors
- Some travel agencies
- Real Estate appraisers
- Credit counselors
- Automotive dealerships
- Tax preparation firms
- Non-federally insured credit unions
- Some investment advisors

The unifying thread here is that all these institutions **handle both customer information and finances.**
The expansion of who is a financial institution gives the FTC stronger grounds on which to impose penalties and enforce these new requirements.

Consequences of noncompliance:
Just by being found negligent, the FTC can impose fines from **$10,000 to $100,000 per violation.** That total amount is at the discretion of the individual regulator, so it is difficult to say how high any single fine will be.
In addition, if you're found to be in gross violation of the rule, you can get up to **5 years in prison**. Now, that last one only really applies to things like intentional abuse of protected information, but the FTC is making a clear case that their new teeth are sharp, and they are not afraid to use them.
Importantly, the FTC is going to be reactive rather than proactive. This means that regulators will come to your business and examine every square inch of your security program with a microscope **after you've had an incident.**

Scenario: You've been hit with a ransomware attack
Your backups have been deleted. Your data has been encrypted down to the last bit. You're having to negotiate a ransom in cryptocurrency to get back access to your information. If you don't get that data back, your company is ruined. While this is happening, you have to explain to your stakeholders what happened. You have to keep your staff from panicking. Investors are getting skittish.
On top of all of that, you're answering regulator questions and paying out fines while trying to recover from the event. You'll also lose crucial time that you need to get your services back on their feet.
Estimates vary, but the average data breach costs between from **$3-5 million**, and that doesn't include the much more difficult to calculate losses that come from **reputation damage**. The first thing your insurance adjustor will ask is whether or not you're compliant, and if you're not, any claims could be denied.
Okay, you're sufficiently invested in why these new regulations are important, so how can your company stay on the right side of them?
These regulations are serious*: Want to be sure that you stay on the right side of these regulations, contact us to schedule a Level 1 Assessment.*
These are the exact worst-case-scenarios that a third-party assessment can help prevent.
In the meantime, these five pitfalls are what
we recommend you be on the lookout for.

5 big mistakes (and how to avoid them)

Mistake #1: Senior leadership isn't in the loop

Surely this couldn't happen to your company though. Right? After all, you have a good IT person/staff. But how do you know? Unless your company is in the information technology sector, there's a good chance your senior leadership doesn't know what goes into keeping an IT department running, much less what it takes to stay FTC compliant. That's changing. The new regulations require company leadership to receive r**eports on your security program status** including:

- **Assessments:** This means having a qualified expert find all the holes in your security (and if you don't do regular third-party assessments, there very likely are holes).
- **Improvement recommendations**: You know what is wrong, and that's a great step one. But now you need to know what your company plans to do to address it.
- **Incident reports:** When something goes wrong, senior leadership needs to be briefed on incidents and kept apprised of how they are being addressed.

Back to that ransomware attack: How would you learn that hackers are holding your whole infrastructure hostage? When would you learn that it happened? Hopefully before you're approached by a reporter on your way out of the office. Now, your company is making front page news, and the headlines are not flattering.

What can you do? Take a vested interest in your security:

You're already reading this report, so let's assume we've got buy-in. Great! Now is the time to get to know what your security program looks like. Ask questions. Don't get bowled over by jargon. If it doesn't make sense, keep pressing for more information until it does. This starts in the C-suite and works down through every part of the company.

Remember, if anything goes wrong, it might be *you* giving a press conference and having to answer the tough questions.

Mistake #2: Oversight/implementation of your security program got neglected

Maybe you didn't **designate a qualified individual,** or you assumed **designating someone outside your organization** keeps you off the hook. Either way, as the business owner, **you're responsible** for your organization's compliance.

There isn't much of a definition of a "qualified individual" in the rule. This is a double-edged sword. It's easy enough to make a case that your security person is qualified. By the letter of the rule, your IT person would be okay. However, the FTC giving leeway with who can run your security program does not equate to getting leeway with how well your program functions.

Couldn't the IT department handle it then?

The short answer: They aren't equipped to handle this *in addition* to the litany of other responsibilities they have. On a given day, IT is keeping a hundred plates spinning to keep your hardware and software running smoothly. By definition, they have to function as generalists. Do you think there is time in their schedules to keep up with the ever-changing landscape of security?

Would you bet your reputation on it?

We are focused on security. It's our bread and butter. We're looking for the next big vulnerability before it crashes your systems. Our job isn't to put your employees out of a job. It's to make sure that all their hard work doesn't go up in smoke when a hacker picks your company as their next target.

You cannot proofread your own work

Think about the last time you got on an airplane. The pilot goes through a preflight checklist and

confirms it with the tower. The pilot is double-checking to make sure that everything that was done by other people is done correctly. Very likely, you get some comfort knowing that someone is maintaining the plane, fixing problems, and looking for flaws. It's even more comforting that an objective third party is double checking that work. The same holds true for security. Your people know what they're doing, but they also know what *should be there* when examining your system. That leads to inattentional blindness, the kind that an extra pair of eyes will catch.

Mistake #3: Your training program is nonexistent or insufficient

The FTC REQUIRES you to implement a training program. It **must** teach your employees the latest tricks that hackers are using to get in. You could build a program from scratch and update it with each new development in the security space (see Mistake #2 and ask if that's the right way to go). On top of that, you have to ensure your employees understand the material (*and document it)*.

How can you handle this?

Get your training materials from subject matter experts. In the same way a specialist can help build your security program, a specialist can educate how to keep your data safe. Around 70% of all data leaks (though some sources put it as high as 90%) come from social engineering. That puts you in a place where every single person in your company has to be the first line of defense against hackers.

Not everyone has access to sensitive data

That's true, but if one employee is hacked, there's a wedge in the door. Suddenly, phishing attempts are coming from that unwitting employee, and the hackers can use this as a beachhead to get more information. Essentially, you're only as strong as your weakest link, and you cannot afford for it to be your security training program.

Mistake #4: You haven't set up your incident response plan

Back to your hypothetical ransomware problem: Can you imagine answering tough questions about how an incident occurs without so much as a briefing to prepare yourself? When an event occurs, you want to project strength. You know exactly how it happened and are already taking steps to mitigate it. You **can't** "just figure it out" after you've been hacked. Remember, all of the disaster of a breach (the bad press, the FTC investigation, dealing with hackers, reputation recovery) is happening at the same time. It's already a three-ring circus. Don't let it be your lion tamer's first day on the job.

Yes, it can happen to you

Hackers are largely opportunists. They attack systems that are easy targets. If your plan is being created on the fly, they are going to extract more value from information that they steal. Think about how we secure a car. Yes, there's the door locks. That's your security program. There's also the alarm though. A big flashy noise that shortens the amount of time the thief has to make off with your car. A good incident response plan puts you in a position to respond *quickly* to an event. It limits how far they'll get in your systems, how much data they can steal, and how much money they can make off that data.

The FTC requires you to document your plan

We're way past scout's honor on having an incident response plan. When they are investigating you, the FTC wants to be sure that you did everything you could to protect that data. They want to be sure you're doing everything you can from the moment something goes wrong. If you aren't...it gets costly very quickly.

Mistake #5: You don't have a method for validating controls

Would you buy a safe that the manufacturer is "pretty sure" it'll work? Of course not. You want the safe that stumped professional safe crackers. That's because if you are bothering to buy a safe, you want its contents to remain secure. Now imagine that instead of being in your office, cleverly hidden behind

a painting, the safe is in the middle of Times Square. Suddenly, that safe needs to be foolproof. Anything less than that, and it's a deterrent, not a defense.

That's your data

Everything that we do: Encryption, password protection, biometrics, multi-factor authentication; it's all security features for the digital equivalent of a safe in Times Square. That's why validating your controls is important. If you don't, you'll find out there's a problem on Monday when the safe door is blown off and you have to walk through police tape to get in the front door.

You have to test your controls

This isn't just a smart thing to do. It's **legally required** under the FTC safeguards rule. Now, you could try to verify in-house (see Mistake #2 for why you shouldn't). However, you've seen how complicated all of this is. You know that there are a multitude of sensitive, moving pieces at play to make sure your security plan is up to snuff.

Put another way:

You're (hopefully) starting to see the value in third party **penetration testing** and **vulnerability analysis**. There isn't room for this increasingly common problem to happen to you. We can help get you from where you are to where you need to be.

What can we do to help?

You're legally obligated to have a risk mitigation strategy. Shouldn't you go into it with open eyes?

I want to offer you a Level 1 Risk Assessment.

This isn't a tool that you're left to figure out. Our goal is to help you understand your risks and what to do to address them.

This is a $3,000 value that I'm offering to you free of charge if you begin this process with us in the next 30 days.

You're at the center of this process:

We'll have a 45-minute call to discuss threats and risk. This is just the beginning of the process. We get to know you, and don't worry; our non-disclosure agreement means that your information remains confidential.

After that, we'll analyze your current processes to see where you stand with respect to the FTC requirement. After that, you and I can work together to build a roadmap to get you up to the new rule's requirements.

We won't be giving you the hard sell because this process is meant to take time. We want to help you do it right. That means the more time we have to work with you before the FTC Safeguards implementation deadline, the better (You wouldn't start your taxes in mid-April, would you?).

IS YOUR CURRENT IT COMPANY DOING THEIR JOB?

TAKE THIS QUIZ TO FIND OUT

If your current IT company does not score a "Yes" on every point, they are NOT adequately protecting you. Don't let them "convince" you otherwise and DO NOT give them a free pass on any one of these critical points. Remember, it's YOUR business, income and reputation on the line.

That's why it's important to get verification on the items listed. Simply asking, "Do you have insurance to cover our company if you make a mistake?" is good but getting a copy of the policy or other verification is critical. When push comes to shove, they can deny everything.

☐ **Have they met with you recently – in the last three months – to specifically review and discuss what they are doing NOW to protect you?**

Have they told you about new and inexpensive tools such as two-factor authentication or advanced endpoint security to protect you from attacks that antivirus is unable to detect and prevent? If you are outsourcing your IT support, they should, at a MINIMUM, provide you with a quarterly review and report of what they've done – and are doing – to protect you AND to discuss new threats and areas you will need to address.

☐ **Do they proactively monitor, patch and update your computer network's critical security settings daily? Weekly? At all? Are they reviewing your firewall's event logs for suspicious activity?**

How do you know for sure? Are they providing ANY kind of verification to you or your team?

Have they ever asked to see your cyber liability insurance policy?

Have they verified they are doing everything your policy REQUIRES to avoid having a claim denied in the event of a cyber-attack? Insurance companies don't make money paying claims; if you are breached, there will be an investigation to prove you weren't negligent and that you were actually doing the things you've outlined in your policy.

Do THEY have adequate insurance to cover YOU if they make a mistake and your business is compromised?

Do you have a copy of THEIR CURRENT policy? Does it specifically cover YOU for losses and damages? Does it name you as a client?

Have you been fully and frankly briefed on what to do IF you get compromised?

Have they provided you with a response plan? If not, WHY?

Have they told you if they are outsourcing your support to a third-party organization? DO YOU KNOW WHO HAS ACCESS TO YOUR BUSINESS AND THE DATA IT HOLDS?

If they are outsourcing, have they shown you what security controls they have in place to ensure that a rogue technician, living in another country, would be prevented from using their free and full access to your network to do harm?

Have they provided you evidence that they have a third-party that audits their network?

Did you know that if their network gets hacked, the hackers will have access to your network too? If you haven't seen evidence of their third-party audits, request it immediately.

Have they kept their technicians trained on new cybersecurity threats and technologies, rather than just winging it?

If they don't have a way to show you that their team is learning about threats hitting your industry and to validate that their team is up-to-date on current security protocols, how can they guarantee providing you with secure solutions?

Do they have a ransomware-proof backup system in place?

One of the reasons the WannaCry virus was so devastating was because it was designed to find, corrupt and lock BACKUP files as well. ASK THEM TO VERIFY THIS. You might *think* you have it because that's what your IT vendor is telling you.

Do they have controls in place to force your employees to use strong passwords?

Do they require a PASSWORD management system to prevent employees from using weak passwords? If an employee is fired or quits, do they have a process in place to make sure ALL passwords are changed? Can you see it?

Have they talked to you about replacing your old antivirus with advanced endpoint security?

Anti-virus tools from two or three years ago are useless against today's threats. If that's what they have protecting you, it's urgent you get it resolved ASAP.

Have they implemented "multifactor authentication," also called 2FA or "two-factor authentication," for access to highly sensitive data?

Do you even know what that is? If not, you don't have it.

Have they implemented web-filtering technology to prevent your employees from going to infected websites, or websites you DON'T want them accessing at work?

I know no one in YOUR office would do this, but why risk it? Adult content is still the #1 thing searched for online. Then there's gambling, shopping, social media and a host of other sites that are portals for hackers. Allowing your employees to use unprotected devices (phones, laptops, tablets) to access these sites is not only a security risk but a distraction where they are wasting time on YOUR payroll, with YOUR company-owned equipment.

Have they given you and your employees ANY kind of cybersecurity awareness training?

This is now required for insurance providers to cover breaches. Employees accidentally clicking on a phishing e-mail or downloading an infected file or malicious application is still the #1 way cybercriminals hack into systems. Training your employees FREQUENTLY is one of the most important protections you can put in place. Seriously.

Have they properly configured your e-mail system to prevent the sending/receiving of confidential or sensitive data?

Properly configured e-mail systems can automatically prevent e-mails containing specified data, like social security numbers, credit cards, and other sensitive data from being sent or received.

Have they had a third-party analyze your network to validate their work?

You would never attempt to proofread your own work. Why would you expect your IT person to? Many regulatory bodies require at a minimum an annual third-party assessment for this reason.

SECURITY IS NOT COMPLIANCE – AND BEING COMPLIANT IS NOT A GUARANTEE THAT YOUR DATA IS SECURE!

MAKE SURE YOUR IT COMPANY IS TAKING THESE 3 STEPS

As previously discussed in this report, a mistake many organizations make is thinking that because they're compliant, they are automatically secure. Sorry. Not so. You can be compliant and completely insecure, but there are three key steps to ensure you are actually secure.

Most IT companies are only doing one or two of the three. You want to make sure they are checking ALL the boxes so if and/or when a breach occurs and you get audited, you are brilliantly prepared, and the damages are minimized. Here they are in order:

1. A regular third-party security assessment with a remediation plan.

Hackers are constantly coming up with new ways in. Security tools that worked just two years ago are no longer are sufficient today. If they aren't having a third-party security assessment performed at least every quarter like clockwork, they are missing gaping holes that are actively being exploited by hackers. Problem is, this is where most businesses stop and don't go on to steps 2 and 3 below.

2. Full and true IMPLEMENTATION of their plan.

Best-laid plans are worthless if not implemented. You can give a patient a treatment plan – but if they refuse to follow it, or skip steps and cherry-pick your advice, they cannot expect to get well.

Same goes for security – your IT consultant should be giving you options, timelines and a weighing of pros and cons for choices you make about how to implement a plan to become compliant based on your risk tolerance, situation, budgets, resources, etc. A good IT company or consultant will guide you through this.

But the most important aspect is to make absolutely certain that the IT team or company you put in charge to implement the remediation plan is actually doing it. Based on our personal experience, 90% of the companies selling outsourced IT services and support are NOT being diligent about the full and complete implementation of a security and compliance plan.

In a world of marketing promises, how do you know your IT and security partner is delivering as promised? Please see the previous section of this report to know if they are truly implementing the plan. Further, we are offering a free, independent Security Assessment to audit your current IT company and tell you the truth about what they are (or aren't) doing for you.

3. Documentation.

This is the part most IT companies and medical practices skip. Behind every security compliance measure is a documentation requirement.

If you have a breach and subsequently get audited, you will be required to produce documentation of your security activities and policies. If you do not have those documents, your business will not be able to sustain a major attack or breach. If you do not have documented plans for how to address a ransomware attack, data breach, or disclosure and clear instructions on who needs to do what when, you are putting yourself and your business at risk of not surviving the consequences.

WILL YOU WAIT UNTIL YOU ACTUALLY HAVE A BREACH OR REPORT FILED AGAINST YOU BEFORE DOING SOMETHING ABOUT IT?

Over half of all home security systems and cameras are bought (or beefed up) by homeowners after a burglary or home invasion.

Across the country, warnings of bad storms drive hordes of people to the store to stock up on water, food and other supplies – and anyone who hesitates or waits to hit the store AFTER work or WHEN they have the time often arrives to find the store shelves empty, and the remaining picked-over supplies at jacked-up prices.

We are strongly cautioning against any assumption that you are truly protected and prepared should a breach occur, or should you get reported for a violation.

Fire prevention is infinitely cheaper, less stressful and more orderly than having to call the fire trucks and work the hose when your house is ablaze. Cancer is BEST treated when found EARLY and aggressively treated, not left to get worse until the point of no return.

The time to have an in-depth, fresh look at the state of your security program is right now, with a friend who has your best interests in mind – NOT an insurance agent or an attorney – when there is no crisis happening, no auditors calling, no security breach occurring.

OUR FREE PREEMPTIVE IT SECURITY ANALYSIS WILL REVEAL IF YOUR CURRENT IT COMPANY IS

DOING WHAT THEY SHOULD

Over the next couple of months, we will be conducting free Security Assessments to find and expose vulnerabilities and failings in your security BEFORE a cyber event happens.

Fresh eyes see things – so the biggest value of our Assessment is getting us to sit on YOUR side of the table and give you straight answers to whether or not your IT company or person is actually doing what they should to minimize your chances of experiencing a breach and minimize the losses that can occur. You get a "Sherlock Holmes" investigating on your behalf.

Here's How It Works:

We will conduct a thorough, CONFIDENTIAL investigation of your IT network, backups and security protocols through the lens of not only an IT company, but also from the perspective of a hacker and an insurance provider. Your time investment is minimal: one half hour for the initial meeting and one hour in the second meeting to go over our Report Of Findings.

When this Assessment is complete, here are just a few of the most frequently discovered problems we are likely to uncover and the answers we'll be able to provide you:

- ☑ Is your current IT company or team actually implementing critical security protections, protocols and systems that would not only minimize the chances of a breach, but also ensure your insurance claims would not be denied due to not following through on something YOU agreed to do on your insurance policy's declarations contingent for coverage?

- ☑ What are the least expensive, most impactful things you can do to secure your network and avoid getting slapped with "Willful Neglect" should a breach happen?

- ☑ Is your security configured well enough that you can pass a simple cybersecurity analysis called a penetration test? We'll issue one and be able to demonstrate, in a matter of hours, if your IT company is doing their job or completely failing you.

All of these are tiny "ticking bombs" in your security, waiting to go off at precisely the wrong time. We urge you to go to the URL below and book your free assessment now:

BOOK YOUR ASSESSMENT TODAY

WHEN OTHERS AUDIT – INSURANCE COMPANIES, GOVERNMENT REGULATORS – THERE IS NO KINDNESS

Government auditors and insurance providers won't give you the benefit of the doubt. They know what to look for and where the failings typically occur. They are experienced in finding lax protocols and know what stones to turn over.

When such audits reveal problems, there is serious stress and strain placed on your staff and on you personally. Tensions rise, fingers get pointed and resentment can build.

Your own preventive, independently conducted, completely confidential compliance assessment is the ONLY practical way to prevent embarrassment or worse consequences. It's also the smart way to unearth problems you can fix now.

Candidly, no one should proofread their own work - so if you do have an IT company you are paying, this will give you a free, no-risk way to tell for sure if they are doing the job you're paying them to do.

PLEASE…DO NOT JUST SHRUG THIS OFF

WHAT TO DO NOW

If you have scheduled an appointment, you don't have to do anything but be sure to show up, ready with any questions you might have.

If you prefer to talk to us first, call us at 615-615-1511 or send an e-mail to Patrick Maley Patrick.Maley@NashvilleComputer.com

I know you are extremely busy and there is enormous temptation to discard this, shrug it off, worry about it "later" or dismiss it altogether. That is, undoubtedly, the easy choice…but the easy choice is rarely the RIGHT choice.

This I can guarantee: At some point, you will have to deal with a cyber security "event," be it an employee mistake, malware infestation or even a ransomware attack.

We want to make sure you are brilliantly prepared for it and experience only a minor inconvenience at most. But if you wait and do nothing and ignore our advice, I can practically guarantee this will be a far more costly, disruptive and devastating disaster.

You've spent a lifetime working hard to get where you are today. Let us help you protect and preserve it.

Dedicated to serving you,

Web: nashvillecomputer.com
E-mail: Charles.Henson@NashvilleComputer.com
Direct: 615-645-1511

WHY NASHVILLE COMPUTER IS UNIQUELY QUALIFIED TO ADVISE YOU IN THIS MATTER

IT security has brought high-fee “experts” out of the woodwork who are, quite honestly, woefully inexperienced and uninformed. Software and IT companies, medical practice consultants and even insurance agencies see this as their golden opportunity, rushing to present themselves as saviors.

But how do you know someone actually has the depth of experience to handle this hyper critical part of your practice? For 34 years my organization has excelled at cybersecurity for Medium to Large Businesses. Here are just a few of the things that make us uniquely qualified to handle your IT security needs:

An Entire Team of Experts at Your Service

Our technology specialists are certified and have both the IT expertise and business insight to align your technology with your business goals

Customized IT Solutions

We take a good look at your business before devising strategic and scalable solutions that match your specific needs

Top-Tier Products at SMB Price

We use our business partnerships with global vendors to offer high-quality products at discounted prices as you can enjoy maximum value for money.

We Are Dependable and We Stand Behind our Services

We have been in business since 1988 for a reason, if you aren’t happy with our services, we’ll go out of our way to make it right.

DON'T TAKE IT FROM US

HERE'S WHAT OUR CLIENTS SAY

"I RELY ON THEM FOR EVERYTHING"

"We have been with Nashville Computer for over 15 years. They are quick to respond and provide excellent customer service. They always help me with what I need and then ask if there is anything else. They bring IT and computer issues to my attention that I hadn't thought about. That is wonderful because I function as the firm's IT person, but I rely on them for everything."

Dawn Fritton, Office Manager FMC CPA

"THEIR UNIT COST APPROACH IS REFRESHING"

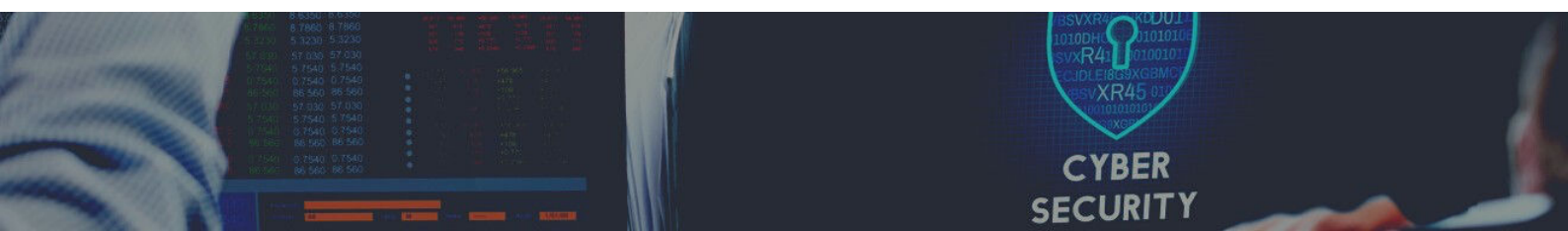
"Our experience with Nashville Computer has been positive in every way. They bring knowledge and experience to the table coupled with helpfulness, responsiveness and commitment. Their unit cost approach is also refreshing in that it is completely predictable and consistent. There are no hidden charges. Our hearty recommendation of Nashville Computer is unqualified and resounding."

Tom Anderson, American Geothermal, Inc.

"QUICK RESPONSE TIME"

"Nashville Computer provides a quick response to your IT needs and questions. Nashville Computer Technician's give you detailed notes, and their explanations are always easy to understand. We appreciate Nashville Computer's quick response, efficiency, and attention to detail."

Tonya Sweeney, Wright & Company, Inc.



WHAT TO DO NEXT?

NEXT STEPS

TIME TO GET INTO ACTION!

☐ BOOK A CALL WITH CHARLES HENSON AND HIS TEAM AT NASHVILLE COMPUTER FOR A CYBER SECURITY ANALYSIS.
GO TO WWW.NashvilleComputer.com
OR TEXT/CALL (615) 645-1511

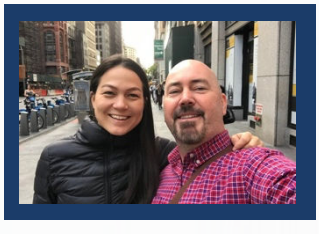
☐ FOLLOW CHARLES HENSON ONLINE FOR DAILY UPDATES ON KEEPING YOUR BUSINESS SECURE:

WORKING WITH THE BEST

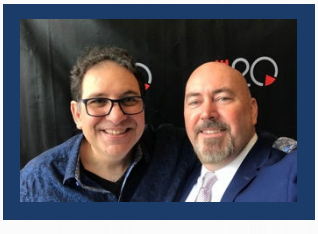
IS YOUR FIRST LINE OF DEFENSE!











FREE REPORT:

THE 5 BIGGEST MISTAKES COMPNIES ARE MAKING WITH THE FTC SAFEGUARDS RULE AND WHAT YOU CAN DO TO AVOID THEM

2022-2023 // PREPARED BY CHARLES HENSON, CEO OF NASHVILLE COMPUTER, INTERNATIONAL BEST-SELLING AUTHOR, ENTREPRENEUR, AND INVESTOR