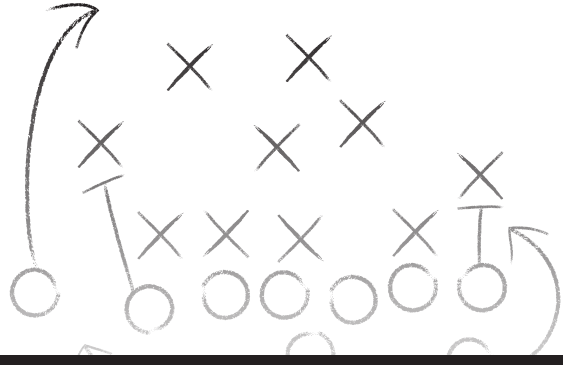
# THE CYBER PLAYBOOK

A No-Nonsense Guide To Cybersecurity And Compliance For Business Owners

ZACHARY HAMBLEN

Featuring Cybersecurity Experts From Around The World

# THE CYBER PLAYBOOK



**A No-Nonsense Guide To Cybersecurity And Compliance For Business Owners**

**Featuring Cybersecurity Experts From Around The World**

BigRedMedia
a TMT company

Nashville, Tennessee

## Chapter 16:
# Securing Your Future: The Cyber Insurance Checklist Simplified

*Zachary Hamblen*
*Owner & Manager, Your IT Guys*

It's another typical Monday morning. You arrive early, hoping to catch up on some paperwork and jump-start the coming week. With a fresh cup of coffee in hand, you sit down at your desk to log into your system. Suddenly, a menacing pop-up message issues this demand: *"Send me $50,000 via Bitcoin NOW, or else all your data will be destroyed!"*

Think it can't happen to you? It most certainly can, and the danger's only increasing. Cyberthreats from bad actors have skyrocketed in recent years. No matter how carefully you think you've safeguarded your systems, it's almost a sure bet that you still haven't done enough.

The ransomware scenario described above is terrifying but sadly all too common.

However, dealing with the negative consequences of data loss is only the beginning. The costs to your business go way beyond simply paying the ransom – the resulting costs of recovering data, lost productivity, and damage to your reputation can be devastating. Multiple sources,

including the National Cybersecurity Alliance, warn that approximately 60% of small and midsize businesses that get hacked go out of business within six months.

That's why so many businesses today seek protection through cyber insurance.

## The Importance (And Challenge) Of Cyber Insurance

Think of cyber insurance as a shield against enemy assaults. If you've been attacked, it protects you against long-term damages to your business. That's why having a solid policy in place is no longer "nice to have" – it's mandatory. The challenge for businesses, however, lies in navigating the complex and obscure terminology of the cyber insurance application.

Dentists, for example, are experts in oral health, not IT technology and cybersecurity. If you fill out a cyber liability insurance questionnaire incorrectly, you're liable for whatever you put down as answers. Misunderstanding a term or concept and taking a guess can lead to significant issues if a claim arises. For example, let's say you experience a data breach and have to file an insurance claim. The insurance company sends an incident response team out to the office, and, as part of their investigation, they examine all the computers on your network, including those not even involved in the breach.

Suppose they find that the operating system of one of those computers is an outdated version of Windows. Even if this was on an old machine that's rarely used, upon discovering this, the insurance company could deny your claim and immediately stop working on remedying your issue. It doesn't matter that the one computer with the

outdated operating system had nothing to do with the breach; it could still result in denying a claim. You're out of luck, even though you've paid for that coverage and thought you were protected.

Several years ago, cyber insurance companies denied, on average, approximately 60% of all claims submitted. But last year, they only rejected 7%. While that might sound reassuring, it's actually due to the fact that these companies are becoming more selective, and they're dropping potential high-risk clients before they even get a chance to file a claim.

## Your Path Through This Wilderness

The key is to follow a "Cyber Insurance Checklist," ensuring you're protected against cyberthreats and have insurance when something bad happens.

This is a list of what you should do to keep your systems and network secure based on the compliance framework your business operates under: NIST, PCI, HIPAA, etc. It should outline the specific protections you need to implement to secure your business.

At a minimum, your checklist should cover three key areas:

- **Protection:** Are you using strong passwords? Have you implemented Multi-Factor Authentication (MFA)? Are your antivirus and other defenses up to date? Are you making sure your firewall protects against data loss? These are simple things from an IT perspective, but many offices don't realize they're necessary.
- **Training:** Arm your team with the knowledge to detect and deflect cyberthreats. It can be as simple as reminding users to always keep

security in mind. For example, understanding how email protection practices should affect the way you work. If you get an email that looks suspicious, don't click on it. Just delete it. Don't worry about missing out on something mission-critical; if it truly is important, someone will email you again or call and let you know.

- **Data Security:** You must guard your data through encryption and robust backup protocols. Your workstations and your server need to have their data securely protected. Implement "immutable backups" that provide backup continuity and can't be accidentally deleted. This means you have systems in place to ensure that if something happens, your business can get back to work in minutes, not hours or days.

However, following your checklist's guidelines isn't enough to prove to the insurance company that you've properly safeguarded your business.

## You Must Keep A Detailed Record Of Everything You've Done

It's more than just following a checklist: you need to document every step you've taken, every policy you've implemented, and every training session you've conducted.

Just as you keep legal documents in case you ever have to reference them, you'll need to keep records of the steps you've taken to ensure cybersecurity within your business and always have them readily available. For example, when you conduct in-house security training, require everyone to register and keep a record of their participation—track who got the questions right and wrong in any questionnaires during the events. If you send a test phishing email, you must know if

it was viewed. Also, whether your team members clicked on it, visited the test website, or maybe clicked something on the website. Most importantly, did they try to sign into the phishing test site?

You need to know who did what, when, and whether they truly understood the training. If someone repeatedly fails phishing tests, it may indicate a need for further training or restrictions on access to sensitive systems. For example, let's say Sally in accounting clicked on the email and tried to sign in. She then needs to be educated and tested on her mistakes. However, if you find out this is a pattern, Sally should probably no longer have access to email.

Finally, you must treat your documentation as critical data. Don't just print it out or save it to a computer. Make sure you have secure backups you can rely on. By making this effort, you'll streamline the entire insurance process and ensure you've done everything possible to secure the most favorable premiums and smoothest claim process possible.

Now, you might be thinking, "If we do all this work and wind up documenting where we're screwing up, is that going to get us kicked off our insurance?" Even though you might think that would be the risk you face in being that transparent about where you're coming up short, in reality, the answer is no. They only care that you actually did something. You were proactive about security. They don't care that you're not perfect. Nobody's going to be perfect. They want to make sure you're trying.

It's the same thing with achieving and maintaining compliance. For example, there are safe harbor laws with compliance. It doesn't matter that you're not 100% compliant with every line item. What matters is that you have a road map, a plan of attack to get there, and you've been properly documenting that journey.

Now, this might seem like a lot of work. It is. That's why I strongly recommend you don't attempt to do it alone.

## Get Help Along This Journey

Managed Services Providers (MSPs) can act as seasoned navigators across today's challenging cybersecurity landscape. It's not merely that they understand the tech and the terminology. They've done this before and generally are the only people who understand why certain questions are on the insurance questionnaires because there's almost always a question behind the underlying question.

Let's say one of the questions is, "Do you have 2FA (two-factor authentication) or MFA (multi-factor authentication) on remote access?" Remote connection software commonly requires 2FA to log into your account. You may even use one that requires you to type in that 2FA code every time you sign into the website. Therefore, you might answer Yes to that question.

However, most remote software is designed for logging into the app on your remote computer for the first time. It's not always forcing a 2FA code whenever you open the app to connect to the remote system. So, what the question is actually asking is, "Do you have 2FA that requires credentials you must use every time you are accessing the

remote device?" What they really want to know is whether you're using 2FA on that end workstation as part of the final login to the computer.

It's not about the software you're using to do it. It refers to the process of accessing the computer itself. If someone steals your laptop and hacks into it, and it has remote connection software installed, can they make it all the way to your computer without 2FA? If they can, where should there be a roadblock?

So, it's not only about knowing the technology and answering the questions. It's about understanding the underlying concepts and surrounding processes. If you answer incorrectly, your policy rates will increase, and your chances of being dropped will increase. That's why you need the help of someone who's done this before and can help you along the way—someone who, when they see an acronym like SDR in a question, which has no industry standard definition, can spot that and will go back to the insurance company for clarity to make sure you can answer it correctly.

## The Road To Resilience

By following this process, you fortify your position in the eyes of the insurance companies. You're doing all the necessary things to be able to answer true, true, true rather than false, false, false on their questionnaires – and you made those choices wisely, with an understanding of the actual context. Plus, you've not only improved your long-term defensive posture against external threats, but you've also improved your reputation with your insurance company. This means you'll secure the most favorable premiums possible and be much better positioned to renew that policy.

Over the long term, the cost of cyber insurance will almost certainly increase. And as you add more clients and patients, you'll need more insurance. Unless you've done all these things, they can withhold increasing your coverage because you can't prove you're properly handling the security necessary to keep or increase your current level of coverage.

Remember: Their goal is never to pay out a claim. However, using this kind of checklist as you go through the process of getting insurance will help ensure that you implement the things you need to have in place to keep your business safe and secure.

If you're doing everything right – working with a partner, doing all the documentation, doing all the training – then getting increased coverage won't be a problem.

As a final benefit, this adds significant reputational clout to your business. You can honestly assure your customers, "You're safe coming here and dealing with us because we take the security of your information seriously."

All of this makes it so that when you arrive at work early on Monday morning, coffee in hand, hoping to catch up on some paperwork and jump-start the coming week, and you sit down at your desk to log into your system, nothing unusual will happen. You can savor that cup of coffee and focus on the tasks at hand, free from worry.

## About Zachary Hamblen

Zachary Hamblen owns and manages Your IT Guys, an IT firm whose mission is to provide dental practices with the IT support they need to thrive in the digital age. Today, Your IT Guys serves practices of all shapes and sizes across Central Florida.

Zachary has over 15 years of IT experience working in organizations serving the dental industry and hospitality. His background includes being the IT director at HVS Corporation, as well as having worked for nearly five years as a technical service technician for Patterson Dental, a leading provider of equipment and technology to the dental industry.

He understands the challenges dentists face in balancing the needs of their patients with the requirements to keep practice data accurate and safe. He strives to work as a true partner to his clients, working closely with them to provide customized solutions that improve their practice's efficiency and productivity while at the same time keeping their systems operational and secure.

The entire Your IT Guys team was built from the ground up around experts certified in various technology fields; they are passionate about consistently updating their knowledge and certifications to stay ahead of the industry's technology trends. They also belong to multiple industry associations and partner with best-of-breed technology vendors to provide every client with the best possible service and support.

Zachary has three children he adores and loves to spend time with his family, often working together to create amazing Lego structures. He's also raising chickens as a reprieve from technology for a bit and experiencing the pleasures of having fresh eggs every day.

Zachary believes that everything provides an opportunity for your business and your life to thrive. He is proud of his company and team's reputation as a reliable and trustworthy IT partner to dental practices. They have many clients who have been on board for over 10 years, all thanks to the quality of service they just can't find anywhere else.

**For more information, contact Zachary Hamblen at Your IT Guys:**
**Phone:** 321-221-2991
**LinkedIn:** linkedin.com/in/youritguys/
**Email:** zach@youritguys.biz
**Web:** help.dental/

THE
# CYBER PLAYBOOK

## ABOUT ZACHARY HAMBLEN

Zachary Hamblen owns and manages Your IT Guys, an IT firm whose mission is to provide dental practices with the IT support they need to thrive in the digital age. Today, Your IT Guys serves practices of all shapes and sizes across Central Florida.

Zachary has over 15 years of IT experience working in organizations serving the dental industry and hospitality. His background includes being the IT director at HVS Corporation, as well as having worked for nearly five years as a technical service technician for Patterson Dental, a leading provider of equipment and technology to the dental industry.

He understands the challenges dentists face in balancing the needs of their patients with the requirements to keep practice data accurate and safe. He strives to work as a true partner to his clients, working closely with them to provide customized solutions that improve their practice's efficiency and productivity while at the same time keeping their systems operational and secure.

The entire Your IT Guys team was built from the ground up around experts certified in various technology fields; they are passionate about consistently updating their knowledge and certifications to stay ahead of the industry's technology trends. They also belong to multiple industry associations and partner with best-of-breed technology vendors to provide every client with the best possible service and support.

Zachary has three children he adores and loves to spend time with his family, often working together to create amazing Lego structures. He's also raising chickens as a reprieve from technology for a bit and experiencing the pleasures of having fresh eggs every day.

Zachary believes that everything provides an opportunity for your business and your life to thrive. He is proud of his company and team's reputation as a reliable and trustworthy IT partner to dental practices. They have many clients who have been on board for over 10 years, all thanks to the quality of service they just can't find anywhere else.

Designed and Produced by Big Red Media
Printed in the USA

BigRedMedia
a TMT company