CYBERSECURITY
for Small Business Owners

The Owner's Handbook

Iurii Zhurov

SMB Cybersecurity Advisors LLC

Palm Harbor, Florida

A practical field guide.

No jargon. No upselling. No 200-page PDFs.

Cybersecurity

for Small Business Owners

The Owner's Handbook

by Iurii Zhurov

M.Sc. Cyber Security

SMB Cybersecurity Advisors LLC

Palm Harbor, Florida

Version 1.3 · 2026

DOI: 10.5281/zenodo.21689449

This is the Owner's Handbook — a field guide for working business owners. The longer methodological companion volume is the Practitioner Edition, written for the cybersecurity research community. The methodology is the same; the audience is different.

About the Author

Iurii Zhurov is a cybersecurity consultant who used to be a small business owner. Before moving into cybersecurity in 2017, he spent over a decade running businesses in Ukraine — an internet provider, a hardware import company, and a 360-degree photography studio.

That detail matters: most cybersecurity advice is written by people who've never had to make payroll. This book is written by someone who has.

He holds a Master of Science in Cyber Security from the National Aviation University of Ukraine and runs SMB Cybersecurity Advisors LLC out of Palm Harbor, Florida.

CHEAT SHEET

Tear this out. Pin it to the wall.

The Five Things to Do This Week

If you do nothing else from this book, do these five. They block most attacks.

1. Turn on two-step login (“MFA”) on every email account in the business.
2. Turn on two-step login on your accounting software and any system that holds customer data.
3. Make sure you have a backup of important files — and try restoring one to make sure it actually works.
4. Tell everyone who handles money: any unusual wire request gets verified by phone before action.
5. Write down who you'd call if something went wrong (next page).

Phone Numbers to Have Handy

Fill these in now. Don't wait.

IT person / company: _____

Cyber insurance hotline: _____

Bank fraud line: _____

Lawyer: _____

Phishing Red Flags

- Sender's email address is one character off (amaz0n.net).
- Urgent language: “act within 24 hours.”
- Asks you to log in from an emailed link.
- Asks for money, gift cards, or wire changes.
- Asks you to keep it confidential.

If You Clicked Something You Shouldn't Have

1. Don't panic. Don't reboot.
2. Disconnect from Wi-Fi and unplug any network cable.
3. Tell your IT person.
4. Change the password on the account that was open.
5. Watch your bank account for the next 48 hours.

Contents at a Glance

Introduction

Look — here's the deal. Cybersecurity sounds scary. The word alone makes you think of hooded guys in basements and movies where the screen flashes red and somebody yells “We're in!”

For your business, cybersecurity is mostly a few habits. Turn on a couple of settings. Train your team to spot a few patterns. Keep a small disciplined practice that catches problems before they become disasters. That's it. The rest is details.

This book is the owner's handbook. It tells you what to do, in what order, and why. It doesn't try to turn you into a security professional, and it doesn't try to scare you into buying anything. Your job is running your business. Your security job is making sure your business doesn't get hijacked while you're busy running it.

About This Book

If you want the long methodological version — the one written for cybersecurity researchers — that's a separate book called the Practitioner Edition. It's free. You don't need it. This is the book you need.

This one is short on purpose. Long cybersecurity guides exist by the dozens. They sit on shelves unread. This one is written to be read.

Foolish Assumptions

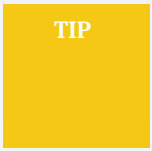
To write this book I had to assume a few things about you. Specifically:

- You own or run a small business — somewhere between 1 and 100 employees, probably under 50.
- You don't have an IT department. Maybe you have one IT person who's busy, or an outside company that handles "the computers."
- You have approximately zero hours a week to spend on cybersecurity, and you want to do something anyway.
- You can use a computer. That's the whole technical prerequisite.

Notice what I didn't assume: that you know anything about cybersecurity, that you have a budget for fancy tools, or that you're a tech person. If you're reading this, that's enough.

Icons Used in This Book

In the margin of various pages, you'll see little tags. They mean:



TIP marks a small bit of advice that'll save you time, money, or a headache. Read these even if you skim everything else.

WATCH OUT marks something that's bitten other small businesses hard. Pay attention.

REMEMBER

REMEMBER marks something I'll mention more than once because it's important. If you take only a few things from this book, take these.

OWNER MOVE

OWNER MOVE marks something only you can do — not your IT person, not an employee, you. These are decisions, not tasks.

Chapter 1

Why You're Holding This Book

In This Chapter

- ► The bad news (we'll get it out of the way fast)
- ► The good news (longer than the bad news, on purpose)
- ► How to read this book without reading the whole thing

Somebody handed you this book. Or you searched for it. Or your insurance carrier sent you a stern email about cybersecurity and you decided to do something about it before they raise your premium again.

Whatever the reason: welcome. This is the part where I tell you it's not as bad as it sounds — and then I prove it.

The Bad News

I'll keep this short.

Small businesses are not incidental targets. Verizon's 2026 report puts about 96 percent of ransomware victims of known size at businesses under 1,000 employees, with a median ransom of $139,875 — before downtime and recovery.

REMEMBER

Attackers don't care that you're a 12-person dental office or a 6-person law firm. They aren't picking on you. They're running automated tools that hit millions of small businesses at once and waiting to see who answers. Most of small business cybersecurity is about not answering.

The Good News

It's mostly habits, not technology.

The five things in your Cheat Sheet at the front of this book block most of what's coming for you. They cost between zero dollars and a couple hundred. They take an afternoon. After that, the maintenance is about fifteen minutes a week.

That's the whole game. Everything else in this book is just explaining those things in more detail and adding the next layer for when you're ready.

How to Read This Book

If you have time, read it cover to cover. It's not long. It'll take you a couple of hours, spread across a few sittings.

If you don't have time, do this:

1. Tear out the Cheat Sheet at the front and pin it where you'll see it.
2. Read Chapter 3 (Locking the Front Door) and Chapter 5 (The Wire Transfer Rule).
3. Come back to the rest when something specific happens.

That's perfectly fine. This book is a tool, not a requirement.

Chapter 2

What Attackers Actually Want from You

In This Chapter

► The five things attackers actually want

► Why “we're too small” is the most dangerous sentence in cybersecurity

► What this means for what you actually defend

Cybersecurity advice gets a lot more useful once you understand what attackers are actually trying to take. Spoiler: it's almost never “secrets.” Your business probably doesn't have any. What it has is more interesting.

The Five Things Attackers Want

1. Your money, the obvious one

Most attacks against small businesses are after money — directly. Wire transfer fraud, gift card scams, payroll redirection, ransomware. The attacker wants you to send money somewhere, and the entire attack is built around that goal. The biggest dollar losses for SMBs come from this category.

2. Your email account

A compromised business email account is enormously valuable, even if there's nothing private in it. Why? Because it gives the attacker your relationships. They can read your conversations with vendors, identify upcoming payments, learn how you write, and then send realistic emails as you to your customers, your vendors, or your bookkeeper. Email is the launching pad for almost everything else.

3. Your customer data

Lists of names, addresses, phone numbers, emails, payment information, social security numbers — these have a market price. Attackers either sell the data on dark web forums or use it for targeted fraud against your customers. If your customer data ends up in a public dump, you have notification obligations under state privacy laws, regardless of business size.

4. Your computers themselves

Sometimes the goal isn't anything in your business — it's just your computers as infrastructure. Botnets (networks of

hijacked computers used for further attacks) need machines. Cryptominers need computing power. Both of these can run on your network for months without you noticing, while quietly making your machines slow, your electricity bill higher, and your business an unwitting participant in attacks against other people.

5. Your reputation, as a launching pad

This is the most underestimated category. Attackers don't always want to take something from you — sometimes they want to use you to take something from your customers. If you're a 6-person law firm whose clients trust your emails, that trust is what attackers want. Same for accountants, marketing agencies, IT providers, vendors. You become the path into someone else's business.

REMEMBER

Most cybersecurity advice talks about "protecting your data." But attackers want five different things, and "data" is only one of them. Wire fraud, email impersonation, infrastructure abuse, supply-chain attacks — these are just as common, often more expensive, and frequently invisible until the damage is done.

"But We're Too Small to Attack"

This is the most dangerous sentence in small business cybersecurity. It's also wrong on two levels.

First, attackers don't pick targets. They run automated tools that hit millions of businesses simultaneously. Your size doesn't make you invisible. It just makes you cheaper to attack — and once they're in, they figure out what you're worth.

Second, your size is exactly what makes you attractive. A Fortune 500 has dedicated security teams and 24/7 monitoring. You have someone who's good with computers. The attacker is looking for the easier target. That's you. Sorry.

WATCH OUT

If you've been telling yourself “they wouldn't bother with us” — that's not a security strategy. That's a reason your insurance carrier will deny your claim.

What This Means for What You Defend

Knowing what attackers want changes what you focus on. Specifically:

- Email gets the strongest protection (because it enables everything else).
- Wire transfer procedures get the strictest rules (because that's where the money goes).
- Customer data gets encrypted and access-controlled (because losing it triggers legal obligations).
- Computers get monitored for unusual activity (because cryptominers and botnets hide there).
- Vendor and supply-chain trust gets explicit verification (because you're a path to your customers).

Each of these gets its own chapter. The next one is the most important.

Chapter 3

Locking the Front Door (Passwords and MFA)

In This Chapter

- ► Why your password is not the problem
- ► The 30-second explanation of MFA
- ► What to set up this week (free)
- ► What to add later (cheap)

If you do nothing else from this book — nothing — do what's in this chapter. The single biggest security upgrade for a small business costs zero dollars and takes about an hour.

Your Password Is Not the Problem

Here's the uncomfortable truth: human-memorable passwords are bad. Always. Even your “good” ones.

“MyDog$Buster2019” is a memorable password. It's also breakable. Worse, you probably use a version of it on more than one site, which means when one of those sites gets breached (and they do), attackers have a working password for everywhere else you used it.

The problem isn't that you pick bad passwords. It's that you can't pick good passwords, because good passwords look like “rf2X@p9!ZkQv8mB&” and you'll never remember that for thirty different sites.

REMEMBER

The solution is not better passwords. The solution is to stop trying to remember passwords altogether.

Password Managers, Plain English

A password manager is a small piece of software that does three things:

1. Generates random unbreakable passwords for you.
2. Remembers them so you don't have to.
3. Fills them in automatically when you visit a website or log into an app.

You only have to remember one password — the master password to the password manager itself. That one matters. Make it long. Make it unique. Don't use it anywhere else.

Bitwarden is free, works on every device, and is what I recommend. There are paid options that add features your business probably doesn't need yet. Start free.

TIP

When you set up Bitwarden, the one thing not to do is forget your master password. Write it on paper, put it in a sealed envelope, and put that envelope somewhere safe (your home safe, your safe deposit box). If you lose the master password, you lose everything in the vault.

MFA in Thirty Seconds

MFA stands for Multi-Factor Authentication. The thirty-second version: when you log in, you have to prove who you are with two different things — usually something you know (your password) plus something you have (your phone).

It's exactly the same idea as your debit card. The card alone won't get someone money — they need the PIN too. Lose the card? Whoever finds it still can't drain your account because they don't have the PIN. MFA is that, for online accounts.

Every modern email service has it. So does every modern accounting platform, every cloud service, every banking site. Most of them have it turned off by default. Your job is to turn it on. Everywhere.

OWNER MOVE

MFA on every email account in your business is the single highest-impact security action you will ever take. If you do it this week and never do anything else from this book, you'll have done more for your security than most small businesses ever do.

Setting Up MFA on Email

Microsoft 365 and Google Workspace both have MFA built in. Setup time per account: about three minutes. Steps differ slightly but the path is roughly:

1. Sign in to the admin console for your email.
2. Find the security or authentication section.

3. Turn on multi-factor authentication for all users.
4. Each user installs an authenticator app on their phone (Microsoft Authenticator or Google Authenticator — free) and follows the prompts.

That's it. Next time anyone logs in, they enter their password and then approve a prompt on their phone. The whole thing adds about three seconds to login.

The SMS Trap

Some services let you do MFA via text message instead of an app. It's better than nothing — but only barely.

SMS-based MFA is vulnerable to a specific attack called SIM swapping, where an attacker convinces your phone carrier to transfer your number to their phone. Then your security codes go to them. This is rare for small targets, but real, and the consequences are severe.

Use the authenticator app, not SMS, whenever the service supports it. Most do.

WATCH OUT

If a service only offers SMS-based MFA, that's better than no MFA. But for the high-value accounts — owner email, bookkeeper email, banking — get an authenticator app or a hardware key (next section).

Hardware Keys: When and Why

A hardware key is a small USB device about the size of a thumbnail. It's the strongest form of MFA — even stronger than authenticator apps, because it's physically resistant to phishing. Even if you accidentally enter your password into a fake site, the hardware key won't authenticate the attacker.

YubiKeys are the standard. About $55 each. Buy two per high-value account (the spare lives in a drawer in case the primary is lost).

Worth it for: owner accounts, bookkeeper accounts, anyone with access to financial systems. Probably overkill for everyone else, at first. Add them later if your business grows.

Chapter 4

Backups That Actually Work

In This Chapter

- ▸ The 3-2-1 rule (and why it matters)
- ▸ Why “we back up” usually doesn't
- ▸ The quarterly test ritual

If ransomware encrypts your computers tomorrow morning, the only thing standing between you and a $50,000 ransom payment is whether your backups actually work.

“Actually” is the operative word.

The 3-2-1 Rule

This is the rule professional IT people follow. It's been around for decades. It works. Three numbers:

1. THREE copies of your important data total.
2. TWO different types of storage (so a single failure doesn't kill them both).
3. ONE copy stored offsite or in the cloud (so a fire, flood, or theft doesn't take everything).

In practice, for most small businesses, this looks like:

- The original data on your working computers (1).
- A copy on an external drive or office server (2 — different storage type).
- A copy in cloud backup like Backblaze, IDrive, or your Microsoft/Google subscription (1 — offsite).

That's it. That's the whole rule. Set it up once, check it every quarter, sleep better.

Why “We Back Up” Usually Doesn't

Most small businesses say they back up. Most are wrong. Common ways the backup turns out to be a hope, not a fact:

- The backup software stopped working months ago and no one noticed.
- Backups exist but only for some folders — and the ones that mattered weren't on the list.
- The backup drive was in the same office as the originals when the office flooded.
- The backup is on a network drive, which ransomware encrypted at the same time as everything else.
- The backup files exist but won't restore — corrupted, missing, or encrypted with a key on the dead computer.

Each of these is something I've seen in real businesses. None of them are theoretical.

WATCH OUT

Microsoft 365 and Google Workspace are not backup services. They sync and they hold deleted files for limited time, but they're not designed for ransomware recovery. If you rely on them as your only backup, you're a single compromised account away from losing everything. Use a separate backup tool (Veeam Backup for Microsoft 365 is the standard).

The Quarterly Test

Once every three months, you actually test the backup. Not check that backups exist. Not look at the dashboard. Test it.

Pick one important file. Pretend it was deleted or corrupted. Restore it from backup to a different location. Open it. Confirm it's the right file. Time how long it took.

That's the test. Fifteen minutes. Once a quarter.

If the test fails — file missing, restore won't run, can't open the result — you found out today, when there's no urgency. If the test never gets done, you find out the day a ransomware attack requires you to restore everything immediately. Nobody wants to find out then.

OWNER MOVE

Put the quarterly backup test on your calendar right now. First week of January, April, July, October. Fifteen minutes. Take it as seriously as paying your taxes — your business survives one of those things and not the other.

Chapter 5

The Wire Transfer Rule

In This Chapter

- ▸ The single most expensive type of cybercrime for SMBs
- ▸ The one rule that prevents most of it
- ▸ What “unusual” actually means

Business Email Compromise — the technical name for wire transfer fraud — is the costliest form of cybercrime aimed directly at businesses. The FBI's Internet Crime Complaint Center reported $3.05 billion in losses in 2025 alone, across 24,768 complaints. Wire transfers move fast, and recovery usually depends on catching it within hours.

The good news: one rule prevents most of it. It costs nothing. It takes a minute per transaction. Here it is.

The Rule

Any unusual financial instruction received by email gets verified by phone — using a known number, not one in the email — before action is taken.

That's the whole rule. Communicate it to everyone who handles money in your business. Post it where they'll see it. Then enforce it.

“Unusual” includes:

- Any wire transfer that's a different amount than expected, or to a different account, or with different timing.
- Any vendor request to change banking or payment information.
- Any executive request to make an urgent payment, especially marked confidential.
- Any customer request to redirect a payment to a different account.
- Any payroll change request — adding new accounts, modifying direct deposit info.

If it fits any of those patterns, the answer is the same: pick up the phone, call a number you already know, confirm. Then act, or don't.

Why It Works

BEC scams work because they exploit two things: trust and speed. The email looks like it's from a real person you trust. The request creates urgency so you act before thinking.

The wire transfer rule defeats both. The phone call breaks the trust assumption — you're verifying through a different channel. The phone call also breaks the urgency — even a sixty-second pause to dial is enough to surface the doubt that prevents the fraud.

REMEMBER

The reason BEC works isn't that the attackers are technically sophisticated. It's that the targets are busy. The defense isn't technical sophistication on your side — it's a reflex that survives being busy.

The Deepfake Variant

A new wrinkle on this: some attackers now call you instead of emailing. They use AI-generated voice clones of your CEO or CFO. The voice sounds right — same accent, same speech patterns — because it's built from a podcast appearance, a webinar, or a public video they found online.

In early 2024 a multinational firm lost $25 million to one of these attacks. It happens to small businesses too, just at smaller dollar amounts.

The defense is the same. Even if it's a voice you recognize, even if the call seems to come from a number you know, any unusual financial instruction gets verified through a separate channel. Hang up. Call back to the number in your contacts, not the one that just called you. Confirm in person if possible.

WATCH OUT

Caller ID can be spoofed. Voice can be cloned. Video conference deepfakes are a real category in 2026. If a financial decision is being made on the basis of a voice or video alone, you have not yet verified it. The verification reflex applies regardless of how convincing the request is.

Chapter 6

Training Your Team Without Making It Boring

In This Chapter

- ► Why traditional security training fails
- ► The 15-minute lunch meeting that works
- ► Three patterns to teach your team
- ► What to do when someone clicks something

The human element shows up in about 62% of breaches. Someone clicked a link. Someone wired money. Someone opened the wrong attachment.

This is not a technology problem. Technology can help, but the front line is your team. The good news is your team doesn't need a course. They need three patterns and one rule.

Why Most Training Fails

Most security training is designed by security people for security people. It's long, technical, full of jargon, and assumes employees care as much about security as the trainer does. They don't. They have jobs to do.

The training that works for small businesses has three properties:

- It's short. Fifteen minutes, not fifteen hours.
- It's specific. “Here's the actual phishing email we received last week” beats theory.
- It's repeated. A fifteen-minute conversation every quarter beats a four-hour course once a year.

TIP

If you have a team of five to fifty people, the highest-leverage training format is a fifteen-minute lunch meeting once a quarter. Bring sandwiches. Show two real phishing emails. Discuss what's wrong with each. Ask one question. Done.

Three Patterns to Teach

1. The Sender Doesn't Match

The email looks like it's from amazon@billing-update.net or your-it-support@msft365.co. These domains are not Amazon and not Microsoft. Real companies use their real domains. Hover over the sender (without clicking) to see the actual address.

2. The Urgency Is Off

“Click here within 24 hours or your account will be suspended.” “Wire this transfer immediately, the deal closes today.” Real businesses don't operate this way. Real urgency comes through phone calls and known channels, not surprise emails.

3. The Request Is Unusual

Your bookkeeper has never been asked to buy gift cards before. Your CEO has never asked for an urgent confidential wire transfer. The pattern is itself the warning. If it's the first time someone has asked you to do this, that's the moment to verify.

The One Rule for Your Team

Beyond the three patterns, your team needs one explicit rule:

Report it. Don't fix it. Don't ignore it. Tell IT.

If something seems off, the right action is always to forward the email to the IT contact, or report the suspicious phone call, or flag the unexpected attachment. Not delete it (that destroys evidence). Not click to see what it does (that's how breaches happen). Not ignore it (and let the next person fall for the same thing).

REMEMBER

Your team's job is to spot something suspicious and tell someone. That's it. They're not security professionals. They don't need to understand the threat. They need to know that when something feels wrong, the right move is to ask, not act.

Chapter 7

Reading Vendor Proposals Without Getting Snowed

In This Chapter

- ► Three questions that filter sales pitches from real advice
- ► Words to ignore in vendor proposals
- ► IT support vs. cybersecurity (they're different)
- ► What your IT person should be doing

If you run a small business, you'll be approached. By cybersecurity firms. By IT vendors. By insurance brokers. By managed service providers offering “comprehensive protection.”

Most of them are selling. A few are actually helping. This chapter is how to tell.

The Three Questions

When someone pitches you a security product, service, or upgrade, ask these three questions. The answers tell you everything.

1. “What specific risk does this address for my business?”

Vague answers (“all kinds of attacks,” “comprehensive coverage,” “modern threats”) mean they don't know your business. Specific answers (“this protects against the wire fraud schemes that hit accounting firms last year”) mean they've at least thought about you. Trust the second one.

2. “What free or low-cost alternative exists?”

Every paid cybersecurity tool has a free or near-free alternative that's adequate for most small businesses. A good vendor will acknowledge this and explain why their version is worth the price. A bad vendor will dismiss the question. The acknowledgment alone separates pros from salespeople.

3. “What does success look like in 90 days?”

Cybersecurity outcomes are hard to measure, but a competent provider will commit to specific deliverables: “We'll have MFA on every email account, a tested backup, and a documented incident response plan.” A salesperson will speak in vague reassurances. The committed answer is real. The vague answer is marketing.

Words to Ignore

Cybersecurity marketing has a vocabulary of meaningless words. When you see them, lean back.

- “Industry-leading” — meaningless.
- “Robust” — meaningless. So is “enterprise-grade” for a 12-person business.
- “Cutting-edge” — usually means “untested in your environment.”
- “AI-powered” — sometimes real, often pasted on for marketing.
- “Turnkey solution” — almost always involves you turning a lot of keys.
- “24/7 monitoring” — by what? a person? an alert system? does anyone read the alerts?

Ask what these phrases actually mean in concrete terms. If the vendor can't explain in plain English, the words are decoration.

IT Support vs. Cybersecurity

This is the most common confusion in small business and the most expensive one. Two different professions, often in the same company.

IT support keeps things running. The email is delivered, the printer prints, the new laptop gets configured. They install antivirus and apply patches. That's their job.

Cybersecurity thinks adversarially. How would someone break in? What would they do once inside? How would we know? They write policies, test responses, train people. That's a different job.

Many MSPs (managed service providers) offer cybersecurity as part of their package. Some genuinely deliver it. Most don't. They install antivirus and call it cybersecurity.

OWNER MOVE

Ask your current IT provider these questions: What's our incident response plan? What threat modeling have you done specifically for our business? What cybersecurity certifications do your staff hold? If the answers are vague or evasive, you have IT support, not cybersecurity. That's not a reason to fire them — IT support is valuable. It's a reason to recognize the gap.

Chapter 8

Cyber Insurance Without the Headache

In This Chapter

- ► Why you need cyber insurance
- ► What's typically covered
- ► The social engineering trap (read this carefully)
- ► How to compare quotes

If you have general liability insurance, property insurance, professional liability insurance — fine. You also need cyber insurance. If you don't, the next chapter saves the rest of this book from being academic.

Why You Need It

A serious cyber incident at a small business routinely runs into six figures once you count ransom, downtime and recovery. That doesn't include lost revenue from operational disruption, which often doubles or triples the total.

Most small businesses cannot absorb a six-figure hit unexpectedly. Cyber insurance turns a business-ending event into a manageable claim. Cost: typically $1,500 to $5,000 a year for $1 million in coverage at a small business. Compared to general liability premiums, that is reasonable.

Beyond the money, most cyber insurance policies include free or discounted incident response services. When something goes wrong, you call a hotline staffed by professionals who handle the response on your behalf. This is enormously valuable when you're in the first hours of a crisis and don't know what to do.

What's Typically Covered

A standard small-business cyber policy covers, in some combination:

- Direct losses from ransomware, including the ransom (if approved by the carrier).
- Investigation and recovery costs (forensics, system rebuild, data restoration).
- Legal expenses related to a breach.
- Customer notification costs and credit monitoring services.
- Regulatory fines (in some policies, with limits).
- Business interruption losses while you recover.
- Wire fraud losses (this is the important one — see next page).

The Social Engineering Trap

Here's the part most small businesses don't read carefully enough.

Wire fraud — where an employee was tricked into sending money to an attacker — is covered under most cyber policies, but separately, with a sub-limit. The total policy might be $1 million. The wire fraud sub-limit might be $50,000 or $250,000.

If your business handles wire transfers regularly, this number matters. The FBI puts the average reported wire fraud loss at about $123,000. If your policy caps social engineering at $50,000, you're covered for a good deal less than you think.

WATCH OUT

Read the social engineering / cyber crime sub-limit on every cyber insurance policy. Get it as high as your business needs. If your sub-limit is $50,000 and you handle six-figure wire transfers regularly, you're underinsured. Most carriers will increase the sub-limit for an additional premium.

Required Controls = Your Security Checklist

Most cyber insurance policies require certain controls to be in place. If they aren't, the policy may not pay out when you have a claim.

These typically include:

- Multi-factor authentication on email and remote access.
- Regular backups, tested periodically.
- Endpoint protection (antivirus) on all computers.
- Employee security awareness training.
- Patching of operating systems and software.

Read these required controls on your policy. They are essentially the floor of acceptable cybersecurity for a small business. If you're doing them, your insurer is happy. If you're not, your insurer will use it as a reason to deny claims. Either way, the list of required controls is your starting checklist.

OWNER MOVE

When you renew your cyber insurance, get three quotes. The cybersecurity insurance market changes frequently and shopping around can meaningfully cut the premium or get you better coverage. Compare on three things: total policy limit, social engineering sub-limit, and what controls are required.

Chapter 9

Fifteen Minutes a Week

In This Chapter

- ► The weekly review ritual
- ► Four questions to ask each week
- ► The monthly, quarterly, and annual extensions
- ► Why discipline beats technology

Cybersecurity in a small business doesn't fail because the right controls were never set up. It fails because the right controls weren't maintained.

The MFA was enabled, then someone disabled it during a troubleshooting session and forgot to turn it back on. The backup ran for six months, then the agent broke and nobody noticed for fourteen months. The password manager was rolled out, then half the team stopped using it because it was inconvenient on a Tuesday.

None of these are technology failures. They're attention failures. The fix is a small, regular, disciplined practice: fifteen minutes a week.

The Weekly Review

Same time every week. Pick a time. Put it on your calendar. Defend it the way you defend a meeting with your most important client. If you skip it once, the practice survives. If you skip it three weeks in a row, the practice is dead.

During the fifteen minutes, ask four questions:

1. Did anything weird happen this week? Suspicious email, slow computer, unusual login alert, surprise payment, weird call?
2. Are the systems applying their updates? Computers, phones, software?
3. Did backups run this week, and did they succeed?
4. Is anything left over from last week's review that I haven't followed up on?

Write down what you find. Even “nothing unusual” is worth recording. The pattern of weeks with nothing unusual interspersed with occasional findings is the signature of a working practice.

The Monthly Extension

Once a month, on top of the weekly review, take an extra fifteen minutes for an access check:

- Anyone leave the business this month? Did their access actually get revoked everywhere?
- Anyone change roles? Did access get adjusted?
- Any contractor or vendor whose access should have expired by now?

Old access is a slow leak. Each unrevoked account is a potential entry point. Monthly review keeps it from accumulating.

The Quarterly Extension

Once every three months, the backup test from Chapter 4. Pick a file, restore it from backup to a test location, confirm it works. Time how long it took. Document the result.

Fifteen minutes. Once every ninety days. Survives a ransomware attack.

The Annual Extension

Once a year — same week every year, perhaps when you renew insurance — read this book again. Or at least Chapter 3 (passwords and MFA), Chapter 4 (backups), and Chapter 5 (wire transfer rule). Re-do the Cheat Sheet at the front.

Your business has changed. The threats have changed. Some of what mattered last year matters less this year, and some new things matter more. The annual review catches the drift.

REMEMBER

Total time budget for sustained cybersecurity in a small business after initial setup: about twenty hours per year, distributed in fifteen-minute pieces. That's the real number. Do the twenty hours. The rest of it — the headlines, the warnings, the breach reports, the consultants who want to scare you into buying more — is mostly noise.

Chapter 10

When to Call for Help (And When Not To)

In This Chapter

- ► What you can handle yourself
- ► When you need a professional
- ► How to find one without getting fleeced

This book is structured so that most small businesses can implement most of it without hiring a cybersecurity consultant. You're not building a Fortune 500 security program. You're building a defensible small business posture.

That said, there are specific moments when professional help is the right investment. Knowing which is which saves money.

When You Don't Need a Consultant

You don't need a consultant for any of the following. They're inside the scope of this book.

- Setting up MFA on email and cloud services.
- Choosing and rolling out a password manager.
- Establishing the wire transfer verification rule.
- Setting up backup and testing it quarterly.
- Running quarterly cybersecurity awareness conversations with your team.
- Reading and acting on cyber insurance requirements.
- The weekly fifteen-minute review.

All of these are owner-operable. Hiring someone to do them costs you money you don't need to spend.

When You Do Need a Professional

Specific triggers where outside expertise is the right choice:

After a real incident

If something has happened — confirmed phishing breach, ransomware, wire fraud — call a professional. The first hours of an incident response are not the time to learn on the job. Your cyber insurance carrier likely has incident response services included; use them.

Customer or regulatory requirement

HIPAA compliance for a healthcare practice, PCI DSS for businesses handling credit cards, SOC 2 for B2B software companies, specific contract requirements from major customers — these need professional attestation. Don't try to self-audit.

Major business change

Acquiring a competitor, expanding into a regulated industry, signing a contract with a much larger customer who requires a security review — these are good moments to bring in a professional.

Periodic outside review

Every two or three years, an outside professional looking at your security posture catches drift you can't see from inside. Worth the expense once it's been a few years.

Finding a Good One

How to filter when choosing a professional:

1. Ask for references — actual small businesses they've worked with, not testimonials on a website.
2. Ask the three questions from Chapter 7 — what specific risk, what alternatives, what does 90 days look like.
3. Ask about their staff's certifications. CISSP, CISM, GIAC certifications are real. Vendor-specific certifications mean less.
4. Ask for a sample deliverable, with confidential information redacted.
5. Get two or three quotes. Quotes vary widely for the same scope.

OWNER MOVE

Pick your “phone a friend” cybersecurity person now, before you need them. When you actually need help — at 11 p.m. on a Friday during a ransomware attack — having an established relationship with someone who already knows your business is worth real money. Most of what they'll do is reassure you that you're handling it correctly.

The Part of Tens

If you've ever read a For Dummies book, you know the Part of Tens. Top-ten lists you can act on in five minutes. Here are five of them.

Top 10 Things to Do This Month

1. Turn on MFA on every email account.
2. Turn on MFA on the accounting software and any system holding customer data.
3. Set up Bitwarden Free for your team.
4. Confirm you have a backup. Test restoring one file.
5. Establish the wire transfer rule. Tell everyone who handles money.
6. Make a list of who you'd call in an incident. Pin it where you'll find it.
7. Get cyber insurance if you don't have it. Read the policy.
8. Run a fifteen-minute team meeting on phishing recognition.
9. Schedule the weekly fifteen-minute review on your calendar — every week, recurring.
10. Pick a quarterly date for the backup test.

Top 10 Phishing Red Flags

1. Sender's address is a near-miss for the real one (amaz0n.net, micros0ft.com).
2. Urgent or threatening language demanding action within hours.
3. Requests for credentials, passwords, or financial information by email.
4. Unexpected attachments — especially .zip, .exe, .docm, .iso, .htm files.
5. Links that display one URL but go to a different one (hover to check).
6. Requests that seem out of character for the apparent sender.
7. Requests to bypass normal procedures or keep things confidential.
8. Offers that seem too good to be true.
9. Requests for urgent wire transfers, gift cards, or payment changes.
10. QR codes asking you to scan them to access a document or pay something.

Top 10 Questions to Ask Your IT Provider

1. “What's our incident response plan? What happens if our email is compromised tomorrow morning?”
2. “What threat modeling have you done specifically for our business?”
3. “Which of your staff hold cybersecurity certifications, and what are they?”
4. “Can you show me a sample security assessment, with confidential information redacted?”
5. “What free or low-cost alternatives exist for what you're recommending?”
6. “What does success look like in 90 days?”
7. “When was our last backup actually tested by restoring files?”
8. “Is MFA enabled on every account in the business right now?”
9. “Which employees have administrative privileges, and why?”
10. “What do you not do that we should be paying someone else to do?”

Top 10 Cybersecurity Lies You Should Stop Believing

1. “We're too small to be a target.” Attackers don't pick. They scan.
2. “Our IT person handles security.” IT and cybersecurity are different professions.
3. “We don't have anything an attacker would want.” Yes you do — see Chapter 2.
4. “Our antivirus protects us.” Helpful, not sufficient.
5. “Microsoft 365 backs up our data.” It syncs. That's different.
6. “We trained employees last year.” Once doesn't stick.
7. “Our passwords are strong.” They're memorable. That's not the same.
8. “We haven't had any incidents.” That you know of.
9. “It's too expensive.” Most of this book is free.
10. “We'll deal with it if something happens.” That's a six-figure bill you don't have.

Top 10 Free Tools That Actually Work

1. Bitwarden Free — password manager.
2. Microsoft Authenticator or Google Authenticator — MFA app.
3. Microsoft Defender (built into Windows) — antivirus.
4. BitLocker (Windows Pro+) or FileVault (Mac) — disk encryption.
5. Quad9 (DNS server 9.9.9.9) — blocks malicious websites at the network level.
6. ProtonVPN Free — VPN for occasional remote access.
7. Veeam Backup for Microsoft 365 — backup specifically for Microsoft 365 (paid, low-cost; here for completeness).
8. CISA Cyber Essentials Toolkit — free framework and training.
9. FTC Small Business Cybersecurity training — free awareness materials.
10. Have I Been Pwned (haveibeenpwned.com) — check if your email was in a known breach.

Index

A Final Note

If you've read this far, thank you. The fact that you cared enough to read a small book about cybersecurity puts you ahead of most small business owners — and frankly, ahead of some Fortune 500 executives I've met.

You don't need to be perfect at this. You need to be better than you were last week. Do the Cheat Sheet things. Schedule the fifteen-minute weekly review. Read Chapter 5 again before you wire any money. Come back to the rest when something specific happens.

I wrote this for you. If something in here saves you from a bad day — that's the whole point.

Iurii Zhurov

Palm Harbor, Florida · 2026

Revision History

Version 1.3 — July 29, 2026

Statistical figures have been updated to the Verizon 2026 Data Breach Investigations Report and the FBI Internet Crime Complaint Center 2025 Annual Report. Where a figure describes organizations with fewer than 1,000 employees, the text says so, following the publisher's own segment definition. Figures that could not be traced to a primary source have been removed rather than re-attributed. The advice, the structure and the checklists are unchanged.

Persistent identifier

DOI: 10.5281/zenodo.21689449 (this version)

Version 1.0 — 2026

Initial publication.