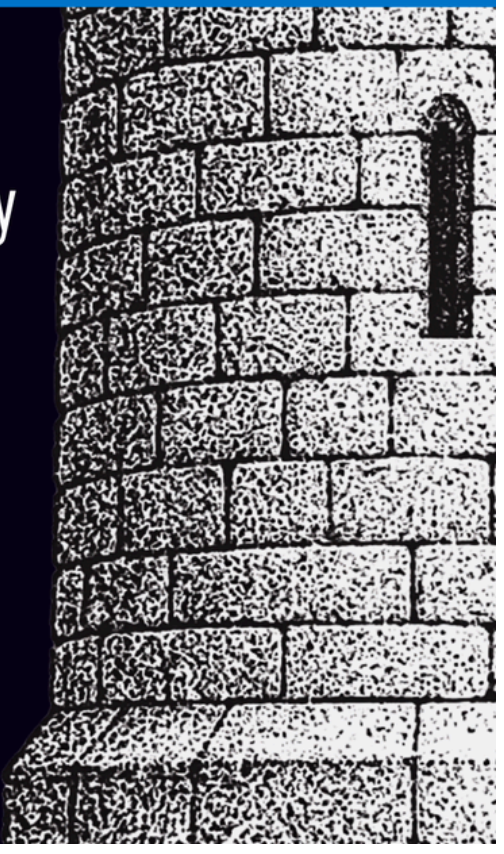
SECURED



The Cybersecurity Survival Guide for Protecting Your Business

JACK RAMSEY

SECURED

The Cybersecurity Survival Guide for Protecting Your Business

Copyright © 2026

All rights reserved. This publication is provided under a limited use license for educational purposes only.

It may be shared, printed, or distributed freely, provided it remains complete and unaltered in its original digital or physical form.

No part of this publication may be modified, edited, repackaged, or claimed as your own. The copyright and all intellectual property rights remain with the original author and publisher.

The original author reserves the right to publish, bind, and commercially distribute this material in any format.

This publication is intended to provide accurate and helpful information regarding the subject matter covered. It is shared with the understanding that the author is not offering legal, financial, or professional advice. If such advice is needed, the services of a qualified professional should be sought.

Use of this material is at the reader's own discretion and responsibility.

Compliance with all applicable laws, regulations, and licensing requirements is solely the responsibility of the reader. The author assumes no liability for any actions taken based on the content of this publication.

TABLE OF CONTENTS

Why a Book on Cybersecurity? 3

PART I - The What & The Why

What Cybersecurity Is 6

The ROI of Investing in Cybersecurity 10

The Most Common Threats 14

Follow a Framework 24

PART II - The Top Controls

People & Identity 28

Devices & Endpoint Security 36

Email, Web, & Collaboration Security 43

Data Protection 50

Networks & Cloud Basics 57

Vendor & Third-Party Risk 63

PART III - The Final Layer of Protection

Incident Response & Business Continuity 70

Compliance & Governance for SMBs 80

Conclusion 86

Legend (Jargon Decoder) 90

WHY A BOOK ON CYBERSECURITY?

To no one's surprise, what you're holding in your hand (or reading on your screen) is a book on cybersecurity.

But why does the world need another book on a topic that has been turned upside down and inside out so many times?

Because many business owners still see cybersecurity as a big, scary word they would do anything to avoid. For many, it creates that same stomach-crunching, heart-in-your-throat feeling they get when they're about to visit their dentist.

That feeling often stems from the unknown and from years of fear-mongering. So, cybersecurity remains somewhat of a fringe topic, often pushed aside for "better" subjects like sales, marketing, and operations.

After all, no one wants to contemplate the horror scenarios their business or even their lives could face, especially when they could be focusing on how to grow their business instead.

The bad part about this is that fear can lead to "techno-stress" and apathy. If a problem seems too overwhelming or complex, business owners tend to feel helpless and disengage completely, ironically making them more vulnerable to those very threats they fear.

With that in mind, I promise you this book is not meant to create manufactured urgency or use fear-mongering as a tactic to compel you to invest in cybersecurity.

The goal of this book is to demystify cybersecurity, make it digestible, and, at the risk of pushing it too far, maybe even exciting.

It aims to give you the confidence that you can implement cybersecurity in your business without being an expert, providing you with knowledge of how cybersecurity works and how simple it can be if you follow a framework.

Simply put, you're about to dive into how to keep your business secure and protected from those pesky hackers.

Now, I can't promise that just reading this and putting it into practice will make your business totally unbreachable, as that's just not realistic. But it will make your defenses a whole lot stronger!

The truth is, there's no such thing as a 100% secure business or organization. If an IT provider tells you that, they're probably not being completely straight with you.

Even big governments, with all their fancy resources, can get hit by sophisticated attacks.

That being said, you will be able to protect your business against most threats out there. You might even be surprised to hear that a huge chunk, 80-90% of breaches, comes from incredibly simple, often overlooked things.

The good news about this is that it also means it's pretty straightforward to put effective safeguards in place.

And as we go further, you'll see that a big part of cybersecurity is really just about building new, consistent habits. Easy, actionable steps that you and your team can add to your everyday routines.

Take this book one step at a time.

Don't feel like you need to implement everything at once. Instead, just pick one or two practical things from each chapter that you can start doing right away. The main goal here is to make incremental progress, rather than stressing about being perfect overnight.

We'll kick things off by getting a good handle on the basics, and from there, we'll walk through the most important habits for keeping both your people and your valuable data safe and sound.

So, grab a coffee (or whatever your favorite beverage is), and let's get started on building a more secure future for your business together!

Regards,

JACK RAMSEY
Co-Founder | CEO
209-920-4077 | jack@rj-pro.net | rj-pro.net
1919 Vista Del Lago Drive, Suite 3
Valley Springs, CA 95252

RJ PRO TECH GROUP
INNOVATIVE I.T. SERVICES

PART I

CHAPTER 1:

WHAT CYBERSECURITY IS

CHAPTER 1:
WHAT CYBERSECURITY IS

I want to start this chapter by clarifying what cybersecurity is NOT.

Tech experts often make simple subjects complicated, and that's exactly what I aim to avoid in this book.

For the average business owner, cybersecurity is not an overwhelmingly complex subject. While it's true that cybersecurity can become complex for Fortune 500 companies, government agencies, or scientific laboratories, it's a different story if your company isn't dealing in highly sensitive data or operating in critical infrastructure sectors.

For most small to medium-sized businesses, the fundamentals are straightforward and manageable.

Cybersecurity isn't a product you buy. It’s a collection of smart business habits to manage digital risk. Essentially, cybersecurity is how we reduce the likelihood and impact of events that could misuse, disrupt, or expose valuable data and systems. It’s simply risk management for the digital parts of your company.

And cybersecurity does not discriminate. Many owners think they’re too small to be a target. That’s a dangerously outdated assumption.

Most hackers aren't master criminals looking to take down a government. They're running a business based on volume, using automated software to scan the entire internet for easy openings. Your size doesn't make you invisible; it can make you an easier target because hackers assume you have weaker defenses.

This is why **43% of all cyberattacks are aimed at small businesses,** and a shocking 60% of them shut down within six months of a major attack.

But here’s the most important part: The vast majority of these attacks aren’t sophisticated, high-tech assaults. They prey on simple, overlooked things.

The latest data shows that **between 60% and 95% of all breaches involve a non-malicious human element**, like an employee accidentally clicking a bad link or being tricked by a convincing email.

This means that straightforward, effective safeguards are completely within your reach. The power to protect your business is in your hands, and it doesn't require a million-dollar budget.

So, how do you protect against these common threats? You just need a simple way to think about it.

Everything in cybersecurity really comes down to three core pillars:

The first is **Identity**. This is all about who has the keys to your business—your people, their accounts, and the devices they use. If your habits here are sloppy, like sharing passwords or not removing access for ex-employees, your entire business is fragile. Strong identity management is your first line of defense.

The next is **Data**. This is what you're trying to protect—your financials, your customer lists, your secret sauce. Knowing where this data is stored, controlling who has access to it, and keeping reliable, tested copies of it is your ultimate safety net.

And finally, **Operations**. This is the discipline to keep things updated, monitor for strange activity, and have a plan for when things go wrong. It’s where your habits live, like the two-minute phone call to verify a change in bank details before making a payment or regularly backing up your systems. Effective operations ensure your defenses are always active and ready.

These three pillars form the foundation of effective cybersecurity for any business.

The solution to managing cyber risks, which this entire book is built on, involves two core concepts: building a few key habits and following a clear plan.

Much of this is about small, consistent actions that you and your team take every day. And just like any other area of your business, using a simple, proven framework brings order to chaos and prevents you from wasting time and money on things that don't matter.

This brings me to the single most important point in this entire chapter. **Cybersecurity is not an "IT thing."**

It is a leadership responsibility.

You would never let your bookkeeper be the only person who cares about the company's financial health; you, as the owner, ultimately have that responsibility.

The same is true for the digital health of your business. Your IT team or provider can do the work, but accountability starts and ends with you.

This book is designed to give you the confidence to ask the right questions, set the right expectations, and lead your team to a safer way of operating.

CHAPTER 2:

THE ROI OF INVESTING IN CYBERSECURITY

CHAPTER 2:
THE ROI OF INVESTING IN CYBERSECURITY

So, what's the return on investment for cybersecurity?

The answer isn't something you'll find in your bank statement, at least not if everything goes as planned.

The ROI of investing in cybersecurity is similar to investing in sturdy locks for your doors or a sprinkler system for your warehouse.

You're spending a bit of money now to significantly reduce the risk of a much larger, more painful loss later. In business terms, you're simply lowering your expected loss.

It's a simple formula:

Expected Loss = Financial Impact of Incident × Likelihood of Happening

Your entire goal with cybersecurity spending is to aggressively push both of these numbers down.

Let's make that "financial impact" number more real, because it's not just about a ransom demand.

First, consider the **cost of downtime**. What would it cost for your business to be completely shut down for three days?

For example, if you normally make $10,000 in revenue per day, that's $30,000 lost right there.

Add to that three days of payroll for a team that can't do their work, and then all the overtime you'll have to pay to catch up once you're back online.

Next is **the risk of direct theft**. This commonly occurs through fake invoices or compromised email accounts.

The average loss for one of these incidents is around $137,000. What would an unexpected $137,000 hole in your cash flow do to your business this quarter?

Finally, there are the cleanup costs. This is the bill you receive after the attack is over. This includes emergency cybersecurity experts, forensic investigations, system restoration, legal advice, and regulatory compliance.

For small and midsize organizations, recovery expenses often exceed **$100,000 to $500,000**, while larger enterprises face average incident costs of $4.4 million globally and over $10 million in the U.S., according to the IBM Cost of a Data Breach Report 2025.

Nearly a third of cases now involve regulatory fines, **with half of those penalties surpassing $100,000.**

When you add it all up, the total financial impact of a single incident can easily climb into the high six figures, which is why so many small businesses don't survive an attack.

So, how do you push those numbers down? You start by making investments that offer the biggest and clearest payback.

To reduce the chances of these attacks, year after year, data shows that attackers typically gain access through a few common entry points: stolen passwords and outdated software. This tells you exactly where to focus your efforts.

To reduce the likelihood of theft, begin with strong identity controls. The most important of these is multi-factor authentication (MFA), which is that small code you receive on your phone when you log in.

It stops most attacks that rely on stolen passwords. The cost of enabling MFA is tiny compared to the six-figure fraudulent transfer that never happens because an attacker couldn't get past the login screen.

To reduce the financial impact of ransomware, you need tested, offline backups.

This investment transforms a potential multi-week, business-ending disaster into a manageable one-weekend recovery.

When your files are locked and a criminal demands a ransom, the difference between "we can be back up and running by Monday" and "we have to consider paying these guys" is a clean copy of your data that the attacker couldn't touch.

With **75% of small businesses saying they could not continue operating if hit with ransomware**, a tested backup is your ticket out of that statistic.

To reduce your cleanup costs, you need modern endpoint protection and a routine for keeping your software updated.

Old antivirus software is no longer sufficient.

Modern tools look for suspicious behavior, not just known viruses. This can stop an attack in its tracks, containing it to a single computer instead of allowing it to spread across your entire network.

But good security does more than just prevent bad things from happening; it can also become a tool for growth.

The first way it does this is by making your insurance policy valid. Cyber insurance isn't a blank check.

Insurance underwriters now require you to have these basic controls, like MFA and backups, as a condition of your policy.

If you don't have them, they have clear grounds to deny your claim, leaving you to face the full financial impact of an incident alone.

The other way it helps you grow is by helping you win bigger deals.

When you demonstrate robust cybersecurity, you're proving to your prospects that you are a professional, reliable partner they can implicitly trust with their sensitive data and business operations.

This confidence can be the deciding factor in competitive bids, allowing you to secure lucrative contracts that might otherwise go to less secure competitors.

CHAPTER 3:

THE MOST COMMON THREATS

CHAPTER 3:
THE MOST COMMON THREATS

If you run a small or mid-size business, the cyber threats you face look nothing like they do in the movies.

Criminals operate like a business. Like you, they seek efficient ways to make money. This means they rely on a playbook: a small set of reliable, high-return strategies that work repeatedly.

In this chapter, we'll examine this playbook, one category at a time. We'll explore tactics they use against your people, technology, and daily operations. Understanding these plays will help you protect against them.

Category 1: Threats Targeting Your People

Most security incidents don't begin with a hacker bypassing a firewall. They start with a person.

Year after year, data shows that the "human element" is a factor in most breaches. The 2025 Verizon Data Breach Investigations Report found this **in 60% of incidents.**

Attackers know your team is your biggest asset, and they exploit this strength to find an opening.

Threat #1: Phishing & Social Engineering

At its core, phishing is a con game. It's a deceptive attack designed to trick someone into doing something they shouldn't, such as clicking a malicious link, opening a dangerous attachment, or revealing their password.

The most common form is the broad phishing campaign, where an attacker sends millions of generic emails hoping a small percentage of recipients will fall for it. These include fake FedEx delivery notices or urgent "Your Microsoft account is about to be suspended" alerts.

However, the more dangerous version is "spear phishing."

Here, the attacker does their homework. They research your company, identify key personnel in departments like accounting, and craft a personalized email that appears to come from you or a trusted vendor.

This often leads to Business Email Compromise (BEC), one of the most financially damaging attacks a small business can face.

Attackers might insert themselves into an ongoing email conversation, wait for the right moment, and then send a message like, "Hi, we've updated our bank details. Please send this month's payment to this new account."

Because it looks legitimate and is part of an existing conversation, it's incredibly effective.

BEC is a massive problem, **accounting for nearly $2.8 billion in reported losses in the U.S. in 2024 alone**, according to the FBI's Internet Crime Complaint Center (IC3) 2024 Annual Report.

At this point, you might be thinking "My employees are too smart to fall for this." And you're probably right. The problem is that these attacks don't rely on intelligence.

They exploit the distractions we all are exposed to during a busy workday. Data shows that when someone falls for a phishing email, it happens quickly, as the median time from receiving the email to clicking the link is less than 25 seconds.

So, how can you and your team recognize these attacks? They almost always share a few common traits:

- **A sudden sense of urgency.** The email creates pressure, insisting you act now or face negative consequences. Words like "Urgent," "Important," and "Attention" are common in scam subject lines. This is a psychological trick designed to induce panic and bypass normal safety checks.
- **A request that breaks the rules.** The message will ask you to do something outside your normal company process, often with a reason to keep it quiet. For example, "I'm in a meeting and can't talk, can you please just pay this invoice for me and not mention it to anyone?"

- **Slight imperfections.** The sender's email address might be off by one letter, or if you hover your mouse over a link, the destination address won't match the displayed text. These are small details that are easy to miss when you're in a hurry.

Threat #2: Insider Threats

This is a sensitive topic because it involves people you've hired and chosen to trust.

An insider threat occurs when a current or former employee, contractor, or partner uses their authorized access to harm the business.

It's more common than many owners realize, with one 2024 report showing that **48% of businesses experienced more frequent insider attacks compared to previous years**. It's important to understand this isn't always malicious.

Sometimes, it's an **unintentional insider threat**. This involves a well-meaning employee who makes a mistake.

For example, they might email a sensitive customer list to their personal Gmail account to work on it over the weekend. While they don't intend harm, they've moved company data outside your control, creating a security risk.

Other times, it's a **malicious insider**. This could be a disgruntled employee about to quit who downloads a copy of your client database to take to their next job. Or it could be a contractor whose project has ended, but their access was never revoked, allowing them to snoop around weeks later.

While you should trust your team, implementing security controls is essential.

You implement financial controls not because you assume your bookkeeper is a thief, but because it's the correct way to protect the company's money.

The same logic applies to your data. Good controls protect the business from intentional harm and prevent good employees from making accidental mistakes.

Recognizing an insider threat can be difficult because the person already has legitimate access.

The signs are usually changes in behavior:

- **Accessing unusual amounts of data.** An employee in marketing suddenly trying to access engineering blueprints, or someone downloading thousands of files right before they go on vacation.

- **Working at odd hours**. A user who normally works 9-to-5 suddenly logging in at 2 AM and accessing sensitive folders.

- **Trying to bypass security controls.** An employee repeatedly attempting to access parts of the network they're not authorized for, or asking coworkers for their passwords.

Category 2: Threats Targeting Your Technology & Supply Chain

While many attacks begin by targeting your people, they almost always succeed by exploiting a gap in your technology.

Even if an attacker tricks an employee into revealing a password, they still need a technical "door" to enter.

This is where the automated, high-volume aspect of their business model becomes evident. They use software to constantly scan the internet, searching for the digital equivalent of an unlocked window.

Threat #3: Use of Stolen Credentials

Your employees' usernames and passwords are the keys to your business.

The problem is, these keys are frequently copied and sold. When a major company like LinkedIn or Adobe experiences a data breach, the lists of stolen usernames and passwords from that breach often appear for sale on the dark web.

Criminals purchase these massive lists and then use automated software to try those same username and password combinations on other websites, such as your company's email login page.

This is called "credential stuffing," and it works because people reuse passwords. A recent study found that 49% of employees reuse the same credentials across different work-related applications.

If your employee used the same password for their old Myspace account that they now use for your company's payroll system, a breach from a decade ago can suddenly become your problem today.

That might sound like a stretch, but stolen credentials are being used in 86% of web application attacks.

So, how do you recognize if this is happening? Here's what to look for:

- **Login alerts from unusual times or locations.** You might receive an email from Microsoft indicating someone tried to log into your account from a different country at 3 AM.
- **Getting locked out of your own account.** If an attacker repeatedly tries to log in with the wrong password, the system might lock the account for security reasons, preventing even you from accessing it.
- **Seeing activity you don't recognize.** You might notice emails in your "sent" folder that you didn't write, or observe that files have been accessed or downloaded when you weren't working.

Threat #4: Exploitation of Unlocked Digital Doors

This is the fastest-growing type of attack, based on a simple premise: hackers constantly and automatically check for unlocked doors on the internet.

The 2025 Verizon Data Breach Investigations Report found that attacks exploiting these kinds of vulnerabilities as the first step in a breach saw another year of significant growth, increasing by 34% from the previous year.

There are two main types of "unlocked doors" they look for.

The first is **software vulnerabilities.**

Think of this like a car manufacturer discovering a faulty lock on one of their models and issuing a recall. As soon as that recall is announced, car thieves know exactly what to look for.

The same thing happens with software. When a company like Microsoft or Google finds a security flaw in their product, they release a fix, called a "patch."

The moment that patch is announced, criminals begin running automated scans across the entire internet, looking for any business that hasn't installed it yet. With nearly **21,500 new software vulnerabilities disclosed in just the first half of 2025 alone**, criminals have a constant supply of new doors to check.

The second type of unlocked door is misconfigured remote services. These are the tools your team uses to work from outside the office, like a VPN or Remote Desktop Protocol (RDP).

These tools are essential for modern business, but if they're set up with weak, default passwords or aren't protected with multi-factor authentication, they become a wide-open door visible to the entire internet.

Criminals can weaponize a new vulnerability in a matter of hours, while it takes the average organization around 55 days to patch just half of their critical flaws. This massive gap is the window of opportunity attackers exploit.

And the only evidence that someone gained access through an unpatched piece of software or a poorly secured remote login is what they do next, which is often installing ransomware and locking up all your files.

Threat #5: Supply Chain Compromise

Your business doesn't operate alone. You work with many outside vendors like IT providers, accounting firms, and payroll services, and you use various software tools daily. A supply chain attack happens when criminals hack into one of these trusted partners. They then use that partner's legitimate access to get into your systems.

This is an increasingly popular and efficient tactic.

Why attack one hundred small businesses individually when you can attack the single piece of software they all use and gain access to all of them at once?

Data shows this is a rapidly growing problem. Supply chain attacks have doubled in frequency since early 2025, with an average of 26 incidents per month targeting organizations worldwide.

Currently, around **45% of organizations have been targeted through supply chain vectors**. Breaches involving a third party now account for approximately 30–35.5% of all incidents, representing an increase of about 6.5% to 11% year over year.

Third-party access is also responsible for over 41% of ransomware attacks, making vendor security a critical point of focus today.

And if you're thinking that your vendors' security is not your problem, that's no longer true in a modern, connected business.

Your security is only as strong as the weakest link in your supply chain. If your payroll provider is breached, your employees' data is at risk. If your IT provider is compromised, attackers could gain the keys to your entire kingdom.

You must consider your key vendors an extension of your own company and hold them to a reasonable security standard.

Recognizing a supply chain attack is extremely difficult because the attack often originates from a source you already trust:

- **A breach notification from your vendor.** Often, the first you'll hear about a problem is when one of your vendors sends you an email stating they've had a security incident and that you might be affected.

- **Suspicious activity from a legitimate account.** You might observe one of your vendor's user accounts logging in at odd hours or attempting to access parts of your system they don't normally touch. Because the account is legitimate, it can be very hard to spot.

- **Your security tools flagging a trusted application.** Your endpoint protection might suddenly flag a routine update from a trusted piece of software as malicious. This can happen when an attacker has managed to inject their own malicious code into a legitimate software update.

Category 3: Threats Targeting Your Operations

Once an attacker gets past your people and your technology, their next step is to disrupt your operations and turn their access into a payday. These are the threats that directly target your ability to make money, serve your customers, and keep your doors open.

Threat #6: Malware & Ransomware

Malware is a general term for any malicious software an attacker installs after gaining access. It could be spyware that steals information from your computers, or a keylogger that records everything you type.

Often, this kind of malware runs in the background for weeks or months, gathering information and providing the attacker with a clear picture of your business.

However, the type of malware that grabs headlines is ransomware, and for good reasons.

Ransomware is the final payload, a malware with a business model.

Once the attacker has explored your network, they launch the ransomware, which spreads rapidly and encrypts all your important files. Everything is locked, and the only way to recover it is to pay the attacker for a decryption key.

To add more pressure, attackers almost always steal a copy of your data first and threaten to leak it publicly if you don't pay.

This is called 'double extortion,' and it is now a standard tactic, with ransomware involved in approximately one-third to 45% of all breaches.

In some cases, attackers also apply further pressure by targeting third parties or launching denial-of-service attacks, known as triple extortion.

So, how do you recognize these threats?

- **Malware is often hard to notice.** The signs can be subtle, such as unexplained slow computers, strange pop-ups, frequent crashes, or software you don't remember installing. Malware may also cause unusual network activity or disable your security tools, making detection difficult without proper monitoring.

- **Ransomware is the opposite.** The signs are impossible to miss. You'll see a ransom note on the screen, and none of your files will open. It's designed to cause an immediate and total work stoppage.

Threat #7: Denial-of-Service (DoS/DDoS) Attacks

Not all attacks aim to steal data or money. Some are simply about causing disruption. Imagine your business has a single phone line, and a prankster arranges for a hundred people to call it at the exact same time, repeatedly.

Your legitimate customers wouldn't be able to get through. That's essentially what a Denial-of-Service (DoS) attack does to your website or online services. It floods them with so much junk traffic that they become overwhelmed and unavailable to real customers.

When that junk traffic originates from thousands of computers all over the world simultaneously, it's called a Distributed Denial-of-Service (DDoS) attack.

The numbers and scale of these attacks have surged dramatically. In fact, in the first half of 2025, **DDoS incidents rose by over 40% year-over-year globally**, with some reports noting a 108% increase in certain regions.

The largest recorded attack in mid-2025 peaked at 7.3 terabits per second, involving hundreds of thousands of devices worldwide.

So, how do you recognize a DoS or DDoS attack?

- Your website or online systems suddenly become extremely slow or completely unreachable for legitimate customers.
- There may be a sharp surge in Internet traffic, often far beyond normal volumes.
- You might receive an email or message from the attacker demanding payment to stop the flood of traffic, a common extortion tactic.

CHAPTER 4:
FOLLOW A FRAMEWORK

CHAPTER 4:
FOLLOW A FRAMEWORK

When you're building a cybersecurity program, it's easy to get lost in the details or buy tools you don't need. A recognized cybersecurity framework prevents that.

For U.S. businesses, the NIST Cybersecurity Framework (CSF) is the best starting point. Your entire cybersecurity program can be organized around its six core functions: Govern, Identify, Protect, Detect, Respond, and Recover.

This framework acts as your blueprint, guiding you to prioritize what's important, inventory your assets, shield them from threats, spot trouble quickly, respond effectively to incidents, and recover smoothly afterward. It stops you from adding random security controls without a coherent plan.

The latest version, CSF 2.0, added Govern as a central function. This addition acknowledges what business owners have always known: leadership and accountability are crucial. It clarifies that cybersecurity is a fundamental business function, not just an IT problem.

What Each Function Means for Your Business

The NIST framework is valuable because each function translates into a practical conversation you can have, even without a technical background.

- **Govern:** This function is about setting the rules. You'll decide who is responsible for security, how you'll manage risk, and what your tolerance is for downtime or data loss. This is where you establish policies and ensure everyone understands their role.

- **Identify:** You can't protect what you don't know you have. This function guides you to create a complete inventory of everything that keeps your business running: all your systems, user accounts, important data, and key vendors.

- **Detect:** This is where you actively monitor your systems for anything unusual. The goal is to spot strange behavior and potential threats quickly, minimizing their impact.

- **Respond:** When an incident happens, you need a plan. This function involves creating clear steps to follow, so your team knows exactly what to do when a security breach occurs.

- **Recover:** After an incident, this function focuses on restoring your systems and data cleanly from backups. The aim is to get your business back to normal operations on a timeline that minimizes disruption.

Putting the Framework to Work

Using a framework like NIST prevents you from making superficial progress, where you might secure one part of your business but leave other areas vulnerable. With these six functions in mind, you won't skip critical steps.

You wouldn't invest in advanced detection tools before you even know what you're trying to protect. Nor would you consider security training a success if your incident response plan is still uncertain.

The alternative to a framework is what most businesses do: they react. A scary news story about ransomware comes out, so they rush to buy a new backup tool. They hear about a phishing attack, so they sign up for a training video. This "whack-a-mole" approach feels like you're doing something, but it leaves huge, invisible gaps in your security. A framework gives you a complete picture.

This structure is also a powerful management tool. As the owner, you don't need to know the technical details of every single control. You just need to be able to ask your team, "How are we doing on the 'Protect' function this quarter? Can you show me the proof that our backups are working?" The six functions give you a simple, high-level scoreboard to track progress and hold people accountable. It translates all the complex, behind-the-scenes technical work into a straightforward business conversation.

Your team understands what truly matters, your partners see a well-thought-out plan, and your customers feel confident in your preparedness. Instead of reacting aimlessly, you implement controls because your comprehensive plan requires them.

A quick note before we move on: The next part of this book will walk you through the specific actions and controls you need to implement, the "how-to" for things like MFA, backups, and securing your devices.

My strong recommendation is to not just do these things randomly. Do them as part of the framework we just talked about. When you do that, it gives you a clear path, so you're always working on the most important thing first.

It also makes it much easier to prove your security to big customers or your insurance company, because you can show them you're following a recognized standard. It makes security a simple routine, not a bunch of random projects.

PART II

CHAPTER 5:

PEOPLE & IDENTITY

CHAPTER 5:
PEOPLE & IDENTITY

Your business has important digital stuff: customer lists, prices, and sales plans. Without good planning, these can get out when an employee leaves, or worse, get stolen in a cyberattack.

This chapter will show you how to control who gets into your systems and data, so your key info stays safe.

Everyone who works for you—employees, contractors, and even your accountant—needs specific access to do their job. Also, the software you use often needs to talk to other apps.

The goal is to make sure everyone and everything only gets access to what's needed, and only for as long as needed. For example, your sales team needs sales software, but they shouldn't see payroll records. When a contractor's project ends, their access should be cut off right away.

You wouldn't let an ex-employee keep their office keys, and it's the same for your digital systems, and so on.

What You Need to Do

You only need four basic habits to get the maximum return with the lowest effort. If you do these four things right, you'll fix most of the problems we've talked about before.

1. Use Multi-Factor Authentication (MFA).

You probably use MFA every day for your bank app. It's that extra code you get on your phone after typing your password. MFA is just a second check to make sure it's you.

Your password is the first check ("something you know"), and the code on your phone is the second ("something you have").

A criminal might steal your password, but it's much harder for them to also have your phone.

MFA is important because passwords get stolen often. It's not a question of if your employees' passwords get exposed, but when, and how many.

Without MFA, a criminal who gets one of your employee's reused passwords can easily get into your systems. But with MFA, that stolen password is useless.

The criminal might have the password, but when they try to log in, the system will ask for the code from your employee's phone, stopping the attack at the door. This is the single best thing you can do to protect your business. It's not too much to say that this one control stops most cyberattacks.

The numbers are clear:

- **Microsoft said that using MFA blocks 99.9% of automated password attacks**. It's almost a magic bullet in security.

- The 2025 Verizon Data Breach Investigations Report found that stolen passwords were used in 88% of web application attacks. MFA directly stops this main attack method.

Even with that in mind, a recent report noted that nearly half of all small and midsize businesses still rely on passwords alone without using multi-factor authentication.

This is the biggest difference between good security and what businesses actually do. This is also why your cyber insurance company will almost certainly require it. It's not an option anymore.

To get cyber insurance, or more importantly, to get a claim paid if something happens, you'll need to prove you're using MFA on your important systems, especially your email and any remote access. It's a must-have for any modern business.

2. Use a Business Password Manager.

Let's be real about passwords. The average person manages dozens, and for some jobs, it's closer to a hundred. Remembering that many unique, complex passwords is impossible. So, people take shortcuts: they reuse passwords, use small changes, or use personal details like their kid's name or pet's name. They also write them on sticky notes.

Finding shortcuts is part of our human nature, so there's nothing you can do about that. But these habits create a huge security risk for your business.

Data clearly shows that weak or stolen passwords are why most business breaches happen.

Instead of just telling your team to "use better passwords," you need to give them a tool that manages passwords for them: a business password manager.

This is a secure program where your team can safely create, save, and share passwords. Each employee gets their own encrypted account and only needs to remember one strong master password to open it.

The password manager does the rest, creating random, impossible-to-guess passwords for every website and app they use, and remembering all of them.

This is important for several reasons.

First, it completely solves the password reuse problem. When every site has its own unique, strong password, a data breach at another company doesn't affect you. If an employee's LinkedIn password is stolen, it doesn't matter because their company email password is completely different.

Second, it stops the use of weak, easy-to-guess passwords. Believe it or not, common passwords like "123456" and "password" are still widely used. A password manager makes it easy to use a complex password like "**Tr0c3[sub4dour\&R3fls2za@eX\!**" for every site, because the user doesn't have to remember it.

The numbers show how big this problem is:

- About half of all employees say they reuse passwords across different work apps .
- **Nearly 60% of adults use personal info like names or birthdays in their passwords**, making them incredibly easy for an attacker to guess.
- Even in 2025, "123456" is still the **most-used password globally**, appearing in millions of leaked accounts.

A business password manager also provides a safe way to handle shared accounts. Think about your company's social media accounts or a shared vendor login.

How do you share those passwords now? In a spreadsheet? An email? Hopefully not (fingers crossed).

A password manager lets you give specific team members access to that login without them ever seeing the password itself. When an employee leaves, you can remove their access to all shared accounts with one click, turning an unsafe process into a controlled one.

3. Follow the "Principle of Least Privilege."

An employee should only have the absolute minimum access needed to do their job, nothing more.

Your marketing person needs social media accounts and the marketing drive, but not your accounting software. Your sales team needs the Customer Relationship Management (CRM) software, but they shouldn't see employee HR files.

While this seems like common sense, in many businesses, access is given freely "just in case" someone might need it and is rarely checked or removed.

Over time, this means almost everyone can get into almost everything. One study found that in a typical company, thousands of sensitive files are open to every single employee.

This principle is important, because if an employee's account is ever hacked, the damage is limited.

If an attacker steals a password from one of your sales team members, their first goal will be to move around your network to find valuable stuff, like financial data or server backups. This is called "**lateral movement**." But if that salesperson's account never had access to the financial system, the attacker is stuck.

They are only in the sales department. The attack is contained, and the damage is limited. A 2025 report found that 41% of attacks used too much access to move around and do more damage. By making sure people only have the access they need, you take away this weapon from attackers.

4. Have a Clear Process for When People Join or Leave.

This solves the problem we talked about at the start of the chapter. You need two simple, non-negotiable checklists: one for when a new person starts and one for when a person leaves.

The "joining" checklist, or onboarding process, makes sure a new employee only gets access to the systems needed for their specific role, based on the rule of least privilege.

They don't get a general login that everyone else has; their access is custom-made for their job from day one.

The "leaving" checklist, or offboarding process, is even more important.

The moment you know an employee is leaving, this process should start right away. It should be a simple list of every account that person has, from their email and main network drive to all the software-as-a-service tools the company uses.

The goal is to shut off all access within minutes, or at the very least within hours. A fast and thorough offboarding process is one of the most important security controls you can have, because former employees are a real risk. One study found that 32% of workers admit they have accessed a former employer's account after they left.

Without a strict offboarding process, you end up with "ghost users"—old, active accounts from former employees on your network.

Research from 2025 shows that a majority of organizations, often **more than 80%, have stale or dormant user accounts in their systems**, creating a significant security risk. For example, Microsoft reports that over 10% of Active Directory accounts as stale.

These accounts are a goldmine for attackers. They are often not watched, and if an attacker gets the password for one, they can access your network looking like a real, though old, employee, making them much harder to spot.

Cleaning up these old accounts and having a process to stop new ones from being created is essential.

Common Mistakes to Avoid

Getting the big things right is half the battle. The other half is avoiding a few common mistakes that can undo all your hard work. These seem small but create huge openings for an attacker.

Sharing "admin" accounts.

This is very common, especially in smaller businesses. You might have one main "admin" login for your server or a key piece of software, and everyone who needs it shares the password for convenience.

This often happens with outside IT help, where their whole team uses one "admin" login.

The problem is you have no idea who did what.

If someone makes a mistake and takes a system down, or worse, does something bad, you have multiple suspects but no proof. You can't hold anyone responsible because there's no record of who was logged in.

When something goes wrong, you need to be able to check a log and see exactly which person's account made the change.

This is the only way to quickly figure out what happened and fix it.

The rule must be simple: one person, one account. Always. This is especially true for any account with the power to change your systems.

Thinking of security training as a one-time thing.

Nobody learns anything from a boring, one-hour security video they're forced to watch once a year.

They click through it to finish, forget everything a week later, and it doesn't change how they act.

What works is short, regular reminders. The goal is to build a habit of healthy caution over time. People are a key factor in the vast majority of breaches, so this isn't a small issue either.

What to Ask Your IT Provider

As a business owner, your job isn't to do the technical work, but to hold your IT team or provider responsible. You do this by asking simple, direct questions that request proof.

These three questions will tell you almost everything you need to know about how well your people and their access are being managed.

- **"Can you show me a report that proves 100% of our employees are using MFA on their email?"**

This is a yes or no question. Don't accept "we're working on it" or "most people are." You need to see proof. Email is the front door to your business, and if even one account isn't protected, it's a huge risk.

- **"What's our formal process for when an employee leaves? How quickly can you guarantee all their access will be shut off after we tell you?"**

The first part of this question forces them to have a real, written process, not just an informal "we'll get to it" plan. The second part needs commitment. The answer you're looking for is a specific time, like "within 30 minutes of your notification."

- **"I need a list of everyone who has admin rights to our network. Let's review it together next week."**

This is one of the most important reviews you can do. Admin rights are the keys to the kingdom. Those who have them can do anything, including creating new users, deleting data, and turning off security controls. Your IT provider can give you the list of who has these rights, but only you, as the business owner, can decide if they still need them.

CHAPTER 6:

DEVICES & ENDPOINT SECURITY

CHAPTER 6:
DEVICES & ENDPOINT SECURITY

Every laptop, computer, and phone used for work is a potential entry point into your business.

If these devices aren't secured and kept up to date, they create serious risks. For example, an old, unmanaged laptop can become infected with ransomware, quickly spreading to your main file server and shutting down your entire business.

This chapter focuses on managing all devices that access your company's data.

Our goal is simple: make sure every device is known, secured, and updated. We're moving from controlling who has access to controlling what they use for that access.

What You Need to Do

Securing your devices involves a few basic habits. Get these right, and you'll prevent most problems.

1. Keep a Live Inventory of All Devices.

This is the basis for everything else. You need a complete, current list of every computer, laptop, and phone used for your business. A list you update regularly (this is very important) showing what's connected to your business right now.

You can't protect a device you don't know exists.

This is also important if a laptop is lost or stolen. You need a list to know what's missing so you can remotely lock it or wipe its data. If a security incident happens, the first question is always, "What device was involved?" Without an inventory, you're guessing, wasting critical time when trying to stop an attack.

- **You can't secure what you can't see.** An inventory is your single source of truth for what you need to protect.

- **It's an early warning system.** A good inventory system alerts you when a new, unknown device connects to your network, or when a known device hasn't checked in and might be missing.

- **It's essential for incident response.** When an attack happens, knowing which device was the entry point is the first step to containing the problem.

2. Enforce a Secure Setup for Every Device.

Once you know what devices you have, make sure each one has standard, required security settings. This isn't optional. If a device accesses your company's data, it must meet these minimums. Two parts are non-negotiable:

First, every laptop and computer must have full-disk encryption turned on. This feature is built into modern operating systems like Windows and macOS. It scrambles all data on the hard drive, making it unreadable without the password.

If an employee's laptop is lost or stolen, encryption makes all data useless to the thief. Without it, a thief gains access to your customer list, financial documents, and payroll.

With encryption, they just have hardware to sell. It turns a potential data breach into a minor inconvenience of replacing a machine.

Second, your employees should not have local administrator rights on their computers for daily work. "Admin rights" means the ability to install software and change core system settings.

If employees have these rights, they can accidentally install malware from an email. Worse, if their account is compromised, an attacker can use those rights to install malicious tools, disable security software, and spread across your network.

This "lateral movement" turns a small problem on one laptop into a company-wide crisis.

Removing these rights creates a huge roadblock for most attacks. If an employee needs new software, your IT provider should have a simple process to approve and install it. This small workflow change makes a huge difference in your security.

- Lost or stolen devices are a huge risk. One report found physical loss or theft of a device was a factor in 21% of security incidents. Full-disk encryption is the simple solution.

- Attackers rely on excessive permissions. A 2025 report from Palo Alto Networks found that **41% of attacks leveraged excessive privileges**, like admin rights, to move around a network and cause more damage. Removing those rights takes that tool away.

3. Use Modern Endpoint Protection (EDR).

Traditional antivirus software, which you've likely had for years, is no longer enough. It stops known threats but is blind to modern attacks designed to look like normal activity, using the computer's built-in tools.

You need a modern tool called Endpoint Detection and Response, or EDR.

An EDR system actively monitors your computer systems for suspicious activities and attack patterns. It can identify when a seemingly normal program, such as Microsoft Word, begins to exhibit unusual behavior, like attempting to encrypt files, and will then alert you to the potential threat.

The "Response" part of EDR is also critical. When it spots a problem, a good EDR can automatically stop the attack from spreading. For example, it can immediately quarantine an infected computer, cutting it off from the rest of the network. This turns a potential company-wide crisis into a contained problem on one laptop. But the tool is only half the solution.

Someone must monitor the alerts and know how to act when a real problem is spotted.

• **Most attacks start at endpoints (employee's computer or phone)**, with estimates generally placing this figure between 60% and 80%, making this your most critical layer of defense.

• **Modern attacks are designed to be invisible.** Attackers now use "malware-free" techniques, using your computer's legitimate tools against you. Traditional antivirus misses this, but an EDR watching for suspicious behavior catches it.

- **A quick response is everything.** The difference between a minor incident and a major breach is often minutes. An EDR that can automatically isolate a device buys you critical time to respond before the situation escalates.

4. Have a Consistent Process for Security Updates (Patching).

This is one of the most important and most overlooked parts of basic security. When a company like Microsoft or Google finds a security hole in their software, they release a fix called a "patch" or an update.

The moment they announce that patch, a race begins. You and your IT provider try to install it on all your computers. At the same time, bad actors use automated tools to scan the internet, looking for businesses that haven't installed it yet. They know exactly what the unlocked door looks like and have powerful tools to find it.

This is why a consistent, repeatable process for installing updates is so important. You can't put it off. Attackers can exploit newly announced vulnerabilities in hours.

If you only install updates monthly or whenever convenient, you leave a massive window of opportunity for them to get in.

Your process doesn't have to be complicated, just consistent. Critical updates for operating systems and web browsers should be installed weekly. For severe, "zero-day" vulnerabilities under active attack, the patch needs to be applied within a day or two.

Your IT provider should manage this automated process, and you should get a simple monthly report showing the percentage of your computers that are fully up to date.

• **Attacks on unpatched software are surging.** According to the 2025 Verizon Data Breach Investigations Report, attacks exploiting software vulnerabilities as the first step in a breach now account for 20% of breaches, a 34% increase compared to last year.

• **The number of new vulnerabilities is overwhelming.** In 2024 alone, nearly 29,000 new software vulnerabilities were discovered and reported. That's a constant stream of new potential doors that need to be locked.

- **The gap between patching and attacking is where you get hit.** The average organization takes **around 55-67 days to install patches** for half of their critical vulnerabilities. Attackers can exploit those same vulnerabilities in hours. A consistent, fast patching process closes that dangerous gap.

Common Mistakes to Avoid

Getting the big things right is half the battle. The other half is avoiding common mistakes that can undo all your hard work. These seem small but create huge openings for attackers.

Letting employees be administrators on their own computers.

This common mistake is usually for convenience. When an employee has "admin rights," they can install any software and change any setting.

The problem is, if they click a malicious link, any malware installed also gains those admin rights. It can embed deep into the computer, disable security, and spread to other network computers.

As I mentioned in a previous chapter, reports found that **41% of attacks used this exact tactic**, exploiting excessive permissions to move around a network and do more damage. Removing these rights is a simple, huge win for your security.

Having no plan for personal devices.

It's common for employees to use personal phones or laptops for work, known as "Bring Your Own Device" (BYOD).

The problem is, you don't know if that personal device is secure. Is it encrypted? Does it have a password? Is its software updated?

If an employee's personal phone with company email access is lost or stolen, your company's data is at risk. One study found that 59% of employers allow employees to access company applications from unmanaged personal devices.

You can't ignore this. If employees use personal devices for work, those devices must meet your minimum security standards, like having a passcode and encryption. Simple tools can enforce this without accessing personal photos or texts.

What to Ask Your IT Provider

- **"Can you show me a report that lists all the devices accessing our company data and confirms that 100% of them are encrypted?"**

This is a yes or no question. Don't accept "we're working on it" or "most of them are." This proves that if a laptop is stolen, the data is safe.

- **"What is our process if an employee's laptop is lost or stolen? How quickly can you guarantee it can be remotely locked or wiped?"**

The first part forces them to have a real, documented process. The second part is for a commitment. You need to know you can contain the damage from a lost device before someone tries to break into it.

- **"What endpoint protection tool are we using? Is it being actively monitored for alerts by a person?"**

This two-part question is critical. First, what tool? You want to hear it's a modern EDR, not just basic antivirus. Second, and more important: is a person watching the alerts? You need to know that if an alert comes in at 2 AM, someone will see it and act.

CHAPTER 7:

EMAIL, WEB, & COLLABORATION SECURITY

CHAPTER 7:
EMAIL, WEB, & COLLABORATION SECURITY

Email, web browsers, and collaboration tools like Microsoft Teams, Slack, and Google Drive are essential for business. They're how teams communicate internally and with customers, carrying everything from invoices and contracts to sensitive customer information and private company plans.

Unfortunately, this makes them prime targets for cyberattacks.

Business Email Compromise (BEC) scams, where criminals impersonate someone you trust to trick you into sending money, cost businesses **nearly $2.8 billion in 2024 alone**, with a median loss of **$50,000 per incident**.

Phishing attacks, often delivered via email, are the most common threat for small businesses, leading to **68% of all data breaches**.

This chapter will show you how to protect these vital communication channels by putting smart filters and safeguards in place to stop attacks and keep your information private.

What You Need to Do

Here are four simple habits and tools to protect your company's communication channels. Get these right, and you'll have a strong defense against the most common attacks.

1. Use an Advanced Email Security Tool.

Basic spam and virus filters in Microsoft 365 or Google Workspace are good for junk mail and known viruses, but they aren't designed to stop targeted, well-crafted attacks.

An advanced email security tool adds an extra layer of protection, like a deadbolt and a security camera, to catch more sophisticated threats.

These tools do things basic filters can't. When an email with an attachment comes in, a good security tool opens it in a safe, isolated environment (a "sandbox") to see if it's malicious. If the attachment tries to install malware, the tool blocks the email before it reaches your inbox.

It also analyzes links in emails. If an employee clicks a link, the tool checks the destination in real-time. If it leads to a fake login page or a site with malware, it blocks the connection and warns the user.

This is your best technical defense against phishing attacks and catches mistakes when busy employees click something they shouldn't.

The numbers show how critical this is:

- Email is the top delivery method for malware, with some studies showing **as much as 94% of all malware is delivered via email.**

2. Create a Non-Negotiable Process for Financial Transactions.

This is a business rule, not a technology solution, and it's the most important thing you can do to prevent wire transfer fraud.

Any request to change a vendor's bank details or make an unusual or urgent payment must be verified with a live phone call to a number you already have on file for that person.

An email or text message is not enough. You must talk to a real person on the phone using a legitimate number you know, not one provided in the email request.

This is crucial because technology alone can't solve this process-based defense.

The scam works by tricking a person. Attackers weaponize your trust in your vendors and your team. The only way to break that deception is to step outside the attacker's channel (email) and use a different one (the phone).

This simple habit, when it becomes a non-negotiable part of your company's culture, stops the most common and costly form of email fraud. It protects your employees from difficult situations and safeguards your company's bank account.

3. Filter Your Team's Web Traffic.

Think of this as a mandatory seat belt for the internet. A web filter automatically blocks your employees from accessing known malicious or suspicious websites.

While these filters used to be physical boxes in the office, now, with remote work, this protection must be installed directly on employee laptops, so it travels with them wherever they are.

This is important because it acts as a critical safety net. Many attacks start with a bad link in an email. A web filter is your last line of defense when a busy employee makes a mistake and clicks.

If the link leads to a website known for malware, the web filter blocks the connection before their computer gets infected. If it leads to a fake Microsoft 365 login page designed to steal passwords, the filter blocks it before they can type anything.

It protects your employees from split-second mistakes that can cause company-wide disasters. It's an automated guardrail that keeps them on the safe part of the road.

The numbers show why this safety net is necessary:

- The 2024 Verizon Data Breach Investigations Report shows that **68% of all breaches involve a non-malicious human element**, often starting with an employee clicking a phishing link.

- When people fall for these scams, it happens incredibly fast. The median time for a user to click a phishing link is **less than 25 seconds**. This isn't enough time to stop and think, which is why you need an automated tool.

- Phishing is the most common attack vector for small businesses, with **61% of SMBs** saying it was the most frequent type of attack they saw last year.

4. Set Secure Defaults for File Sharing.

Collaboration tools like Microsoft Teams, SharePoint, and Google Drive are great for work, but they often prioritize ease of sharing over security.

The most dangerous feature is the "share with anyone" or "public link" option, which creates a link anyone on the internet can use to access a file or folder without a password or login.

Sensitive data often leaks from these platforms when an employee accidentally creates one of these public links. They might be trying to share a folder with a single client but, in their rush, click the wrong option.

Now that folder, potentially containing sensitive contracts or financial information, is public. The link can be forwarded, posted online, and sometimes even found by search engines. This is why it's vital to configure these tools so that any new file or folder is private by default.

Sharing should be an intentional act, not the default. Make the secure way the easy way. An employee should take extra steps to share something publicly, forcing them to think about their action. Setting the default to private prevents this entire category of accidental data breaches.

The data shows how widespread poorly configured cloud tools have become:

- Cloud intrusions have increased by 75% in recent years, largely due to simple misconfigurations like publicly exposed data.

- Another 2025 report found that a shocking **99% of organizations have exposed data in their cloud environments**, often due to these misconfigurations.

Common Mistakes to Avoid

As we previously established, getting the big things right is half the battle; the other half is avoiding common mistakes that can undo all your hard work. These seemingly small things create huge openings for attackers.

Assuming the default security in Microsoft 365 or Google is enough.

Many people think the basic security that comes with Microsoft 365 or Google is sufficient. These default filters often aren't good enough to stop well-crafted, targeted attacks, like the fake invoice scams we've discussed.

Attackers know what these filters look for and design their attacks to bypass them. You need an additional layer of security specifically designed to spot these more advanced, targeted threats.

Trusting email for anything involving money.

This is a big one. Email was never designed to be a secure way to move money.

Attackers can easily make an email look like it came from someone you trust. They can fake the sender's name and sometimes even the email address itself, making it very hard to spot. Any time money is involved, you must assume the email could be fake.

Thinking security training alone will stop phishing.

Security training is important; you should absolutely teach your team what to look out for.

However, you can't expect training alone to solve the problem.

People get busy, distracted, and make mistakes. Attackers design their scams to exploit these moments of distraction. A person only needs to make one mistake on one busy afternoon for an attacker to get in.

That's why you need the technical controls we've discussed, like an advanced email filter and a web filter. They are the safety net for when a person inevitably makes a mistake.

What to Ask Your IT Provider

Your job as the owner isn't to do the technical work, but you must hold your IT team or provider accountable. Do this by asking simple, direct questions that require proof, not just promises.

• **"What specific tool are we using for email security that goes beyond the basic built-in filter? How does it protect us from someone clicking a bad link?"**

If they can't explain in simple terms how the tool protects you from a bad link, then it isn't doing its most important job.

• **"Can you configure our email system to put an automatic warning banner at the top of all emails that come from outside our company?"**

This is a simple but incredibly effective control. A banner saying "EXTERNAL EMAIL" at the top of an email constantly reminds your team to be a little more skeptical.

It's especially helpful for spotting scams where an attacker tries to impersonate you or another company leader. It's a simple nudge that can prevent a huge mistake.

• **"Are our company's file-sharing settings in Teams/Google Drive set to 'private by default'? Can you show me the policy that enforces this?"**

This question checks if you're protected from accidental public sharing leaks. The answer should be a simple "yes." The second part, "Can you show me the policy," is where you get the proof.

They should be able to show you a screenshot of the administrative setting that enforces this across your entire company. This confirms it's a real, enforced rule, not just a suggestion.

CHAPTER 8:
DATA PROTECTION

CHAPTER 8:
DATA PROTECTION

Losing your business data in a cyberattack or technical failure can mean the end of your business. This chapter shows you how to keep your data safe and always available.

We'll cover two key areas: confidentiality, which means only authorized people can see your data, and availability, which means you can always access it.

What You Need to Do

Protecting your data comes down to four basic habits. Get these right, and you'll have a strong safety net for your business data.

1. Follow the 3-2-1 Backup Rule.

This simple, proven strategy helps you recover from any data loss.

• Keep at least 3 copies of your data: your live data plus two backups.

• Store those copies on 2 different types of storage, like your server and a separate backup device, or a local device and a cloud service.

• Keep 1 of those copies offsite and completely separate from your main network.

This rule protects you from a single event destroying everything. For example, if a fire destroys your office, your cloud backup remains safe.

The most important part of this rule today is the one isolated copy.

This is your best defense against ransomware. Attackers know businesses use backups, so they often target backups first, encrypting or deleting them before locking your main files.

An isolated copy is one an attacker can't reach from your main network. There are two main ways to achieve this: an "air-gapped" backup or an "immutable" backup.

An air-gapped backup is physically disconnected from the network, like an external hard drive you plug in, use, and then unplug and store safely.

An immutable backup, offered by many cloud backup services, prevents anyone, even you, from changing or deleting a backup for a set period. This protects against ransomware attacks that spread to connected backup drives, like the one in the story we began with.

- **Attackers target your backups.** A 2024 report found that in 94% of ransomware attacks, attackers tried to compromise the victim's backups.

- **Compromised backups slow recovery.** For businesses whose backups were compromised, only 22% recovered in a week or less.

- **Backup failures are common.** One study found that backup errors, including corrupted backups from ransomware, contributed to about one-third of all data loss incidents.

2. Test Your Backup Restores Regularly.

A backup is only good if you can use it. The "Success" message on your backup software doesn't mean you can recover your business. It only means files were copied. You won't know if those files are usable or if you have everything you need until you test a restore.

A restore test is a scheduled drill where you recover files, folders, or even entire systems from your backup.

You don't have to restore your whole company every time, but you do need to test regularly.

These tests help you find problems when the stakes are low. You want to discover a critical folder was missing, a database is corrupted, or a needed software license key is missing during a test, not during an actual ransomware attack.

Plus, doing these drills helps to build your team's muscle memory.

In a real crisis, they'll follow a practiced checklist instead of trying to figure things out for the first time.

- **Untested backups lead to permanent data loss.** While not 100% validated, a study found that nearly 60% of small businesses that lose their data close within six months.

- **Many businesses don't test**. The 2025 Unitrends State of Backup and Recovery Report found that 25% of organizations test their disaster recovery plans once per year or less.

3. Know Where Your Most Important Data Lives.

You can't protect your most important data if you don't know where it is. Just as you know where physical assets are kept in your office, you need to know where your digital "crown jewels" are. This is often harder to track.

Over time, data spreads out. A critical sales proposal might be saved to someone's desktop instead of a shared drive.

An important financial spreadsheet could end up in a personal Dropbox folder. An old customer list might be on a spare laptop in a closet. When data is scattered, it’s hard to protect it.

Files on desktops or in personal cloud folders aren’t backed up by your company system and lack the same security as files on your main server.

Ask yourself these questions:

• Where are our accounting files?
• Where is our main customer database?
• Where are our employee HR records stored?
• Where do we keep our signed contracts and intellectual property?

Once you know where this critical data should live, you can protect it. You can confirm that location is backed up and apply tighter security controls, limiting access to only those who need it. This lets you focus your efforts on what truly matters.

- **Data sprawl is a big problem.** One study found that at over 64% of financial service companies, more than 1,000 sensitive files were accessible to every employee, showing how easily data spreads and how access is often too broad.

- **Most companies don't track data well.** Another study found that only one out of every 10 companies had a good system for labeling files, making it nearly impossible to track sensitive data.

4. Encrypt Devices That Store Company Data.

You must enable the built-in encryption on all company laptops. This is a feature you already have; you just need to turn it on for everyone.

Encryption scrambles all data on the hard drive, making it unreadable without the password.

This is crucial because laptops are often lost or stolen. If an employee leaves a laptop in a coffee shop or it's stolen from their car, an unencrypted device gives a thief full access to your customer lists, financial documents, payroll information, and saved passwords. This is a full-blown data breach.

With encryption, a stolen laptop is just hardware. The data remains safe. This turns a potential disaster, which you'd have to report to customers and your insurance company, into the simple inconvenience of buying a new laptop.

- **Physical device loss or theft is a major risk.** One report found it was a factor in 21% of security incidents . Encryption is a direct solution to this common problem.

- **Most small businesses don't encrypt.** Despite its effectiveness and ease of use, one survey found that only 17% of small businesses encrypt their data. This simple step puts you far ahead.

Common Mistakes to Avoid

Getting the big things right is important, but avoiding a few common mistakes is equally vital. These seemingly small errors can create big security holes.

Keeping your only backup copy connected to the main network.

Hackers are smart. They often target and destroy backups first, then launch ransomware, leaving you with no way to recover.

Your only safe copy must be isolated from your main network, either physically disconnected (air-gapped) or protected in the cloud where it can't be changed (immutable).

Forgetting to back up key data.

This happens often when you don't know where your important data lives. Your main server might be backed up, but a top salesperson could be saving important proposals to their desktop.

Your finance team might have a critical spreadsheet in a personal OneDrive folder.

This data isn't backed up by your company's system. If that laptop dies or the employee leaves, the data is gone. You need to identify your "crown jewel" data and ensure it's saved in centrally managed locations, so it gets properly backed up.

Confusing a cloud sync service with a true backup.

Many people believe that because their files are in Dropbox, Google Drive, or OneDrive, they are backed up. This is incorrect. These are file synchronization services, great for collaboration, but not backups.

If you accidentally delete a file, it's deleted from the cloud. If ransomware encrypts your files, those encrypted files sync to the cloud, overwriting your good copies.

A true backup is a separate, point-in-time copy of your data, protected from such changes. A sync service is not designed to be a safety net.

What to Ask Your IT Provider

These three questions will tell you almost everything about your data protection.

- **"When was our last full restore test? How long did it take, and can I see the report?"**

This is a direct accountability question. Don't accept "we run backups every night." You need to know about the restore.

The answer should be specific, like: "We did a test last quarter. We restored the main file server. It took four hours, and here's the one-page summary of the results." This proves they are testing and gives you a real idea of how long you'd be down in a crisis.

- **"Show me how our offsite backup copy is protected from a ransomware attack. Is it offline, or 'immutable'?"**

This question addresses the biggest threat to your recovery plan. If offline, ask them to describe the physical process. If immutable, ask them to show you the setting in the cloud backup service that confirms it can't be deleted. This confirms you have a safe copy an attacker can't destroy.

- **"Can you provide me with a list of the critical data locations that are being backed up to confirm we haven't missed anything important?"**

This addresses the "know your data" problem. Give your IT provider a list of your most important data locations—the accounting folder, customer database, contracts drive. They should return with a report or screenshot showing these exact locations are included in the backup job.

CHAPTER 9:

NETWORKS & CLOUD BASICS

CHAPTER 9:
NETWORKS & CLOUD BASICS

Your business network is like the nervous system of your company. It connects everything: your employees' laptops, your servers, and your cloud services.

If an attacker breaches this network, you know what comes next… your entire business is at risk. Yes, this can be said for most of the topics we discussed, and it’s true for your network as well.

This chapter will show you how to set up a secure "floor plan" for your network and cloud services, creating separate, secure zones. This prevents problems in one area from spreading to your whole company, keeping your data private and protected.

What You Need to Do

To manage your network and cloud services securely, focus on these three habits. They prevent most of the problems.

1. Segment Your Network.

Think of your network as an office building. You wouldn't let a visitor from the lobby walk freely into your server room. The same applies to your computer network.

Network segmentation means putting up walls inside your network to create separate, secure zones.

At a minimum, create a separate Wi-Fi network for guests. This guest network should only allow internet access and be completely isolated from your main business network. This simple step stops threats like malware on a guest's laptop from reaching your company's systems.

For even better security, use three separate zones:

- A main network for trusted, company-managed computers.
- A guest network for visitors, with internet-only access.
- A third network for less-secure devices like smart TVs, security cameras, or employees' personal phones.

This segmentation contains threats. If an attacker compromises your smart TV, they can't use it to attack your main server. It limits damage. Without these internal walls (a "flat network"), attackers can move freely—known as "lateral movement"—to find your most valuable data. Segmentation makes this much harder.

- **Attackers rely on moving around.** A 2025 report found that 41% of attacks used excessive privileges for lateral movement and to cause more damage. Segmentation directly blocks this tactic.

- **It protects you from things you can't control.** You can't control the security of visitors' laptops or employees' personal phones. Segmentation gives them internet access without exposing your business to device risks.

2. Secure Your Remote Access.

As more employees work remotely, how they connect to your company's systems becomes a major target for attackers. You must lock down these digital doors.

Never expose tools like Remote Desktop Protocol (RDP) directly to the internet. RDP is a built-in Windows tool for remote computer control. Exposing it to the internet is like plastering a “hack me” sign over your business.

Ransomware gangs use automated tools to scan the internet 24/7, looking for this mistake.

They will find your open RDP server and use other automated tools to guess the password. If they get in, they have full control of your server, and a ransomware attack is often hours away. All remote employee access should go through a modern, secure gateway that requires multi-factor authentication (MFA).

This means even if an attacker steals an employee's password, they can't log in without the employee's phone to approve access.

- **This is a primary target for ransomware.** Microsoft repeatedly states that unprotected RDP is a top attack method ransomware gangs use to enter businesses.
- **It's a very common entry point.** Studies show that exposed remote access services are the initial entry point for over 50% of ransomware deployments.

3. Set Cloud Services to "Private by Default."

When using cloud services like Microsoft 365, Google Drive, or Dropbox, understand your security responsibilities.

The provider (Microsoft, Google, Amazon) secures the cloud itself—physical data centers, servers, and core networks. You are responsible for security in the cloud—how you set it up, who has access, and how you protect your data.

The biggest cloud mistake comes down to simple human error, like many things in cybersecurity.

An employee, in a hurry to share a folder with a client, clicks "share with anyone" or "public link." They've just made that folder, and everything in it, public. Anyone with the link can access it without a password or login.

This is why you must set a rule: any new cloud storage—a new SharePoint folder, a new site, a new Amazon S3 "bucket"—must be created with the most secure, private settings.

Access should never be open by default. You should grant access deliberately, one person at a time. The secure way should be the easy way; the risky way should require extra steps and approvals.

This mistake is the most common cause of massive cloud data breaches. An employee doesn't mean to leak your customer list or financial projections, but if the default is "public," it's incredibly easy to do accidentally.

Setting the default to "private" prevents this type of data leak. It's a simple change that acts as a powerful safety net against everyday human error.

- **Cloud misconfiguration is a huge problem.** A 2025 report from Palo Alto Networks found that 40% of cloud incidents came from unmonitored assets and shadow IT, often including misconfigured folders.

- **Most breaches now involve the cloud.** Data clearly shows this is where the risk is. A 2025 IBM report found that 72% of data breaches involved cloud-stored data.

Common Mistakes to Avoid

Getting the big things right is crucial, but avoiding these common mistakes is just as important. They may seem small but create huge openings for attackers.

Assuming your cloud provider manages all your security.

This is a costly misunderstanding. When you use services like Microsoft 365 or Google Workspace, you're in a "Shared Responsibility Model." The provider secures the cloud itself—physical data centers, servers, and core networks.

You are responsible for security in the cloud—controlling access, permissions, and data sharing. The cloud provider gives you the security tools, but you must use them.

Using a shared password for your main Wi-Fi network.

This is another convenience-driven mistake that creates big risks. If you have one password for your main company Wi-Fi and give it to every new employee, what happens when an employee leaves? To revoke their network access, you must change the password, then update every device in the office.

This is a huge hassle, so it rarely happens. This means an ex-employee could potentially connect to your internal business network months or even years later.

Modern Wi-Fi systems solve this by letting each employee log in with their unique username and password, the same one they use for their computer. When they leave, you simply disable their account, and their Wi-Fi access is gone.

What to Ask Your IT Provider

These three questions will tell you almost everything you need to know about how well your network and cloud services are managed.

- **"Is our guest Wi-Fi network completely separate from our main business network? Can you show me the configuration that proves it?"**

This is a yes or no question.

They should show you a screenshot of firewall rules or network configuration clearly blocking traffic from the "Guest" network to the "Internal" network. This is a simple visual confirmation that the wall is in place.

- **"Do we have any services, especially Remote Desktop (RDP), exposed directly to the internet? I need confirmation that all remote access is routed through a secure, managed gateway."**

This confirms they've closed the most dangerous door and replaced it with a secure one requiring multi-factor authentication.

- **“What is our process for ensuring a new folder or site in SharePoint is created with private, not public, settings by default?"**

This checks if you're protected from accidental cloud data leaks. The IT provider should show you the administrative setting in Microsoft 365 or Google Workspace that enforces this for all users company wide.

It shouldn't be a suggestion to employees; it should be a technical control that makes the secure option the default. This proves they manage your cloud environment proactively, not just reacting to problems.

CHAPTER 10:

VENDOR & THIRD-PARTY RISK

CHAPTER 10:
VENDOR & THIRD-PARTY RISK

All businesses rely on outside partners and vendors to function. Each of these connections is a potential entry point for cyber attackers, even if your own security is strong.

A problem at one of your vendor's companies can quickly become a disaster for your business.

This chapter will show you how to manage these risks. The goal is to understand the risks each partner brings and to set up simple ways to check their trustworthiness and limit their access to only what's necessary.

What You Need to Do

You need to develop four basic habits to manage the risks that come with your partners. If you do these four things well, you'll have a strong, sensible way to protect your business from its supply chain.

1. Sort Your Vendors by Risk.

First, identify all your vendors. In security, a "vendor" or "third party" is any person, company, or software service that connects to your business or handles your data. This includes your IT provider, payroll company, accounting software, CRM for sales, and even your marketing newsletter tool.

Once you have this list, sort them. You can't treat your coffee supplier the same way you treat the company that has access to your server. This isn't efficient or necessary. The goal is to put them into simple groups so you can focus your attention where the risk is highest. To do this, ask two questions for each vendor:

• How critical are they to your daily operations? If they stopped working for a day, would it be a minor or major problem?

• How sensitive is the data you're giving them? Are they just getting your public address, or are they getting your employees' personal information and your company's financial data?

This will naturally group your vendors.

Your "high-risk" vendors are those that are critical to your business and that handle your most sensitive data. This list will be short. It typically includes your IT provider, payroll provider, and perhaps your main accounting or operational software.

These are the partners that, if they had a problem, could put you out of business. These are the only ones you need to spend significant time on. All other vendors fall into a lower-risk category.

2. Ask Basic Security Questions Before You Sign a Contract.

Once you know who your high-risk vendors are, talk to them about security.

For any new high-risk vendor, have a short, simple list of questions to ask before signing the contract. You're just trying to confirm that they take security as seriously as you do.

Here are some good, direct questions to ask:

- Do they use multi-factor authentication (MFA) for all employees who access your data?
- Do they have a consistent process for installing security updates on their systems?
- How do they protect your data when they store it? Is it encrypted?
- What happens if they have a security problem? How quickly will they tell you about it?

This is very important because a problem at your vendor's company can quickly become your problem.

- Data shows that **15% of all breaches in 2024 involved a third party**, a 68% increase from the previous year.
- Another study found that **59% of companies have experienced a data breach caused by one of their third-party vendors**.

3. Give Vendors Limited and Time-Based Access.

You must strictly enforce this rule. When you give an outside person or company access to your systems, do it in a very specific way.

First, never use shared accounts. It's common for a business to create one login, like "IT_Vendor_Admin," and give the password to their entire IT support team. This is a big mistake. If something goes wrong—a file is deleted, a setting is changed that crashes your system—you have no idea who did it.

You only know it was someone from the vendor. This means no accountability. The rule must be simple: every single outside person who needs access to your systems gets their own unique, named account. That way, if "john.smith@itvendor.com" makes a change, you know exactly who it was.

Second, that account should be limited to only what they need for their job. This is the "principle of least privilege" we've discussed before, but it's even more important for outside vendors.

If you've hired a company to work on your website, their account should only give them access to the website server, not your main file server or your accounting software. This is how you limit the damage if that vendor's account is ever compromised.

Finally, every vendor account must have a set expiration date. If you hire a contractor for a three-month project, their account should automatically turn off on the last day of that project.

This is critical because it's easy to forget to remove a vendor's access when their work is done. These old, forgotten accounts, often called "ghost users," are a huge security risk.

This is important because it closes one of the most common security loopholes in business. When a project ends, nobody thinks about the login that was created for it. It just sits there, active and unmonitored, sometimes for years. An attacker who compromises that old account can get into your network while appearing to be a legitimate, if old, partner, making them much harder to spot.

- **Forgotten accounts are a massive problem.** A 2025 report found that a shocking 88% of organizations have these stale "ghost user" accounts in their systems, waiting to be exploited.

4. Include Security in Your Contracts.

The conversations you have with your vendors about security are important, but you need to put those promises in writing. The best way to do that is by adding a simple security clause or a one-page addendum to your contracts with your high-risk vendors.

This is important because it makes security a formal, legal obligation. It sets clear, written expectations for how they will protect your data and what will happen if they don't.

Your security addendum doesn't need to be a 50-page legal document. It just needs to cover a few basic, common-sense points.

It should require the vendor to maintain reasonable security practices, like the ones we've talked about in this book—using MFA for their employees, keeping their systems updated, and encrypting your data.

But the single most important part of this contract clause is the breach notification requirement. Your contract must state that if the vendor suffers a data breach that affects your data, they must tell you about it within a specific, short timeframe, like 24 or 48 hours.

The longer it takes for you to find out about a breach at your partner's company, the more damage an attacker can do to your business. A fast notification gives you a chance to react, to shut off their access, change passwords, and protect yourself before the problem spreads.

- **The time to contain a breach is critical.**

Data clearly shows that breaches identified and contained in under 200 days cost, on average, $1.39 million less than breaches that take longer to find. A contractual requirement for fast notification can save you a huge amount of money.

- **Breaches involving stolen credentials take the longest to find.**

The average time to identify and contain a breach that starts with a stolen password is a full 292 days. If that stolen password belongs to your vendor, you might not know about the problem for months unless they are legally required to tell you.

Common Mistakes to Avoid

Getting the big things right is half the battle. The other half is avoiding a few common mistakes that can undo all your hard work.

Assuming a vendor is secure because they are a well-known brand.

It's easy to assume that a big, well-known company has perfect security. But that's a dangerous assumption. Big companies get breached all the time. In 2023, a single vulnerability in a popular file transfer tool called MOVEit led to breaches at thousands of organizations, including many household names.

In 2025, we've already seen major breaches involving huge companies like PowerSchool and Oracle Health, where a single problem at the vendor affected millions of people. When you connect your business to a vendor, you inherit their security risks, no matter how big they are.

You must do your own basic checks and ask your own questions.

Signing up for new software services without any security review.

This is often called "Shadow IT." An employee needs to solve a problem, so they do a quick Google search, find a new software tool, and sign up for it with the company credit card. They've solved their problem, but they've also just created a new security risk.

You now have sensitive company data, maybe a customer list or some financial information—being stored in a service you don't know about, don't manage, and haven't checked for security. You can't protect data you don't know you have.

What to Ask Your IT Provider

These three questions will tell you almost everything you need to know about how well your vendor risk is being managed.

- **"Can you give me a list of all non-employee accounts with access to our network? Let's review who owns them and when their access is set to expire."**

For every account on that list, there should be a name of a current employee who is responsible for it (the "owner") and a date when that account's access will automatically turn off.

- **"What is our process for reviewing the security of a new software tool before a department starts using it?"**

It should be a simple, fast process where, if a team wants to use a new tool, they fill out a short form, and your IT provider does a quick, 15-minute check to make sure the tool is reasonably secure before any company data goes into it.

- **"Let's say one of our high-risk providers had a security breach. Walk me through the exact steps we would take to immediately disable their access to our systems."**

This is the ultimate "what if" question. It tests their preparedness for a worst-case scenario. They should have a documented "kill switch" plan that details the exact steps they would guide you through to immediately lock them out of your systems to contain the damage.

PART III

CHAPTER 11:

INCIDENT RESPONSE & BUSINESS CONTINUITY

CHAPTER 11:
INCIDENT RESPONSE & BUSINESS CONTINUITY

At the risk of sounding gloomy, I have to state the obvious: a cyberattack could devastate your business leading to lost revenue, a damaged reputation, and legal issues.

That's obviously something you don't want to happen. Unfortunately, sometimes it does. And even more unfortunate, many small businesses lack a clear plan for what to do when an attack happens, leaving them vulnerable.

The good (or reassuring) news is, this chapter will show you how to create a simple, actionable plan to protect your business and keep it running, even during a crisis.

Your plan should have two key parts that people often confuse, but they serve different purposes.

First is your **Incident Response plan**. This is your "firefighting" strategy. It focuses on the technical problem: stopping the attack, finding out how it happened, and fixing the damage. It's all about containing the problem and getting your systems back to a safe state.

Second is your **Business Continuity plan**. This plan focuses on your business operations. It explains how you'll keep taking orders, serving customers, and making payroll while the technical problem is being fixed.

For example, if your main server is down, how will you still ship products? If your accounting system is locked, how will you send invoices? This plan keeps your business functional and money coming in, even when your technology isn't working.

An "incident" is any event that threatens your ability to operate or protect your data. This could be a ransomware attack, a server crash, critical software failing, a stolen laptop with sensitive data, or even a power outage. If it impacts your money, your data, or your customers, treat it as an incident and start your plan.

Step 1: What to Do Before Anything Happens (Preparation)

Your preparation largely determines how well you'll handle an incident. A good plan is a short, simple guide you can use fast, when needed.

Print it out and keep copies in safe, accessible places: in your desk, at home, even in your car. This way, you can get to it even if your office is inaccessible or your computer network is down.

A. Name Your Contacts

Your plan needs a simple list of names and phone numbers. No one should have to guess who to call when something goes wrong.

This list should be the first page of your plan. It needs to name the specific people who will form your small incident response team. You only need to cover three main roles, and one person can fill multiple roles.

- **The Leader:** This person manages the overall response. They make big business decisions, like whether to shut down a system or communicate with customers. This is usually you, the owner, or another senior leader.

- **The Technical Contact:** This is the first person anyone in the company calls if they see something strange. They start the technical investigation. This could be your internal IT person or your main contact at your IT provider/MSP.

- **The Business/Comms Contact:** This person manages communication with employees and customers and finds ways to keep the business running. They handle the business continuity side of things.

For each person, list their name, their role, and their personal cell phone number. Don't just list an office extension. In a real crisis, your phone system might be down, so you need a direct way to reach them.

Your contact list should also include key outside parties.

- **Your Cyber Insurance Provider:** If you have a cyber insurance policy, this should be your very first phone call. Seriously. Do it right away. Most policies give you access to a 24/7 hotline with a team of experts—forensic investigators, lawyers, and crisis managers—who will guide you through the process. Calling them immediately is often a requirement for your claim to be valid.

- **Law Enforcement:** You should report the incident to your local law enforcement. Depending on where you are, you may also need to report it to national or regional cybercrime authorities. This is important for the investigation and for meeting any legal obligations you might have.

- **Your Lawyer:** Have the contact information for your company's legal counsel on this list. You will need their advice on your legal and regulatory responsibilities, especially if customer data was involved.

B. Know Your Critical Operations

This is the business continuity part of your preparation. Sit down with your team and list the parts of your business that must keep running.

Ask questions like:

- If our main server goes down, how do we keep shipping products?
- If our accounting system is locked, how do we send invoices and make payroll?
- If our customer relationship management (CRM) software is offline, how does our sales team track leads and orders?

For each critical operation, figure out a simple, manual workaround. If the shipping system is down, can you switch to paper work orders for a day or two?

If the accounting system is offline, do you have a way to create basic invoices from a template?

Having these fallback plans ready keeps your business from stopping completely while the technical problem is fixed. This list also tells your technical team what to recover first.

C. Create the "Stop and Call" Rule for All Staff

This is the most important rule to teach everyone in your company. If you see anything strange on your computer, stop what you are doing and immediately call the technical contact on your list.

Don't try to fix it yourself. Don't finish that email. Don't assume it's just a glitch. Just stop and call.

This is vital because, in a modern cyberattack, speed is everything. Attackers use automated tools that can spread through a network in minutes. A recent Palo Alto Networks report found that in nearly one in five cases, attackers were stealing data within the first hour of getting into a network.

An employee noticing something strange and reporting it right away is often your only chance to contain the problem before it becomes a company-wide crisis. An employee trying to "just finish one more thing" can be the difference between a problem on one laptop and a ransomware attack that takes down your entire business.

D. Don't Rely on "Heroics"

When you write this plan, don't rely on one person. It's easy to think, "We'll just call Bob," because Bob is your IT genius who knows everything. But that creates a single point of failure. What if the incident happens at 2 AM and Bob's phone is off? What if he's on vacation?

Your plan needs to be a simple checklist that any manager in your company could pick up and follow for the first hour. It should be clear enough that they can make good basic decisions even under stress.

This is even more important with the widespread shortage of cybersecurity skills. Data shows that breaches at companies with a high security skills shortage cost millions more than those without this problem.

You can't let your entire response depend on one person’s availability and expertise. The goal is to create an orderly, repeatable process anyone can follow, not to rely on one specific person to save the day.

Step 2: What to Do During an Incident (Action)

An incident has just been reported. Someone on your team followed the "Stop and Call" rule.

This is where your preparation pays off. The goal now is to move from reacting to acting, following the simple playbook you've already created.

A. Contain the Problem

Your first job is to stop the problem from getting worse. Think of it like a fire: you have to put it out before you can rebuild. In a cyber incident, this is called containment, and speed is key.

The first priority is to isolate the affected computers, without turning them off. If an employee's laptop is acting strangely, your technical contact should immediately take it off the network. Unplug the network cable. Turn off the Wi-Fi. But keep the device powered on.

This stops the problem from spreading from that one computer to your server or other office computers.

Next, change any passwords that might have been compromised. If the incident started on an employee's computer, assume any passwords they used or saved on that machine are now in the attacker's hands.

Their main network password, email password, and any other important accounts need to be changed right away.

Finally, stop any automated processes that could worsen the problem. For example, if you have a system that automatically syncs files between your server and a cloud service, you might need to pause it. Otherwise, it could sync encrypted files from a ransomware attack to your cloud storage, overwriting your good backups.

One more critical point on containment: **you MUST preserve evidence.**

The first instinct in a crisis is to start shutting things down and cleaning things up. You have to fight that urge. The affected computers are now a crime scene, and you need to treat them that way.

Don't turn anything off unless your technical expert tells you to. A lot of important evidence lives in a computer's active memory and disappears the second you pull the plug.

Keep a simple log of every action you take, with the time and the name of the person who took it. This will be incredibly important for the investigation and for any insurance or legal claims later.

• **Speed is everything**. Data clearly shows this. A 2025 Palo Alto Networks report found that **in nearly one in five cases, attackers were stealing data within the first hour of getting into a network**. Your ability to quickly contain the problem prevents a small incident from becoming a major data breach.

B. Keep the Business Running

While your technical team is fighting the fire, you need to keep the business running.

Imagine a manufacturing company hit with ransomware on a Friday morning. All their design files and work orders are encrypted. The business is stuck. But because they had a simple, practiced plan, the team knew what to do.

The floor manager immediately told the operations team to switch to their backup system: paper work orders. They kept production lines moving, just at a slower pace. It was still a huge problem, but not a complete disaster. They could still serve their most important customers because they had a simple, manual workaround ready.

This is what a business continuity plan looks like in the real world.

What's your version of paper work orders? How do you keep taking orders if your main system is down? How do you send invoices? Having these answers ready keeps money coming in during a crisis.

C. Control Communications

Silence is dangerous when under a cyberattack. It creates rumors, fear, and panic. If you don't provide information, employees and customers will make assumptions, usually the worst ones.

You must be the single, trusted source of information.

You don't need all the answers, especially in the early hours. But you need to communicate what you do know, and do it regularly.

Tell your staff and key customers three simple things:

- What you know so far (e.g., "We have a system outage affecting our ability to process orders.")
- What you're doing about it right now (e.g., "Our technical team is finding the problem, and our operations team is switching to our manual ordering process.")
- When you will update them again (e.g., "We will update you in one hour, or sooner if we have major news.")

This shows you are in control, even if the problem isn't solved yet.
To do this effectively, choose one communication channel that isn't dependent on your company's systems.

This could be a private text message group for your leadership team, or a personal email list for all employees. Your company's email or chat system might be down, so you need a reliable way to reach everyone.

Step 3: What to Do After It's Over (Review)

Once the fire is out, systems are restored, and business is back to normal, it's tempting to just sigh with relief and move on. But this is one of the most important parts of the whole process.

You must take time to learn from what happened.

Don’t rush to find someone to blame, though. You need a "no-blame" review to make the business safer, not to punish mistakes. Just gather your small incident response team for a short meeting and ask two simple questions:

• What was the root cause of the problem?

Dig past the surface-level answer. Did an employee click a phishing link? Did an attacker get in through an unpatched server? Did someone use a weak, stolen password on a remote login without multi-factor authentication (MFA)?

You need to find the actual unlocked door so you can lock it properly.

- **What one or two things can we change to stop this from happening again?**

You focus on the one or two changes that would have made the biggest difference. If the problem was a phishing email, maybe the change is a better email security tool. If it was an unpatched server, maybe the change is a more consistent patching schedule.

The UK's 2025 Cyber Security Breaches Survey found that after an incident, the most common change businesses made was to provide additional staff training or communications. Whatever it is, identify it, assign it to someone with a deadline, and follow up to make sure it gets done.

You Must Practice This Plan

A plan that just sits in a binder is useless. The only way to know if your plan works is to test it.

The best way to practice is with a simple, one-hour "tabletop exercise." This is a meeting where you and your small incident response team talk through a fake crisis. It's a fire drill for a cyberattack.

Schedule a one-hour meeting. Get your leader, technical contact, and business contact in a room. Then, present them with a simple, realistic scenario.

"It's 9 AM on a Tuesday. An employee calls and says there's a strange message on their screen demanding Bitcoin payment, and none of their files will open. It looks like we have a ransomware attack. What do we do right now?"

Then, talk it through, step by step. Who calls whom first? What's the first thing the technical person does? How do we tell the rest of the staff what's going on? What's our plan for keeping the business running if the main server is offline?

Talking it through calmly helps you find holes in your plan. You might discover that the contact number for your IT provider is wrong, or that the person making a key decision is on vacation with no backup, or that your plan to switch to paper work orders won't work because the templates are on the encrypted server.

- **Testing your plan saves a lot of money.** A 2025 IBM report found that companies regularly testing their incident response plans save an average of $1.49 million per breach compared to those that don't.

- **A lack of planning is expensive.** The same study found that companies with no formal, tested incident response plan paid 58% more per breach than those that were prepared.

- **Most businesses aren't doing this.** Despite the clear financial benefit, most companies skip this step. One report found that only 30% of organizations regularly test their incident response plans. By doing this simple, one-hour exercise a couple of times a year, you will be far more prepared than most of your peers.

CHAPTER 12:

COMPLIANCE & GOVERNANCE FOR SMBS

CHAPTER 12:
COMPLIANCE & GOVERNANCE FOR SMBS

Now we're getting in the weeds. Compliance is a boring topic I'm sure you don't want to hear about.

It's overwhelming and often filled with unfamiliar jargon. Which is exactly why this chapter simplifies compliance and governance, turning them into manageable steps.

First, let's clarify what these terms mean. While often used interchangeably, they have distinct roles:

• **Security** is the actual work you do to protect your business. This includes installing modern endpoint protection on laptops, testing backups, and teaching your team to spot phishing emails. It's like the locks on your doors and the cameras in your warehouse.

• **Compliance** is the work you do to prove you're following specific rules. These rules might come from laws (like privacy regulations), industries (like credit card payment rules), or large customers who want to confirm you're a safe business partner.

It's the cybersecurity equivalent of showing the fire inspector your sprinkler system's maintenance records.

• **Governance** refers to who is responsible for security, how decisions are made, and how work is checked. It ensures someone is accountable for security and that you regularly review progress.

You need all three.

Good security without proof makes it hard to land big customers. And compliance paperwork without actual security is a house of cards.

The following pages will help you build a simple, practical system that delivers all three without excessive paperwork.

A Simple, Practical Plan

You don't need a team of compliance experts to achieve this. You just need a practical plan built on a few common-sense habits.

A. Use Your Framework as a Guide

You don't (and shouldn't) have to start from scratch.

Remember Chapter 4, where we discussed security frameworks? That framework is your guide.

It lists the essential steps to protect your business and the things you'll eventually need to prove you're doing.

Whether you use the CIS Controls or the NIST Cybersecurity Framework, the idea is the same: pick one guide and follow it.

You only need one good framework to structure your program and keep you focused.

B. Name an Owner

While "governance" sounds formal, for a small business, it means naming one person on your team responsible for security. This doesn't have to be a full-time role; in most small businesses, it's a part-time responsibility.

However, someone must own it. Someone needs to be in charge of making sure backups are tested and security updates are installed. If "everyone" is responsible, then no one is. Just by naming an owner, you're already ahead of many businesses where board-level responsibility for cybersecurity has declined, as noted by the UK's 2025 Cyber Security Breaches Survey.

C. Set a Regular Rhythm

Once you have an owner, set a regular schedule to check in on the security work. A short, 30-minute monthly check-in with the security owner and perhaps your finance or operations lead is enough.

In this meeting, ask these three simple questions:

1. "**What changed in the business this month?**" Did you hire new people? Start new software? Sign a new customer? Any business change can create a new security risk, so discuss it.

2. "**Did we have any security issues or near-misses?**" Did anyone report a convincing phishing email? Did a security tool send an alert? Discussing near-misses helps you find and fix small problems before they become big ones.

3. "**What are we checking this month?**" You can't check everything every month. Pick a few items. For example, this month, review the report showing all laptops are encrypted. Next month, check the log from your last backup restore test.

The "Show Your Work" Habit (Your Documentation)

Documentation often makes business owners groan, but it doesn't have to be a huge, time-consuming project.

You need to get into the habit of "showing your work" as you go. This is what you'll present when a large customer or your insurance company asks for proof of your security.

You only need 3 items:

• **Policies**: These are short pages stating "what we do." For example, a one-page policy might say, "All employees must use multi-factor authentication on their email accounts, and all company laptops must be encrypted." It's a clear statement of your rules.

• **Procedures:** These are step-by-step instructions on "how we do it." For instance, a one-page guide with screenshots could show a new employee how to set up MFA on their phone.

• **Evidence:** This is the most important part: proof that you're doing what you say you do. It's a collection of screenshots, reports, and logs from your security tools.

It could be a screenshot from your Microsoft 365 dashboard showing MFA is enabled for all users, a report from your backup system confirming a successful restore test, or notes from your 30-minute monthly meeting.

When you complete a control check, like a restore test or an access review, save the proof in a folder named with the year and month, like "2025-10 Proofs."

Then, in your monthly meeting notes, add a one-line note saying, "Completed quarterly restore test, report saved in the proofs folder."

It takes an extra two minutes, but when an auditor asks you a year from now to prove you did a restore test, you'll have a clean, dated trail of evidence ready.

Handling Audits & Questionnaires

An audit is simply someone checking your work. Whether it's your cyber insurance company, a potential customer, or a regulator, they're asking you to prove you're taking basic, sensible steps to protect your business.

If you've followed the "show your work" habit, this process becomes incredibly simple. When an auditor asks, "Do you have a policy for multi-factor authentication?" you provide the one-page policy you already have.

When they ask, "Can you prove that all of your employees are using it?" you go to your "proofs" folder, grab the screenshot from last month's check, and hand it over. This shows you're professional, organized, and that your security program is a real, active part of your business.

The same applies to long security questionnaires from big customers. Your framework is your answer key. The questions they ask will almost always align with the basic controls in your framework. You can create a simple document with standard answers to common questions, based on your policies. The first time you fill one out might take a while, but subsequent times will be much faster because you've already done the work and saved the answers.

A Quick Note on Privacy

If your business collects any personal data—which almost every business does, even just employee information—you are responsible for protecting it. This issue is growing in importance, and rules are becoming stricter.

You don't need to be a lawyer to grasp the basic principles:

- Be clear about why you're collecting data.
- Get permission when necessary.
- Only keep the data you need for your business.
- Securely dispose of data when you no longer have a good business reason to keep it.

A simple privacy notice on your website explaining these points is a good start. However, this is an area where you should consult a lawyer. Specific rules can vary significantly based on where you do business and where your customers are located. For example, if you have European customers, you must comply with GDPR. If you have California customers, you must comply with CCPA.

The fines for non-compliance can be substantial. The average cost of a data breach is already high, but for businesses with high non-compliance, that cost is, on average, 12.6% higher. A short conversation with a knowledgeable lawyer can prevent major problems later.

How to Make This a Manageable, Ongoing Process

To tie all this together and maintain it month after month, use one final tool: a "control register."

This is a spreadsheet listing all your key security controls. It's your master to-do list for your security program, with columns for:

- What is the control? (e.g., "Backup Restore Test")
- Who is the owner? (e.g., "Our IT Provider")
- How often do we check it? (e.g., "Quarterly")
- Where is the proof? (e.g., "The 'Proofs' folder")

Use this list in your 30-minute monthly meeting. The security owner pulls up the list, sees which checks are due that month, and asks the owner for proof.

Don't wait until a customer or regulator asks for proof to start collecting it. That's the biggest mistake you can make. Trying to gather a year's worth of evidence afterward is a time-consuming, stressful nightmare and looks unprofessional. You might not even find the proof you need. It’s much better to spend a few minutes saving a screenshot each month.

CHAPTER 13:
CONCLUSION

CHAPTER 13:
CONCLUSION

My goal for this book was to give you a clear, workable path to protect your business without turning you into a security expert.

My hope is that you have found it helpful, and that you now have a better understanding of what cybersecurity is, and most importantly, what it takes to secure your business against threats (hackers).

As you've seen, most security wins don't come from buying the most expensive complicated tools. They come from doing the basics well, repeatedly.

With that in mind, if you walk away from this book with just a few key ideas, I want them to be these:

- **Control the Access.**

You must be in control of who has the keys to your business. That means you use multi-factor authentication everywhere, no exceptions.

It's the single most effective thing you can do (and you can do it as soon as today). It means you have a list of all the devices that are used for work, and you make sure they're secure.

And it means you take away admin rights from your employees for their day-to-day work. It's not rocket science, and it's important.

- **Know Where Your Data Is.**

You can't protect your most important information if you don't know where it is. You need to define the specific, "allowed homes" where your sensitive data can be stored, like a specific folder on the server or in your accounting software.

And you need to stop public file sharing by default. A simple misconfiguration in your cloud storage is one of the most common ways businesses leak huge amounts of data. And that's something you don't want to happen to you.

- **Have a Plan for When Things Go Wrong.**

I don’t mean to be pessimistic, but something will eventually go wrong. It's not a matter of if, but when.

What will make the difference between a manageable problem and a disaster is having a plan.

That means you practice restoring your data from your backups, so you know for a fact that it works. It means you run short, one-hour tabletop exercises to rehearse your incident response plan.

And it means you keep that plan to a single page, with the names and phone numbers of the people you need to call right at the top (Cyber Insurance Provider, IT Provider, Lawyer, Law Enforcement, etc.).

- **Separate Your Networks.**

Your network shouldn't look like one big open room. You need to put up some simple walls in there.

At a bare minimum, you need to keep your guests on a separate Wi-Fi network from your business. You should also put other less-secure devices, like smart TVs and security cameras, in their own separate zone.

This is what prevents a problem on a guest's laptop from spreading to your main server.

- **Manage Your Vendor Risk.**

A problem at your vendor's company can quickly become your problem. You need to sort your vendors by risk and focus your attention on the ones that are critical to your business.

For those high-risk vendors, you need to require them to use unique, named accounts that have an expiration date.

And, where possible, you need to use a simple security addendum in your contracts that makes them legally obligated to tell you if they have a security incident.

- **Get Proof, Don't Just Assume.**

You can't just hope that your security is working. You must check. This is the "show your work" habit.

It just means you get into the routine of saving dated reports and screenshots each month as evidence that your controls are working. It's the report that shows all your laptops are encrypted. It's the screenshot that shows all your employees use MFA. And it means you make sure your written policies are short, simple, and match what you do in the real world.

Last but not least… **Security is a habit.**

This is the most important mindset shift you can make. Security isn't a project. A project has a beginning and an end. You don't "finish" security.

It's a habit, a routine, just like doing your bookkeeping, managing your inventory, or locking up the office at night. It's a normal, ongoing part of running a professional business. It's made up of short meetings, small, regular adjustments, and a simple habit of keeping records.

When you treat security like that, it stops being this big, scary, overwhelming thing. It just becomes a series of small, manageable tasks. You check your backups. You review who has access. You make sure your software is up to date. I say "you," but that can (and should) be handled by your IT Provider/MSP.

The real value of this routine shows when something eventually does go wrong. Because you have a plan and you've practiced it, your team can respond with a clear order of steps instead of panicking.

They'll know who to call, what to do first, and how to keep the business running. That preparation has a massive, measurable financial impact. I already mentioned this, but I'll do it again to really drive the point home: IBM found that companies that regularly test their incident response plans **save an average of $1.49 million per breach compared to those that don't**. And the same study found that companies with no formal tested Incident Response Plan paid 58% more per breach than those that were prepared.

ONE LAST THING BEFORE YOU GO

If you've made it this far, nicely done.

Most business owners never take the time to really think through cybersecurity and the steps needed to implement it properly. You've invested the time, and now you have a clear picture of the necessary steps to secure your business against modern threats.

As a thank you for reading and taking your security seriously, I want to offer you a personal **Reader's Bonus**: **a free, 30-minute advisory call with me.**

Sometimes, even after reading a book, you just need a quick conversation to make sure you're starting on the right foot. This call is a chance for you to ask me anything that's top-of-mind about your security.

During our chat, we can focus on whatever is most critical to you right now. I can help you:

- **Prioritize** the next one or two high-impact security habits for your business.
- Figure out the single biggest **low-hanging fruit** security weakness you need to fix right away.
- **Get clear answers** on any topics from this book that might still be confusing.

To schedule your call, just reach out:

Thank you for reading, and I wish you all the best in securing your business!

JACK RAMSEY
Co-Founder | CEO
209-920-4077 | jack@rj-pro.net | rj-pro.net
1919 Vista Del Lago Drive, Suite 3
Valley Springs, CA 95252

RJ PRO TECH GROUP
INNOVATIVE I.T. SERVICES

CHAPTER 14:
LEGEND (JARGON DECODER)

Welcome to the cybersecurity jargon decoder!

I put this final chapter together to help you make sense of some of the most important and commonly used terms in the industry. It'll come in handy as you implement what you learned in this book and when dealing with IT providers, insurance companies, and vendors.

Authentication

The process of proving you are who you say you are, usually with a password or code.

Botnet

A network of infected computers controlled by a criminal to launch large-scale attacks like sending spam or knocking websites offline.

Business Email Compromise (BEC)

A scam where a criminal impersonates a trusted person via email to trick an employee into sending money or sensitive information.

Cloud Computing

Using someone else's computers and storage over the internet instead of owning and managing your own.

Compliance

The work you do to prove you are following a specific set of security or privacy rules required by laws, industries, or customers.

Cyber Insurance

An insurance policy designed to help your business cover the costs of recovering from a cyberattack.

DDoS (Distributed Denial-of-Service) Attack

An attack that knocks a website offline by flooding it with so much junk traffic that it can't respond to legitimate customers.

Encryption

The process of scrambling your data so it's unreadable to anyone without the correct "key" to unscramble it.

Endpoint Detection and Response (EDR)

A modern version of antivirus that actively watches for suspicious behavior on your computers, not just known viruses.

Firewall

A digital security guard that stands between your internal business network and the public internet, controlling what traffic is allowed in and out.

Incident Response

The plan and actions you take to manage the aftermath of a security breach or cyberattack.

IP Address

A unique address for a device on the internet, similar to a street address for a house.

Malware

A general term for any software—like viruses, spyware, or ransomware—designed to harm or disrupt a computer system.

Managed Service Provider (MSP)

An IT company that you hire to manage your technology and cybersecurity on an ongoing basis.

Multi-Factor Authentication (MFA)

A security process that requires more than one method of proving your identity to log in, like a password plus a code from your phone.

Network Segmentation

Dividing your company's computer network into smaller, isolated zones to prevent an attack from spreading.

Patch Management

The process of regularly updating your software and systems to fix security holes before criminals can exploit them.

Penetration Testing

Hiring a team of ethical hackers to try to break into your systems to find security weaknesses before real criminals do.

Phishing

A deceptive email, text, or message designed to trick you into revealing sensitive information or clicking a malicious link.

Ransomware

Malicious software that locks up all your files and demands a payment (a ransom) to get them back.

Remote Desktop Protocol (RDP)

A built-in Windows tool that allows you to control a computer remotely over a network connection.

Risk

The potential for loss or damage when a threat exploits a vulnerability in your business.

Server

A powerful computer that provides data or services to other computers (called clients) on a network.

Social Engineering

The art of manipulating people into giving up confidential information or performing an action they shouldn't.

Threat Actor

Any person or group who has the intent and capability to launch a cyberattack, from individual hackers to organized criminal groups.

Two-Factor Authentication (2FA)

A security process that requires exactly two methods of proving your identity to log in, such as a password and a text message code.

VPN (Virtual Private Network)

A tool that creates a secure, encrypted connection over a public network like the internet, often used for remote work.

Vulnerability

A weakness or flaw in software, hardware, or a process that could be exploited by an attacker.

Zero-Day Exploit

An attack that takes advantage of a security vulnerability on the same day it becomes known to the public, before a patch is available.

Zero Trust

A modern security model built on the principle of "never trust, always verify," which requires continuous authentication for all users and devices.

REFERENCES

1. https://www.verizon.com/business/resources/infographics/2025-dbir-smb-snapshot.pdf
2. https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/
3. https://www.mimecast.com/resources/ebooks/state-of-human-risk-2025/
4. https://www.verizon.com/business/resources/reports/dbir/
5. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report Cost of a data breach 2025 | IBM
6. https://hoxhunt.com/guide/phishing-trends-report
7. https://gurucul.com/2024-insider-threat-report/
8. https://www.fortinet.com/resources/articles/credential-compromise-attacks
9. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index
10. https://deepstrike.io/blog/vulnerability-statistics-2025
11. https://securityscorecard.com/company/press/securityscorecard-2025-global-third-party-breach-report-reveals-surge-in-vendor-driven-attacks/
12. https://www.fortinet.com/resources/cyberglossary/ransomware-statistics
13. https://ddos-guard.net/blog/ddos-trends-2025-mid-year
14. https://blog.cloudflare.com/ddos-threat-report-for-2025-q1/
15. https://scoop.market.us/multi-factor-authentication-statistics/
16. https://spacelift.io/blog/password-statistics
17. https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report
18. https://nvd.nist.gov/general/nvd-dashboard
19. https://www.paloaltonetworks.com/blog/2025/02/incident-response-report-attacks-shift-disruption/
20. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
21. https://www.crowdstrike.com/en-us/resources/reports/threat-hunting-report/
22. http://varonis.com/blog/state-of-data-security-report
23. https://www.veeam.com/blog/announcing-rw24.html
24. https://www.sophos.com/en-us/content/state-of-ransomware
25. https://www.unitrends.com/resources/the-state-of-backup-and-recovery-report-2025/
26. https://info.varonis.com/en/state-of-data-security-report-2025
27. https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf
28. https://www.ibm.com/reports/data-breach

THANK YOU!