NETWORK PROVIDERS, INC.
FEBRUARY 2023

Cybersecurity TECHNOLOGY

NEWSLETTER

How The New FTC Safeguards Rule Will Radically Change How Even Small Businesses Operate

BY JAY HILL
President & CEO

I wanted to focus this month on our Technology Business Reviews (TBRs). You probably have seen an invitation from our company in your email, asking you to accept an invitation and select a time/date to have one of these meetings with me or with Christoffer Adams, our Business Technology Strategist. If you have not accepted an invite, please do!

TBRs are so valuable. They happen quarterly, and are designed to meet with your IT representative to discuss how you feel about your IT. We want to hear concerns. We want to answer questions. We want to give you ideas to make your processes even more efficient and secure. We hope when you schedule a TBR that you will come with feedback from employees about their experience with the technology they are using, and about their experience with NPI. We want to make sure you are happy and your concerns are resolved. These meetings are an excellent opportunity for you to share honest input. It is also a time for us to share things we see that need to happen on your system to keep it updated and secure. We want to be proactive not reactive when it comes to your technology.

I hope you will sign up for a TBR the next time you get an invitation. We look forward to talking to you in person.

A little over a year ago, the FTC made several amendments to the existing Safeguards Rule requiring even very small businesses to ensure the protection of client data. These changes, set to go into effect back in December of 2022, are now going to be enforced starting June 9, 2023 – and it's very likely that your business, regardless of how small or how your tech is being handled, WILL be required to implement certain new security protocols.

The Safeguards Rule was originally created for financial institutions. However, the new amendments broaden the definition of financial institutions to include real estate appraisers, car dealerships and payday lenders. The FTC goes so far as to include any business that regularly wires money to and from consumers. These organizations are required to develop, implement and maintain a comprehensive security program to keep their customers' information safe.

Here are the provisions you must implement:

Designate A Qualified Individual To Oversee The Information Security Program

That means someone at these companies need to be trained in information security, receive continuing security education and be in charge of ensuring the organization is correctly executing the written information plan. If no one on your team meets this requirement, we can provide someone.

Develop A Written Risk Assessment

A risk assessment is done in two parts: one, a technical scan, and two, a questionnaire designed to reveal common security loopholes. This is typically outsourced to an IT firm like ours and needs to be reviewed annually (by law), but best practices should be quarterly if not monthly in situations where a business is handling a lot of sensitive information and the tolerance for risk by the owner is low. If you need this risk assessment, contact us.

Limit And Monitor Who Can Access Sensitive Customer Information

For example, don't give your entire team access to your credit card processing system. Only allow one employee (the one who works in it day in and day out), as well as one backup person (possibly you, the owner), to be able to log in and access this information.

Encrypt All Sensitive Information

Again, this is typically done by an outsourced IT company like ours, unless your company is large enough to have a robust cyber security team that can handle it. "Sensitive information" is not just medical records and credit cards, but clients' e-mail addresses, phone numbers, Social Security information, driver's license information and birthdays.

Continued from pg. 1

All of this can be used by hackers to exploit your customers using the data you host.

Train Your Employees

Employee cybersecurity awareness training is another key component to not only this law, but also to get and keep insurance coverage on cyber liability, crime and other insurance policies.

Develop A Written Incident Response Plan (WIRP)

Specifically, if (when?) you get compromised, you need to have a plan in place for how you will respond. This is also another service we offer to our clients but should be reviewed by your insurance agent, leadership team, board and other key players in the organization.

Periodically Assess The Security Practices Of Service Providers

This law also requires you to ensure any companies you are doing business with – specifically ones where sensitive information is shared – to be secure and compliant. This may include requiring that vendors state in their contracts that they are adhering to the Safeguards Rule and to certain security frameworks, like CIS or NIST.

Implement Multi-Factor Authentication (2FA)

Also known as "2FA," this process ensures anyone logging in to your accounts must authenticate that request via another device, such as a cell phone or e-mail.

If you want to discuss this new rule with us and how to get started with a Risk Assessment, call us at Ext. 116. We help several of our customers plan their WIRP.

New FTC Safeguards Rule will go into effect and be enforced starting June 9, 2023. Are you ready for these changes?

Data Has Been Cracked Yet Again By Hackers

A Message from our Business Technology Strategist ~ Christoffer Adams

Did you read the recent news about the widespread Comcast Xfinity email account compromise, as well as the other websites that saw intrusions as a result. A number of Comcast customers logged into their Xfinity email accounts only to discover that they had been hacked. The source of these widespread attacks seems to be an exploit that allows an attacker to bypass Xfinity two-factor authentication (2FA) for Xfinity accounts. Hackers appear to be using a privately circulated tool that bypasses the one-time-passcode (OTP) used in 2FA. Essentially, your account will not send the 2FA code to you. Instead, the hackers will get it, cutting you out of the loop.

First, the attackers compromise an Xfinity email account by using stolen passwords from the Dark Web. From there, they login with the stolen passwords and use the private 2FA bypass tool to get around phone verification. After that, the password is reset, and any backup or secondary emails are changed to one the attacker controls. Once they have access to the Xfinity email, hackers can use this email to attempt to password reset other services with the 'Forgot my Password' feature. They've been observed using this method to compromise DropBox, EverNote and even cryptocurrency exchange accounts such as Coinbase and Gemini.

A Few Important Things To Note In These Attacks

- 2FA was not enough. The hackers bypassed it.
- Those who regained access to their accounts did so because they noticed a change in 2FA by monitoring their email accounts.
- The accounts were originally compromised via "credential stuffing" which uses Leaked Passwords found on the Dark Web.

If you have a Comcast email account, we recommend that you immediately update your password and check the recovery email and 2FA information you have on file. Reach out to Comcast Xfinity support if necessary. It is also a good idea to review your other accounts and services for compromise. These are all common pain points for which our 3rd party security assessments identify. Not only do we provide consultation and training, but we utilize alerts to catch compromised accounts as soon as it happens. Our services also scan your environment for accounts using leaked passwords that have been found on the Dark Web.

FREE Report Download:

3 Surefire Signs Your IT Company is Failing To Protect You From Ransomware

NEW And Critical Changes to Cyber Security, Insurance Coverage And Threats That Will Put Your Business At Serious Risk If Not Addressed Immediately.

Discover what the vast majority of businesses don't know and haven't been told about changes to cyber security risks, insurance requirements and threats that are allowing them to operate at UNDERAPPRECIATED RISK for a crippling cyberattack and subsequent costs, lawsuits and fines – and what to do about it now.

We would like to give you a copy of our recently published report.

Claim your FREE copy today at www.networkprovidersinc.com/riskassessment/

Do I Need To Upgrade My Network?

4 Amazing Benefits You'll Experience

A business owner has many responsibilities within their business. They can be so busy that sometimes things are overlooked for an extended period of time. For example, many business owners may forget to upgrade their network infrastructure. In actuality, upgrading your network is extremely important – and it is one of the smartest things you can do as a business owner.

Technology has rapidly advanced over the past few years, and network traffic continues to grow. If you're still using the same network from even five years ago, you've probably noticed your network speed has decreased dramatically. In fact, old networks struggle to keep up with all of the advancements and traffic growth. They can even open your business up to a cyber-attack.

Your network infrastructure should be upgraded every few years for many reasons. If your business has grown consistently over the last few years and your current network can't keep up with your business needs, it may be time to upgrade. If you're continually running into issues with your current network, an upgrade will help. Some industries may even be legally obligated to upgrade their network in order to keep their customer or client information secure.

> Upgrading your network is the best way to keep up with the ever-changing landscape of the digital world.

Upgrading your network comes with an abundance of benefits. Here are four of the best for any business.

Better Network Security

Cybercriminals are much more cunning than we often give them credit for. They continue to develop new cyberthreats and ways to attack various networks. If you haven't upgraded in some time, you are opening your business up to a cyberbreach. New networks come with a plethora of added security benefits that aren't possible with the old and outdated ones. You want to make it as difficult as possible for a cybercriminal to hack into your system and steal valuable information – and one of the best ways to stop a cybercriminal in their tracks is by upgrading your network. One cyberbreach can be incredibly detrimental to your business, so don't take that risk.

Faster Internet Speeds

Think about how much more productive your business would be if you had faster Internet speeds. Your employees can get more done without having to deal with lag from poor Internet services. Older networks can't keep up with the demands of modern technology. With an older network, you will see slower Internet speeds that won't allow your employees to utilize cloud storage systems and business applications at high speeds. Even your customers will notice improvements in the speed of your network if you use client-facing applications in your business. Everyone wins when you have faster Internet speeds.

New And Better Hardware

One of the best parts of upgrading your network is that you'll receive new, more reliable hardware than what you've had in the past. You'll gain access to more computing power and larger storage space. More than anything else, your new hardware will be dependable, and you won't have to worry about it failing on you.

Improved Compatibility

Remember how we said earlier that technology has advanced rapidly? It's true – and there are new advancements made every day. Without an upgraded and updated network, you may be unable to use many applications and technologies that could improve your business. An upgraded network will allow you to connect with any apps you think will benefit your business. You can explore new tools without worrying about crashing your network. You'll also gain more freedom in choosing your new tech investments as you would be more limited when using outdated technology.

Upgrading your network is the best way to keep up with the ever-changing landscape of the digital world. If you haven't upgraded your network in a while, now is the best time to do so. Plenty of benefits come with it, so don't wait until you have to make a change. Be proactive!

How Technology Reaching End of Life (EoL)/End of Service (EoS) Can Impact Your Business

When your organization's software reaches End of Life (EoL) or End of Support (EoS), it will no longer receive critical updates and patches even though it may still function. This can have dangerous repercussions for your business. To save money, some business owners may resist upgrading to next-gen hardware and software. However, the results are pricey in more ways than one. Utilizing software after its "best by" date puts your business at risk for security breaches. The bottom line is that employing EoL/EoS technology puts the security, performance, compliance, and compatibility of your IT infrastructure in danger.

Partnering with an IT service provider is the simplest way to ensure all your hardware and software are regularly maintained and upgraded. Keeping your technology up to date is simple once you have a trusted advisor like Network Providers, Inc. in your corner.

Contact Byron Sherwood, our technology hardware and software expert and he can run a free report on your expired hardware and/or software.

For More Details Call

Byron Sherwood Ext. 107

Major Cyber-Attacks of 2022

If you're a small-business owner, it's essential that you're aware of the IT news, trends and events that took place in the recent past. In fact, knowing what happened in the previous year can allow you to develop plans for the future so 2023 will be successful for you, and your business. You shouldn't continue following old trends because the competition will quickly leave you behind, and that could open you up to cyber-attacks you didn't know existed.

Cyber-attacks happen all the time. As new cyberthreats emerge, we'll see more frequent and severe cyber-attacks over the next few years. Uber saw another cyber-attack this past September that caused the company to shut down its internal messaging service and engineering systems in order to get to the bottom of the incident. Cryptocurrency storage and blockchain were also high-value targets for cybercriminals. Ronin and Crypto.com suffered severe cyber-attacks that required both companies to reimburse their users for the cryptocurrency stolen in the attack. Ronin was hacked for $540 million, and Crypto.com was hacked for $33 million worth of cryptocurrencies.

Small businesses weren't safe from cyber-attacks either. While cyber-attacks on big businesses make national news, small businesses are targeted more often since their cyber security defenses aren't as strong.

That being said, it's imperative you ensure your business has efficient cyber security practices in place, so you won't have to worry as much about cyber-attacks.

The IT industry is consistently changing to keep up with new developments and advancements. If you're a small-business owner, it's vital to keep up with the latest news and information so you can best protect your business and its data. When you stay ahead of the trends, it's much easier to prevent potential cyber-attacks and threats.

Start fighting cyber crime with KNOWLEDGE & ACTION! Sign Up to Receive Our FREE "Cyber Security Tip of the Week" at https://www.networkprovidersinc.com/drip-tips/.

Employee Spotlight:

Neal Hills - Tech of The Quarter

At Network Providers, Inc. we recognize employees who show us their best work performance for each quarter. Neal Hills is one of our most talented Help Desk Support Technicians at NPI.

Here is what one of our customers had to say about Neal, "I'll say that Neal gets it. On both occasions he knew exactly what to do, as well as accommodating a couple of requests. Neal communicates excellently and all was taken care of expeditiously. I was able to continue working while he was remoted in, lending an assist when needed." ~Barry Singer, VP of Sales, Utah Scientific

Let's congratulate Neal for his hard work in keeping our NPI customers happy!