SMB Cybersecurity Framework

Practitioner Edition

A Methodology for U.S. Small and Medium-Sized Businesses

Discipline first.
Then even Excel is a good tool.

Iurii Zhurov, M.Sc. Information Security Management
SMB Cybersecurity Advisors LLC
Palm Harbor, Florida

Version 1.0 · 2026

About This Framework

This framework exists because the cybersecurity market does not work for small businesses, and the small businesses that need protection most are the ones receiving it least.

It is not a simplified version of an enterprise framework. It is a different methodology, built for a different reality: a business owner with no IT department, no cybersecurity budget, and 30 minutes a week to spend on security. It treats discipline as more important than technology, free-tier tools as the starting point rather than the fallback, and the business owner as the primary student rather than the IT employee.

The framework is organized so that any owner of a small business — from a 3-person construction company to a 50-person professional services firm — can read Section 1 in 15 minutes, understand whether the framework is for them, and know what to do next. It is structured to be implementable in phases over 30, 90, and 180 days, with explicit guidance on what to focus on first when time and resources are constrained.

This framework references the principles of the NIST Cybersecurity Framework 2.0, ISO/IEC 27001, and CIS Controls v8 where they are useful. It is not derived from them. It is built on direct experience with small organizations operating under cyber pressure: fifteen years of running small businesses; eight years providing cybersecurity consulting to small organizations in Ukraine — one of the most intensively attacked countries in the world; and current consulting work with U.S. small businesses across construction, automotive, technology, and professional services.

The standards inform; they do not dictate. The owner of a 12-person plumbing company is not the same reader as the CISO of a Fortune 500 bank. The advice they need is not the same.

About This Edition

This is the Practitioner Edition of the SMB Cybersecurity Framework — the canonical methodological document, written in the voice of a cybersecurity practitioner addressing other practitioners and the international research community. It is the version cited in conference proceedings and peer-reviewed publications, and it serves as the source of record for the framework's methodology, terminology, and structure.

A separate companion volume — the Owner's Handbook — adapts the same methodology directly for the working small business owner who needs an accessible implementation guide rather than a methodological argument. The two editions are complementary, not redundant: the Practitioner Edition explains the framework; the Owner's Handbook delivers it.

How to Use This Framework

Read Section 1 first. It explains what this framework is, who it is for, and how it differs from the enterprise-derived guides you may have encountered. If after Section 1 you decide this is not for you, you have spent fifteen minutes — that is the point.

If you continue:

- Section 2 explains the threats your business actually faces, in plain language.
- Section 3 helps you assess your own risk in 30 minutes (for businesses under 10 employees) or in a structured cycle (for larger SMBs).
- Section 4 gives you four core security policies you can adapt and adopt.
- Section 5 lays out a 30/90/180-day implementation roadmap.
- Section 6 is the part most frameworks skip: how to make security a discipline rather than a one-time project.
- Section 7 covers what employees and you, the owner, need to know.

The five appendices are reference material: a free-tier tools matrix, a glossary that translates technical terms into plain English, real-world incident cases organized by industry, descriptions of the Excel templates that accompany the framework, and a plain-language catalog of every threat type you might encounter.

About the Author

Iurii Zhurov holds a Master of Science in Information Security Management from the National Aviation University of Ukraine and has worked in administrative information security for over fifteen years. Before becoming a cybersecurity practitioner, he spent over a decade running small businesses in Ukraine — an internet service provider sold in 2011, a computer hardware import and distribution company, and a 360-degree photography studio. That entrepreneurial background is the reason this framework exists. Most cybersecurity professionals have never run a small business; he has run three. The framework is shaped by what small business owners actually need, not by what consultants are trained to sell.

The author currently operates SMB Cybersecurity Advisors LLC in Palm Harbor, Florida, providing cybersecurity consulting to U.S. small and medium-sized businesses. The framework is the working methodology of that practice, made freely available to any small business that wants to use it.

Table of Contents

Section 1: The Approach

Time required for owner: 15 minutes to read.

1.1 Why This Framework Exists

There are approximately 33 million small and medium-sized businesses in the United States. They produce 44 percent of U.S. economic activity and employ nearly half of the private-sector workforce. About 80 percent of them — roughly 27 million — have fewer than 10 employees. These are the businesses that build houses, fix cars, prepare taxes, run restaurants, treat patients, deliver packages, and quietly hold the American economy together.

Forty-six percent of all cyberattacks target small businesses. Sixty percent of small businesses that suffer a significant cyber incident close within six months. The average breach costs a small business more than $200,000. These are not predictions. They are the present.

And yet the cybersecurity market does not work for small business. It works for enterprise. Large consulting firms — Deloitte, PwC, Mandiant, KPMG — sell to enterprise. The cybersecurity software industry — CrowdStrike, Palo Alto Networks, Splunk, Microsoft's enterprise security stack — is priced and designed for organizations with hundreds or thousands of employees. The cybersecurity workforce is trained to operate in those environments, with those tools, against those threat models.

Below the enterprise tier sits the world of managed service providers — the IT companies that small businesses hire to keep their email working and their printers connected. Many of these MSPs now market "cybersecurity" as part of their offering. Some genuinely deliver it. Most do not. Setting up an antivirus and enabling a firewall is not cybersecurity, in the same way that putting a deadbolt on the door is not a security plan. The skills are different, the training is different, and the incentive structures are different. The MSP is paid to keep things running. The cybersecurity practitioner is paid to think about how things break.

Between the enterprise consulting firms that small businesses cannot afford and the IT support providers that do not actually do cybersecurity, there is a structural gap. Tens of millions of American small businesses sit in that gap, knowing vaguely that cybersecurity matters but having no realistic way to obtain it. They read articles telling them to use stronger passwords. They are sold expensive tools that solve problems they do not have. They are warned about threats whose names they do not recognize, by experts who have never run a payroll for ten people.

Existing frameworks do not close this gap. The NIST Cybersecurity Framework is excellent — and 200 pages long, written for organizations with security teams. ISO/IEC 27001 is a certification standard built for formal management systems. CIS Controls are a strong baseline, but their implementation

guidance assumes resources most small businesses do not have. None of these are wrong. They are simply not designed for a 12-person business with no IT staff and a Wednesday morning that already has too many things in it.

This framework is designed for that Wednesday morning.

1.2 Who This Framework Is For

This framework is written for the owner of a small business — typically between 5 and 50 employees, with a particular focus on micro-businesses of fewer than 10. If you are reading this, you probably:

- Run a business that generates somewhere between $500,000 and $10 million in annual revenue.
- Have no full-time IT staff. Maybe you have a part-time IT contractor or an MSP. Maybe one of your employees is "good with computers" and handles the day-to-day.
- Have no cybersecurity budget — or if you have one, it is implicit, hidden inside what you pay your IT provider, and you are not sure what you are getting for it.
- Know that cybersecurity is important and have known this for years, without being entirely sure what you should actually do about it.
- Have, on a good week, about 30 minutes to spend on this.

If that describes you, this framework is for you. It is not written for cybersecurity professionals. It is not written for businesses with information security officers. It is not written for organizations whose compliance department mandates a specific framework. Those readers will find it useful as a reference, but they are not the audience.

If you have more than 100 employees, dedicated IT staff, or formal compliance obligations under HIPAA, PCI DSS, SOC 2, or sector-specific regulations, this framework can serve as a starting point — but you will quickly outgrow it and should engage a security professional or adopt one of the more comprehensive frameworks (NIST CSF 2.0, ISO/IEC 27001, CIS Controls) directly.

1.3 What Is Different About This Framework

This framework makes specific methodological choices that differ from enterprise-derived guides. They are not stylistic. They are structural, and they shape every page that follows.

Excel and Google Sheets Are the Primary Tool

Enterprise security programs run on dedicated software — governance, risk, and compliance platforms; security information and event management systems; identity and access management

products. These tools cost tens or hundreds of thousands of dollars per year and require specialists to operate. This framework does not assume you have any of them.

Every checklist in this framework can be implemented in Excel or Google Sheets. Every template referenced in Appendix D is a spreadsheet. The asset inventory is a spreadsheet. The risk register is a spreadsheet. The access review log is a spreadsheet. This is not a limitation of the framework. It is the design. A small business that maintains its security posture in a disciplined Excel workbook is more secure than one that buys an enterprise GRC platform and ignores it.

Free-Tier First

Every recommended control in this framework starts with a free or low-cost option. Paid options are listed where they offer real value and where the business has clearly outgrown the free tier — but the free option is the starting point, not the fallback.

This is a deliberate inversion of how most cybersecurity guidance is structured. The enterprise default is to assume budget; the small business reality is to assume there is no budget at all. A password manager that costs $0 and is properly used is more secure than one that costs $8 per user per month and gets shelved because the budget request was denied. Bitwarden, Microsoft Defender, ProtonVPN, and the security features built into Microsoft 365 and Google Workspace can carry a small business a long way. They are listed first because, for most readers, they are sufficient.

Discipline Over Technology

More than 80 percent of successful cyberattacks involve a human element — someone clicked a link, used a weak password, or was manipulated into wiring money to an attacker. The most expensive endpoint detection product in the world cannot stop the receptionist from approving an MFA prompt she did not initiate. Technology controls matter, but they are necessary, not sufficient. The decisive factor in most small business breaches is whether the business had built a habit of paying attention.

This framework treats discipline — the habit of consistent, modest, regular attention to security — as the central security control. Section 6 is dedicated entirely to building that discipline. It is the part of the framework that an enterprise GRC system would automate; in a small business, it has to be a human practice, and this framework gives you the rhythm.

Phased Over Comprehensive

Twenty percent of security controls block roughly 80 percent of attacks against small businesses. Multi-factor authentication on email, basic backup hygiene, password manager adoption, and a half-trained workforce will defeat the overwhelming majority of attacks aimed at SMBs. Comprehensive solutions look impressive but rarely get implemented. Partial implementation actually happens, and partial protection is not 50 percent of full protection — for the most common attack patterns, it is 80 percent.

The implementation roadmap in Section 5 is built on this principle. Phase 1 (the first 30 days) is the high-value, low-effort starting set. Phase 2 (60 more days) builds on it. Phase 3 (the next 90 days) adds depth. The framework is structured so that a business that completes Phase 1 and stops there is still substantially more secure than a business that bought enterprise tools and never operationalized them.

Business Language, Not Security Jargon

Most cybersecurity documentation is written by security professionals for security professionals. Acronyms are introduced without explanation. Concepts assume familiarity with the threat landscape. The reader who is not already conversant in the field is filtered out by page two.

This framework is written in business language. Every technical term is translated to plain English at first use, and Appendix B contains a full glossary with business analogies. "MFA" is "a second proof of identity beyond a password — like a debit card and PIN, not just one of them." "EDR" is "software that watches every computer in your business for suspicious activity, like a security camera with an alarm." The translation is not condescending. It is an admission that the language of the field has become a barrier to the people who most need to understand it.

The Owner Is the Primary Student

Most small business cybersecurity guidance focuses on training employees. That matters — and Section 7 covers it — but it is not enough. The decisions that determine whether a small business is secure are made by the owner: which IT provider to hire, which insurance policy to buy, whether to invest in a particular tool, how to respond to a customer's security questionnaire, what to do when the bank calls about a suspicious transaction.

This framework includes a dedicated owner education layer (Section 7.4) addressing those decisions directly. It does not try to make the owner a security professional. It tries to make the owner a competent decision-maker on security questions, which is a different and more achievable goal.

1.4 Why SMB Cybersecurity Is a National Issue

It is tempting to read the previous sections as describing a small business problem. It is not. It is a national problem that happens to land on small businesses.

Tens of millions of unprotected small businesses are not the periphery of the cybersecurity problem. They are its largest single resource for attackers.

Consider how a modern attack against a Fortune 500 company actually works. Direct attacks on hardened enterprise networks are difficult and expensive. Attacks through the supply chain — through the small vendors, contractors, and service providers that have legitimate access into the larger organization — are dramatically easier. The 2013 Target breach began with a small HVAC contractor. The SolarWinds compromise of 2020 reached its enterprise victims through a software

vendor. Business email compromise schemes against large companies routinely begin with a compromised email account at a small accounting firm or law office that the larger company trusts.

Compromised small business email domains fuel business email compromise campaigns against everyone. Compromised small business websites become watering holes for attacks against high-value visitors. Compromised small business networks become botnet nodes attacking critical infrastructure. The attacker does not need to defeat the Fortune 500 company's security stack; the attacker needs to defeat the security of the 200-person law firm the Fortune 500 company uses, or the 15-person managed service provider that maintains the law firm's email.

This means that the cybersecurity posture of the United States cannot be improved by hardening enterprises alone. As long as the small business segment remains structurally unprotected, the protection of large enterprises and government systems is fundamentally incomplete — regardless of how much is invested in those organizations' own defenses. The unprotected SMB ecosystem is the persistent infrastructure on which attacks against everyone else are staged.

This is not a theoretical argument. It is the explicit framing of the U.S. government's cybersecurity policy. Executive Order 14028, issued in May 2021, identifies the protection of the broader digital ecosystem — including the small business supply chain — as a federal priority. The National Cybersecurity Strategy of 2023 specifically calls for extending cybersecurity capabilities to underserved sectors. The Cybersecurity and Infrastructure Security Agency (CISA) has repeatedly identified small business cybersecurity as a critical systemic vulnerability.

In short: the small business owner who reads this framework and acts on it is not just protecting her own business. She is closing one of the entry points that attackers use to reach the rest of the country. That is a national contribution, even when no one writes a press release about it.

1.5 The Slogan

Discipline first. Then even Excel is a good tool.

If you take only one idea from this framework, take this one. Buying expensive security software without the discipline to maintain it is worse than buying nothing — because it produces a feeling of protection without the substance. Maintaining a simple, disciplined security practice using free tools and a spreadsheet is better than buying an enterprise platform and ignoring it.

Cybersecurity for small businesses is not primarily a technology problem. It is a habit problem. The technology has to be there, and this framework will tell you which technology, but the technology is not the hard part. The hard part is the Wednesday morning when you have ten things to do and the security review is the eleventh, and you do it anyway.

If you are willing to commit to that — 30 minutes a week, every week — this framework will give you the structure to spend those 30 minutes well. That is the offer. The rest of the document is the details.

Section 2: Understanding the Threats

Time required for owner: 30 minutes to read.

Before you can defend, you have to understand. This section explains the threats your business actually faces, in the language your business uses. Each threat is described in four parts: what it is, how it actually happens to a business like yours, what it costs when it succeeds, and a real-world case from a similar business (full case studies are in Appendix C).

These are not seven separate problems. They are seven entry points to the same problem: someone gets access they should not have, and uses it to take something — your money, your data, your customers' trust, or your ability to operate. The rest of this framework is about closing those entry points, in the order that matters most.

If you find yourself reading these and thinking "that could not happen to us" — that is the most common reaction, and it is the reason these attacks succeed. Most of the businesses described in Appendix C thought the same thing the week before.

2.1 Phishing

What it is

Phishing is an email designed to trick someone into doing something harmful — clicking a link, downloading a file, entering a password, approving a transaction. The email looks like it comes from someone trustworthy: a bank, a vendor, a customer, the IRS, your IT provider, or you yourself.

There are three increasingly dangerous variants. Generic phishing is sent to millions of people; about 1 in 1,000 will fall for it, and the volume makes it profitable. Spear phishing is targeted at one person — often the bookkeeper, the operations manager, or the owner — and is researched in advance. Whaling is spear phishing aimed specifically at executives. AI-generated phishing, which is now standard for sophisticated attackers, eliminates the spelling and grammar errors that used to give phishing emails away. The badly-written phishing email is becoming a thing of the past.

How it actually happens

A small accounting firm receives an email that appears to come from one of its clients, asking for an updated W-9 form. The email address is one character off from the real one — easy to miss. The bookkeeper opens the attached PDF, which prompts her to enter her email password to view the secure document. She does. Within an hour, attackers are inside her email account, reading client

communications, looking for invoices and payment patterns. Two weeks later, they send a message from her real account to one of her clients, instructing them to update the wire transfer information for an upcoming payment. The client, trusting an email from their accountant, complies. The next $80,000 invoice payment goes to the attackers' account. By the time anyone notices, the money is gone.

What it costs

The IC3 (FBI Internet Crime Complaint Center) reports that phishing-initiated incidents averaged $173,000 in losses for small business victims in 2023. Beyond the direct financial loss, businesses report 5 to 30 days of operational disruption, depending on how deep the compromise went. Cyber insurance often does not cover losses where an employee was tricked into taking the harmful action voluntarily — read your policy carefully. The reputational cost of having to call clients and say "please disregard the wire instructions you received from us last week" is harder to quantify but is real.

Industry case

Appendix C contains a detailed case from a 9-person legal services practice that lost $124,000 to a phishing-initiated wire fraud over the course of a single Friday afternoon. See Appendix C.7 (Legal Services).

2.2 Business Email Compromise (BEC)

What it is

Business email compromise is the broader category that wire fraud schemes belong to. The attacker either compromises a real business email account or impersonates one convincingly enough to issue instructions that the recipient will follow. The defining characteristic of BEC is that there is often no malware involved at all — the entire attack runs on email, social engineering, and timing.

Common BEC patterns: an email apparently from the CEO instructs the bookkeeper to wire money to a new vendor for an urgent confidential transaction. An email apparently from a familiar vendor reports that their bank account has changed and provides new routing information for the next payment. An email apparently from a customer requests an updated invoice be sent to a different email address. An email apparently from a payroll service requests that an employee's direct deposit information be updated.

How it actually happens

A small construction company has been working with a roofing subcontractor for three years. Every two weeks, the subcontractor invoices around $40,000. Attackers compromise the subcontractor's email — often through a phishing attack on the subcontractor itself, who may not even know they have been breached. The attackers spend several weeks inside the email account, learning the

relationship: who sends invoices, who approves payments, what language is used, what the wire information looks like. When the next invoice is due, they intercept it, modify the wire instructions to point to an account they control, and send it through. Or they send a separate email from the subcontractor's real account: "Hey John, our bank is doing a routing change — for this invoice please use this new account information."

Nothing about the email looks wrong. There is no malicious link to click. The sender's address is the real address. The language matches the relationship. The timing matches the normal cycle. The only defense is verification through a separate channel — picking up the phone and calling a known number — and that is the step that gets skipped because everyone is busy.

What it costs

BEC is the single most expensive cybercrime category by total losses. The FBI's IC3 report for 2023 attributed $2.9 billion in reported losses to BEC, with an average loss per incident of approximately $137,000. For small businesses, the loss is often unrecoverable — wire transfers move quickly, and once money has left the country it is rarely returned. Insurance recovery is partial at best. Some businesses do not survive the loss; many cut staff or take on debt to absorb it.

Industry case

Appendix C contains a case from a 12-person construction company that lost $87,000 to a vendor email compromise over a single Wednesday. See Appendix C.1 (Construction).

2.3 Ransomware

What it is

Ransomware is malicious software that encrypts the files on your computers and servers, making them unreadable, and demands a payment — usually in cryptocurrency — for the decryption key. Modern ransomware also typically steals copies of your data before encrypting, so even if you can restore from backup, the attackers threaten to publish the stolen data unless you pay. This is sometimes called "double extortion."

Ransomware is no longer a hobbyist threat. It is operated by organized criminal groups using a business model called ransomware-as-a-service: a core team develops the malware, partners ("affiliates") deploy it against victims, and they split the proceeds. Some of these groups have customer support, payment portals, and negotiation processes. They are functioning criminal businesses.

How it actually happens

An employee at a small medical practice clicks a link in what appears to be a Microsoft 365 password reset email. The link installs malware on her computer. The malware does not act immediately. It

quietly establishes communication with the attackers' servers and waits, sometimes for weeks or months, while the attackers map the practice's network — what computers exist, what files are on them, what backups are running, what the patient database looks like. When they have understood the environment, they strike: simultaneously, every computer in the practice is encrypted, the network is severed from any external backup, and a ransom note appears demanding payment. The practice cannot access patient records, schedule appointments, process insurance claims, or operate.

The attackers have already copied the patient data and threaten to publish it on a public leak site if the ransom is not paid. The practice now faces a HIPAA breach reporting obligation regardless of whether they pay.

What it costs

Ransom demands against small businesses typically range from $50,000 to $500,000. Whether the ransom is paid or not, the operational disruption usually runs 7 to 21 days. Recovery costs (incident response, system rebuild, legal counsel, regulatory notification, customer communication) routinely run 2 to 5 times the ransom amount. The 2024 Sophos State of Ransomware report found that the average total cost of recovery, excluding ransom, was $2.73 million across all sectors. For small businesses the figure is lower in absolute dollars but often more devastating relative to revenue.

Industry case

Appendix C contains a case from a 14-person dental practice whose ransomware incident closed the practice for 11 days and ultimately led to the sale of the practice. See Appendix C.5 (Healthcare — Dental).

2.4 Credential Theft and Password Reuse Attacks

What it is

Credential theft is the broad category of attacks that steal usernames and passwords. The most damaging form, and the most common, is not theft from your business directly — it is theft from somewhere else. When your employee uses the same password for the company email that they use for a fitness app, and that fitness app gets breached, the attackers now have a working password for your company email. They run automated tools that test stolen credentials against thousands of business email systems. This is called "credential stuffing," and it succeeds against businesses that have done nothing wrong themselves.

Related attacks: brute force attacks (trying many passwords against one account), password spraying (trying one common password against many accounts), and session hijacking (stealing the active session token rather than the password itself).

How it actually happens

Three years ago, your office manager created a LinkedIn account using her work email and her usual password — the one she also uses for the office email. Last year, a database of credentials stolen from various consumer websites was published on a hacker forum. Her credentials were in it. Six months later, an automated tool tested those credentials against Microsoft 365 login. They worked. The attackers logged into her email, read it for a few weeks, and identified that she handled vendor payments. They then sent a message from her account to your bookkeeper requesting a new vendor be set up — a vendor whose bank account they controlled. The first invoice from this "vendor" was paid before anyone realized the office manager's account had been compromised. None of this was the office manager's fault in any sense she would recognize. She used a password she liked and could remember. The fitness app that originally lost her password was a household name.

What it costs

Direct losses from credential theft attacks vary widely depending on what the attacker does once inside — anywhere from a few hundred dollars (a compromised account used to send phishing) to tens or hundreds of thousands (where the credentials enable wire fraud or data theft). The structural cost is broader: a compromised account is often used as a launching point for further attacks, and the original compromise may not be discovered for weeks or months. By the time it is found, the attacker may have established additional access points throughout the business.

Industry case

Appendix C contains a case from a 7-person real estate brokerage where a single reused password led to a multi-month compromise and $43,000 in fraudulent commission redirections. See Appendix C.9 (Real Estate).

2.5 Supply Chain Compromise

What it is

Supply chain compromise is the category of attacks that reach you through your vendors, software providers, or service providers — and the category of attacks that reach your customers through you. There are two perspectives on the same problem, and a small business is both a target and a vector.

As a target: the software you use, the cloud services you depend on, and the IT provider that manages your computers all become potential entry points. If your accounting software vendor pushes a malicious update, it runs on your systems. If your email provider gets breached, your email may be readable to attackers. If your IT support company has its remote management tools compromised, every customer of that IT company is exposed at once.

As a vector: your business has access to your customers' systems, data, or trust. If you are compromised, attackers can use that access to reach your customers. If you are a contractor with

access to a Fortune 500 client's systems, you are a path into that client. If you are an accounting firm with access to dozens of clients' financials, you are a path into all of them. If you are a small marketing firm that sends emails on behalf of your clients, you are a path into their customer relationships.

How it actually happens

A 6-person marketing agency uses a popular email marketing platform to send campaigns on behalf of about 30 small business clients. The platform requires the agency to upload customer email lists. One day, the agency receives a notification from the platform: "unusual activity detected, please re-verify your password." The owner clicks the link, enters her credentials. The link was a phishing page — not from the platform, but from attackers who had researched which marketing platform the agency used. With her credentials, the attackers log into the real platform, send phishing emails to all 30 clients' customer lists, and burn the agency's reputation in a single afternoon. The agency did not breach the email platform. The email platform was not breached. But the agency's clients were all attacked through the agency, and from each client's perspective, the agency was the source of the breach.

What it costs

Supply chain incidents are particularly painful because the cost is often disproportionate to the size of the original breach. The agency in the example above lost no money to the attackers directly — but lost about half its clients within 60 days, as those clients understandably questioned whether the agency could be trusted with their customer relationships. The reputational damage from being the entry point for an attack on your customers is often greater than the damage from being attacked directly.

Industry case

Appendix C contains cases that illustrate both directions: a 6-person IT services company whose remote management tool was compromised, exposing all of their clients (Appendix C.15), and a small marketing agency whose breach harmed dozens of downstream clients (Appendix C.13).

2.6 Insider Threat

What it is

Insider threat is the category of harmful actions taken by people who already have legitimate access to your systems. The popular conception of insider threat is the disgruntled employee who deliberately steals or sabotages — and that does happen — but the far more common form is accidental: the employee who emails the wrong file to the wrong person, the contractor who keeps a copy of the customer database after the engagement ends, the bookkeeper who saves the master password file to a personal cloud drive "for safekeeping." There is also a middle category: employees

who break the rules without malicious intent because the rules were inconvenient and nobody was watching.

Related attack: account takeover. When a legitimate employee's account is compromised by an outsider, the resulting actions appear as insider activity in your systems. Most insider-looking incidents are actually outsider attacks running through compromised insider accounts.

How it actually happens

An office manager at a 22-person professional services firm has been there for eight years. She has access to nearly everything because over time she has been granted access to nearly everything — and nobody has ever taken anything away. She is not malicious. But when the firm misses bonus expectations one year, and her cousin offers a job at a competitor, she copies the firm's complete client list and project history to a personal USB drive on her last Friday. The competitor uses the list to make targeted approaches to the firm's clients. By the time the firm understands what happened, six clients have moved their work.

A different scenario: that same office manager has not gone anywhere. But her email account is compromised by attackers via a phishing email. The attackers, now operating with her access, do the same thing — copy the client list, sell it on a hacker forum or use it for targeted attacks. From the firm's perspective, the activity logs show "office manager downloaded client database." It looks like insider exfiltration. It is not. But the damage is the same.

What it costs

Insider incidents (genuine and apparent) are among the most damaging for small businesses, because insiders have legitimate access and know what is valuable. The cost includes immediate damage (data loss, theft, sabotage), legal cost (litigation against former employees, regulatory exposure), and trust cost (other employees become harder to trust, the workplace culture is damaged). The Ponemon Institute's 2024 report on insider threats found average organizational cost of insider incidents at $16.2 million across all sizes — small business numbers are smaller in absolute terms but proportionally similar.

Industry case

Appendix C contains a case from a 22-person professional services firm where an office manager's compromised account was used to exfiltrate the client database (Appendix C.10), and a separate case from a small medical practice where a departing employee took patient information in violation of HIPAA (Appendix C.4).

2.7 Deepfake and AI-Enabled Social Engineering

What it is

This is the newest category and the one your defenses are least prepared for. Generative AI has industrialized social engineering. The same technology that produces a passable LinkedIn post can produce a passable phishing email, a convincing voice recording of your CEO, or a video of a person who does not exist. The era in which phishing emails could be identified by spelling errors and awkward grammar is ending. The era in which a voicemail from your boss authorizing a wire transfer is presumed to be genuine is also ending.

Three specific variants are now in active use against small businesses: AI-generated phishing emails (indistinguishable from professional writing, customized per recipient using publicly available information); deepfake voice impersonation (a few seconds of audio from a public source — a podcast appearance, a webinar, a video on the company website — is enough to clone a voice); and deepfake video on conference calls (where the "CEO" you see and hear on the call is an AI impersonation).

How it actually happens

The CFO of a 40-person engineering firm receives a Microsoft Teams call from the CEO. The CEO is on a flight, the connection is poor, the video is glitchy, but the voice and face are recognizable. The CEO explains there is an urgent acquisition opportunity, confidential, the deposit must be wired today to secure exclusivity, will explain everything Monday. The CFO authorizes a $290,000 wire transfer. The CEO is, in fact, on a flight — and has no knowledge of any of this. The Teams call was a deepfake, the audio cloned from the CEO's TEDx talk three years earlier, the video synthesized from his publicly available LinkedIn headshot.

This is no longer a hypothetical scenario. It has been documented multiple times in 2024 and 2025, with reported losses ranging from $25 million (a 2024 Hong Kong incident at the multinational firm Arup) down to small business losses in the $50,000 to $500,000 range.

What it costs

Direct loss tracks with the wire amount that was authorized. The structural cost is broader: deepfakes erode the foundational trust that business communication runs on. If you cannot trust a video call from your CEO, you have to install verification procedures that slow down legitimate business communication. The defense is process — a callback to a known number for any unusual financial instruction, a code word for high-stakes verbal authorizations, a written confirmation requirement for wire transfers above a threshold. These are inconvenient. They are also, increasingly, mandatory.

Industry case

Appendix C contains a case from a 40-person engineering firm that lost $290,000 to a deepfake CEO call (Appendix C.12).

2.8 The Shape of the Problem

Reading these seven threats in sequence may have produced a particular feeling: that there are too many of them, that they are too varied, that defending against all of them is too much. That feeling is mistaken, and it is the most important thing to correct before reading further.

These are not seven separate threats. They are seven manifestations of the same underlying pattern: someone gets access they should not have, and uses it to take something. The seven entry points differ; the destination is the same. And the defenses against them overlap heavily. Multi-factor authentication on email defeats phishing, BEC initiated by credential theft, and most credential reuse attacks. A disciplined backup practice mitigates ransomware, accidental insider data loss, and many forms of supply chain compromise. A verification procedure for wire transfers defeats BEC, deepfake-initiated wire fraud, and certain insider exfiltration patterns.

Twenty percent of controls block roughly 80 percent of attacks across all seven threat categories. The framework's job — particularly Section 5's implementation roadmap — is to identify that 20 percent and put it within reach. You do not have to defeat every threat. You have to make yourself harder to attack than the next business in the attacker's queue. The attacker is running a business; if you cost more to compromise than the next target, the attacker moves on.

That is the offer. Not perfection. Not invulnerability. Substantially harder to attack than your peer businesses, achievable with 30 minutes a week, free or low-cost tools, and the willingness to build a habit. The next sections explain how.

Section 3: Risk Assessment

Time required for owner: 30 minutes (micro-business version) or 3 hours (full version, can be split across multiple sittings).

A cybersecurity risk assessment answers three questions: What do you have that is worth protecting? What could go wrong with it? Where should you spend your limited time and money first?

This section gives you two ways to do a risk assessment: a 30-minute version designed for businesses under 10 employees, and a structured four-step methodology for larger SMBs. Both produce a usable risk picture. The 30-minute version sacrifices some completeness for speed; the full version sacrifices some speed for completeness. Pick the one that matches your business and your available time.

3.1 The 30-Minute Risk Assessment

Designed for businesses with fewer than 10 employees and no dedicated IT staff.

If you have a few hours, do the full assessment in Section 3.2. If you have 30 minutes, do this version. It will not be as thorough — but it will produce a real, useful risk picture, which is dramatically better than no risk picture, which is what most micro-businesses have.

Sit down with a notepad or open the Risk Assessment template (Appendix D, Template 2). Set a timer if it helps. Answer these questions in order:

Question 1 (5 minutes): What would actually hurt your business?

List the things that, if they went wrong, would seriously damage or end your business. Be specific. Think in terms of consequences, not technologies. For most businesses, the answer includes some or all of the following:

- Losing access to your operating systems for a week (you cannot run the business while waiting for recovery).
- Losing your customer list, customer payment information, or customer trust through a public breach.
- Wiring money to an attacker who impersonated a vendor, customer, or executive.
- Having an employee account compromised and used to attack your customers.
- Losing intellectual property, trade secrets, or proprietary work product.

- Failing a security questionnaire from a major customer and losing that contract.
- Being subject to a regulatory penalty (HIPAA, state privacy law, PCI DSS) due to a data incident.

Pick the three that are most concerning to your specific business. Write them down. These are your priority risks.

Question 2 (10 minutes): Where is the valuable data?

List, in plain language, where your business keeps the data that matters most. Most small businesses use:

- Email (Microsoft 365, Google Workspace, or similar) — often the most valuable target, because attackers can use email access to impersonate you.
- Accounting software (QuickBooks, Xero, Wave) — contains banking information, customer payment details, financial records.
- Customer relationship management (CRM) software (HubSpot, Salesforce, or similar) or a spreadsheet — contains customer contact information and history.
- Cloud file storage (Google Drive, Microsoft OneDrive, Dropbox) — contains contracts, internal documents, possibly intellectual property.
- Industry-specific software (medical records software, legal practice management, construction estimating software, etc.)
- Employee laptops and phones — copies of much of the above.
- Backup locations — wherever you back up the data.

For each location, write a one-line note: who can access it, whether it has multi-factor authentication enabled, and whether it is backed up somewhere separate.

Question 3 (10 minutes): Where are the obvious gaps?

Compare your answer to Question 2 against this list of common gaps. For each one, mark whether your business has it, does not have it, or you are not sure:

- ☐ Multi-factor authentication is enabled on all email accounts.
- ☐ Multi-factor authentication is enabled on the accounting software.
- ☐ Every employee has their own login (no shared accounts, no shared passwords).
- ☐ Former employees no longer have access to anything (including email forwarding rules they may have set up).
- ☐ Computers automatically install security updates.
- ☐ Backups exist for the most important data, in a location separate from the main system.
- ☐ You have personally tested that you can restore from a backup within the last six months.

- ☐ Employees know to verify any unusual financial instruction (wire transfer, vendor change, urgent payment) by phone using a known number, before acting on it.
- ☐ You can name the IT person or company who would be the first call if something went wrong.
- ☐ If your computers were all encrypted by ransomware tomorrow morning, you have at least a rough idea of what you would do.

Every "no" or "not sure" answer is a gap. Every gap is a risk.

Question 4 (5 minutes): Pick three things to fix this month.

From your gap list, pick three. Pick the three that, if you fixed them, would meaningfully reduce the risks you identified in Question 1. For most businesses with a typical gap profile, the three to start with are:

1. Enable MFA on every email account in the business — every account, not just the owner's.
2. Verify that backups exist for the data you cannot afford to lose, and test that you can actually restore from them.
3. Establish a verification rule: any unusual financial instruction received by email must be confirmed by a phone call to a known number before action is taken. Communicate this rule to everyone who handles money.

If you do nothing else this month, do those three. They are the highest-impact, lowest-cost actions for the typical small business. Section 5 covers them in implementation detail.

3.2 The Full Risk Assessment Methodology

Designed for SMBs with 10 to 50 employees, or for any business that has time for a more thorough assessment.

The full risk assessment follows four steps: identify what you have, identify what could threaten it, identify where you are vulnerable, and prioritize what to do about it. Each step has its own template in Appendix D.

3.3 Step 1: Asset Inventory

Before you can protect your assets, you have to know what you have. Most small businesses underestimate the complexity of their digital footprint by a factor of three. The asset inventory exercise is uncomfortable in part because it makes the actual scope visible. Do it anyway.

> **Time required**
>
> 1 to 2 hours, depending on business size. Use the Asset Inventory template (Appendix D, Template 1).

Hardware Assets

- ☐ All desktop and laptop computers — make, model, owner, primary location.
- ☐ All mobile devices used for business (phones, tablets) — including personal devices that access company email or data.
- ☐ All network equipment — router, modem, switches, firewalls, wireless access points.
- ☐ All servers, including network-attached storage (NAS) devices, on-site or hosted.
- ☐ Printers, scanners, and other networked peripherals.
- ☐ Internet-connected devices (cameras, smart thermostats, voice assistants, smart locks) — often overlooked, often the weakest point on the network.
- ☐ Any device that stores or processes sensitive customer or business data, regardless of category.
- ☐ Distinguish company-owned from employee-owned (BYOD) devices.

Software and Cloud Service Assets

- ☐ All business-critical software applications and their versions.
- ☐ All cloud services in use (Microsoft 365, Google Workspace, accounting platforms, CRM, project management, file storage, payroll, HR, marketing tools, e-commerce platforms).
- ☐ Industry-specific software (medical records, legal practice management, construction estimating, etc.).
- ☐ Any active subscription or service that holds business data.
- ☐ Legacy software still in use that is no longer supported by the vendor — these are major vulnerabilities.

Data Assets

- ☐ Where customer personal information is stored (names, contact details, identifiers).
- ☐ Where customer payment information is stored or processed.
- ☐ Where employee personal and payroll information is stored.
- ☐ Where financial records and accounting data are stored.
- ☐ Where intellectual property and proprietary work products are stored.
- ☐ Where backups are stored — local devices, external drives, cloud backup services.

Account and Access Assets

- ☐ All user accounts across all systems and services — current employees, former employees, contractors, vendors, third parties.
- ☐ Administrative accounts (accounts with elevated privileges) — these are the highest-value targets.
- ☐ Shared accounts and group mailboxes — these violate good practice but commonly exist.
- ☐ Service accounts and integration accounts (used by automated systems, often forgotten about).

3.4 Step 2: Threat Identification

With the asset inventory in hand, identify which threats are most relevant to your business. Use the threat list below as a starting point. Section 2 of this framework explains each threat in detail; Appendix E provides a quick-reference catalog of every threat category an SMB might encounter.

> **Time required**
>
> 30 minutes.

Threats Most SMBs Face

- ☐ Phishing — fraudulent emails designed to steal credentials or install malware.
- ☐ Business email compromise — wire fraud through email impersonation or compromise.
- ☐ Ransomware — malware that encrypts files and demands payment.
- ☐ Credential theft and password reuse — attackers using passwords stolen from other breaches against your accounts.
- ☐ Supply chain compromise — attacks reaching you through vendors or software providers.
- ☐ Insider threat — accidental or intentional harm by people with legitimate access.
- ☐ Physical theft of devices — laptops, phones, external drives stolen from cars, offices, hotel rooms.
- ☐ Social engineering by phone or text — attackers calling employees or sending text messages to manipulate action.

Industry-Specific Threats

In addition to the general threats above, certain industries face elevated or specific threats:

- Healthcare and dental practices: HIPAA breach exposure, ransomware against patient records, prescription fraud.

- Legal services: confidentiality breaches, wire fraud through escrow accounts, target for client information theft.
- Construction and trades: BEC through subcontractor relationships, theft of bid information, building security system compromise.
- Real estate: wire fraud at closing, escrow account targeting, customer financial information theft.
- Retail and e-commerce: payment card theft, account takeover of customer accounts, inventory and shipping fraud.
- Professional services (accounting, financial advisory): tax fraud, client financial information theft, IRS impersonation.
- Manufacturing: intellectual property theft, supply chain disruption, industrial control system targeting.

Industry-specific incident cases for over 25 sectors are in Appendix C. Read the cases relevant to your industry; they will surface threat patterns specific to your business model.

3.5 Step 3: Vulnerability Assessment

A vulnerability is a weakness that a threat could exploit. The asset inventory tells you what you have; the threat list tells you what could go wrong; the vulnerability assessment connects them. Where, specifically, is your business exposed?

> **Time required**
>
> 1 to 2 hours.

For a small business without specialized assessment tools, vulnerability assessment is largely a structured walk-through using the categories below. The goal is not to find every theoretical vulnerability — that is what enterprise penetration testers do. The goal is to identify the obvious, common gaps that account for the vast majority of actual breaches against small businesses.

Authentication Vulnerabilities

- ☐ Are there accounts (especially email and accounting software) without multi-factor authentication?
- ☐ Are passwords reused across business and personal accounts?
- ☐ Are default passwords still in place on any device or system (router, network camera, printer)?
- ☐ Are there shared accounts where multiple people use the same login?

Access Control Vulnerabilities

- ☐ Do any former employees still have access to email, files, or applications?
- ☐ Do contractors or vendors have access that should have been revoked when their work ended?
- ☐ Do employees have access to systems they no longer need (because they changed roles but their access did not change)?
- ☐ Are administrative privileges given to people who do not need them?

Data Protection Vulnerabilities

- ☐ Are sensitive data (customer payment information, healthcare records, financial records) protected with encryption when at rest and in transit?
- ☐ Are backups verified to actually work? When was the last successful test restoration?
- ☐ Is sensitive data stored in places it should not be — personal email accounts, employee personal cloud storage, USB drives?
- ☐ Are old devices disposed of securely (data wiped or drive physically destroyed)?

Endpoint and Network Vulnerabilities

- ☐ Do all computers have up-to-date antivirus or endpoint protection?
- ☐ Are operating systems and software receiving automatic security updates?
- ☐ Are unused services and software removed from computers?
- ☐ Is the wireless network secured with a strong password and using current encryption (WPA2 or WPA3)?
- ☐ Is guest Wi-Fi separated from the business network?

Process and People Vulnerabilities

- ☐ Is there a written policy for how to respond to suspicious emails?
- ☐ Is there a verification procedure for unusual financial instructions (wire transfers, vendor changes)?
- ☐ Have employees received any cybersecurity training in the last year?
- ☐ Does someone in the business know how to recognize a security incident and what to do first if one occurs?

3.6 Step 4: Risk Prioritization

With vulnerabilities identified, the final step is prioritization: which gaps should you fix first? This is where most enterprise risk methodologies become elaborate, with quantitative scoring, weighted

formulas, and risk registers running into hundreds of entries. For a small business, a simpler approach works: rate each gap by its likelihood and its potential business consequence, and act on the high-likelihood, high-consequence items first.

> **Time required**
>
> 30 minutes.

The Risk Prioritization Matrix

For each vulnerability identified, rate two things:

Likelihood — how likely is it that this vulnerability will be exploited?

- Likely: this kind of attack happens regularly to businesses like yours.
- Possible: this kind of attack happens occasionally, depending on circumstances.
- Unlikely: this kind of attack is rare for businesses like yours.

Business consequence — what happens if this vulnerability is exploited?

- Could close the business: catastrophic — bankruptcy, legal liability that destroys the business, total loss of customer trust.
- Lose major customers: serious — significant contracts at risk, reputational damage, loss of certification.
- Regulatory penalty: substantial — fines, mandatory disclosure, ongoing oversight.
- Operational disruption: meaningful — days or weeks of impaired operations, recovery costs in the tens of thousands.
- Recoverable: limited — inconvenient and costly but absorbed without lasting damage.

The intersection of likelihood and consequence determines priority:

Consequence \ Likelihood	Unlikely	Possible	Likely
Could close the business	High	Critical	Critical
Lose major customers	Medium	High	Critical
Regulatory penalty	Medium	High	High
Operational disruption	Low	Medium	High

Consequence \ Likelihood	Unlikely	Possible	Likely
Recoverable	Low	Low	Medium

Address the items in this order: Critical immediately, High within 30 days, Medium within 90 days, Low when convenient or as part of routine maintenance. The implementation roadmap in Section 5 is structured around the same priority framework — Phase 1 corresponds to the Critical and High items, Phase 2 to Medium, Phase 3 to Low and to depth-of-protection improvements.

A Worked Example

A 14-person dental practice does an asset inventory and discovers, among other vulnerabilities, that two former employees still have access to the practice email system. The practice rates this:

- Likelihood: Likely. Former employees with active access is a common point of incident; either the former employee uses the access deliberately, or their account is compromised by an outsider who exploits it.
- Consequence: Could close the business. Email access enables impersonation that could trigger HIPAA violations and patient information disclosure. The combination of regulatory penalty, patient trust damage, and remediation cost can be existential for a small practice.
- Priority: Critical. Address immediately.

The practice revokes the access that afternoon. This is the kind of finding the framework is designed to surface. It cost nothing to fix and removed a substantial risk.

3.7 What to Do With the Results

The output of a risk assessment is a prioritized list of gaps. The next step is closing them. Section 4 (Security Policies) provides the policy frameworks; Section 5 (Implementation Roadmap) provides the phased plan; Section 6 (Building the Discipline) provides the operational practices that keep gaps from reopening over time.

Schedule the next risk assessment now. For most small businesses, an annual risk assessment is appropriate, with a quarterly check-in on whether anything has materially changed (new systems, new employees, new vendors, new regulatory obligations). Add the annual review to your calendar before you put this document down.

Section 4: Security Policies

Time required for owner: 2 hours to read and adapt; ongoing time for implementation tracked per policy.

A security policy is a written rule that governs how your business handles information and technology. Without policies, security depends on individual judgment — which is inconsistent, unpredictable, and forgotten the moment the person who held it leaves. Written policies do four things: they create accountability, they set clear expectations for everyone, they form the basis of training, and they give you something to enforce.

This section provides four core policies. They are not a complete policy library — large enterprises have dozens of policies — but they cover the controls that actually matter for the threats described in Section 2. Each policy is presented in three parts: why it exists (the business rationale), what it requires (the controls), and how to implement it (free-tier options, paid options, and when to upgrade).

Adapt the language to your business. Where this section uses placeholder names, replace them with your business name. Where it specifies thresholds (number of days, password length), adjust them to your circumstances if needed — but adjust thoughtfully, not reflexively. The defaults are reasonable starting points.

4.1 Why Your IT Provider Is Not Enough

Before reading the four policies that follow, address the most common objection: "We have an IT provider who handles security. Why do we need policies?"

This objection is the most dangerous illusion in small business cybersecurity. It feels reassuring; it is not protective. Here is why:

IT Support and Cybersecurity Are Different Professions

Your IT provider — whether an in-house IT person, an outsourced managed service provider, or your nephew who is good with computers — is a different professional than a cybersecurity practitioner. The skills overlap at the edges, but the core of each profession is different. IT support is about keeping things running: the email is delivered, the printer prints, the computers are not slow. Cybersecurity is about thinking adversarially: how would someone break in, what would they do once inside, what evidence would they leave, how would we know.

Most IT providers do not have specialized cybersecurity training. They install antivirus, configure firewalls, and apply patches — all of which are good and necessary, and none of which constitute a cybersecurity program. Threat modeling, security architecture, incident response planning, security awareness training, policy development, and continuous monitoring are not in the typical IT support job description.

The Incentive Structure Is Wrong

Your IT provider is paid to keep things running. Their performance is measured by uptime and ticket resolution time. They are not paid for finding vulnerabilities; they are paid for not letting things break. Many genuinely concerning security findings — outdated software, weak permissions, dormant accounts — represent extra work for the IT provider with no corresponding revenue. This is not a moral failing on their part; it is what their business model produces.

Some MSPs Do Cybersecurity Well — Most Do Not

A growing number of managed service providers genuinely offer cybersecurity services and have the staff and processes to back it up. They will charge accordingly — typically $100 to $500 per employee per month for a meaningful security program, on top of standard IT support fees. If you are paying $50 per user per month and being told that cybersecurity is included, you are receiving the IT support, not the cybersecurity.

How to tell the difference. Ask your IT provider these questions:

1. "Can you describe our incident response plan? What happens in the first hour if our email is compromised?"
2. "What threat modeling have you done for our specific business — what are our most likely attack scenarios?"
3. "Which of your staff hold cybersecurity certifications (CISSP, CISM, Security+, GIAC certifications)?"
4. "Do you provide written cybersecurity assessments — and may I see a sample?"
5. "What security awareness training do you provide for our employees?"

If the answers are vague, evasive, or treated as unusual questions, your provider does IT support, not cybersecurity. That is not a reason to fire them — IT support is valuable. It is a reason to recognize that you still need the policies and practices in this framework, because no one else is providing them.

The Bottom Line

This is principle 9 of the framework, stated plainly: IT support and cybersecurity are different professions. Your IT provider may be excellent at the IT support part. The cybersecurity part is your responsibility, even if you delegate the implementation. The policies in this section are written for

the person responsible for the cybersecurity outcome — which is you, the business owner — even if the day-to-day work is done by someone else.

4.2 Password and Authentication Policy

Why This Policy Exists

Stolen and weak passwords are the single largest cause of business email compromise, ransomware, and data theft incidents against small businesses. Multi-factor authentication — requiring a second proof of identity beyond the password — defeats the overwhelming majority of these attacks. The 2024 Microsoft Digital Defense Report estimated that MFA blocks 99.2 percent of automated account compromise attempts. This policy exists because it is the highest-impact, lowest-cost control your business will adopt.

Without this policy: a single password reused from a website breach can give attackers access to your email, your accounting system, your customer database, and your bank accounts.

With this policy: an attacker who steals a password still cannot access your accounts, because they cannot also intercept the second factor on the employee's phone.

Policy Requirements

- ☐ Multi-factor authentication is required on all email accounts (Microsoft 365, Google Workspace, or any other email system).
- ☐ Multi-factor authentication is required on all accounting and financial systems.
- ☐ Multi-factor authentication is required on all cloud services that hold business data (CRM, file storage, project management, payroll, HR systems).
- ☐ Multi-factor authentication is required on all administrative accounts (any account with elevated privileges).
- ☐ Multi-factor authentication is required for all remote access to business systems.
- ☐ Passwords are at least 12 characters long, contain a mix of character types, and do not contain the user's name, business name, or obvious patterns.
- ☐ Passwords are not reused across business accounts or between business and personal accounts.
- ☐ A password manager is provided to and used by all employees who handle business credentials.
- ☐ Default passwords on all devices and systems (routers, network cameras, printers, IoT devices) are changed before deployment.
- ☐ Each user has a unique account; shared accounts and shared passwords are prohibited.
- ☐ Inactive accounts are disabled after 30 days of non-use.

- ☐ Terminated employees' access is revoked the same day employment ends.

Implementation

Free and low-cost options for each control:

Control	Free option	Low-cost option	When to upgrade
Password manager	Bitwarden Free	Bitwarden Teams ($4/user/month)	When you need centralized administration, secure sharing, or compliance reporting
Multi-factor authentication	Microsoft Authenticator, Google Authenticator (free apps); built-in MFA in Microsoft 365 and Google Workspace	Duo Free for up to 10 users; Duo Essentials beyond that ($3/user/month)	When you need conditional access policies, single sign-on, or compliance attestation
MFA hardware tokens	Not applicable	YubiKey 5 NFC ($55 per key, one-time purchase)	When you have phishing-resistant authentication requirements (recommended for owner and finance roles regardless)

> **Recommendation for most small businesses**
>
> Use Bitwarden Free for the password manager, Microsoft Authenticator or Google Authenticator (whichever matches your email provider) for MFA, and consider one or two YubiKey hardware tokens for the owner and the bookkeeper or anyone with access to financial systems. Total cost: $0 to $110, one-time. This combination defeats most automated attacks and a substantial fraction of targeted attacks.

4.3 Access Control Policy

Why This Policy Exists

People accumulate access over time. New systems are added; new responsibilities require new permissions; old responsibilities end without anyone removing the corresponding access. Within two or three years, the typical employee at a small business has access to substantially more systems than they actually use, and former employees and contractors often retain access long after their work has ended. Each unnecessary access point is an attack surface.

Without this policy: an attacker who compromises any single account inherits whatever that account has access to — including everything the user has accumulated over years of unmanaged permission growth.

With this policy: each account has only the access it currently needs; departed users have no access at all; sensitive systems are reachable only by people whose work requires them.

Policy Requirements

- ☐ Access to systems and data is granted only when needed for current job function (the principle of least privilege — give people only the access their job requires).
- ☐ Access rights are reviewed when an employee changes roles or responsibilities; access no longer needed is removed.
- ☐ All access is revoked the same day an employee leaves the business — including email, file storage, applications, and any saved or stored credentials.
- ☐ A formal onboarding and offboarding checklist exists, lists all systems requiring access changes, and is followed for every personnel change.
- ☐ Administrative accounts (with elevated privileges) are separated from regular user accounts; admins use their regular account for daily work and switch to the admin account only when needed.
- ☐ Remote access to business systems requires both VPN and multi-factor authentication.
- ☐ Third-party vendor access is time-limited (with a defined expiration date), monitored, and revoked when the engagement ends.
- ☐ Access to critical systems is logged; logs are retained for at least 90 days.
- ☐ Physical access to network equipment, servers, and storage devices is restricted.
- ☐ Workstations lock automatically after 5 to 10 minutes of inactivity.

Implementation

Control	Free option	Low-cost option	When to upgrade
Account management	Built into Microsoft 365	Same — no upgrade	Only at enterprise

Control	Free option	Low-cost option	When to upgrade
	and Google Workspace admin consoles	typically needed for SMB	scale (200+ users) or specific compliance requirements
VPN for remote access	Built into Windows (Windows Defender Firewall + native VPN); ProtonVPN Free	ProtonVPN Plus ($4.99/month per user); NordLayer ($7-14/user/month)	When you have many remote employees, multiple offices, or need site-to-site connectivity
Screen lock and device control	Built into Windows (Group Policy) and macOS (Configuration Profiles)	Microsoft Intune ($6/user/month) or Jamf Now ($4/device/month)	When you have BYOD employees or need compliance attestation
Access logging	Built-in audit logs in Microsoft 365 and Google Workspace	Same — typically sufficient	When you have compliance requirements (HIPAA, PCI DSS, SOC 2)

4.4 Data Protection Policy

Why This Policy Exists

Data is the most valuable asset most small businesses possess and the most valuable target for attackers. Customer information enables identity theft and fraud. Financial records enable wire fraud and tax fraud. Intellectual property enables competitive harm. Healthcare and legal records carry regulatory exposure. The data that runs your business is the data attackers want, and protecting it requires more than just keeping it on a computer that has antivirus.

Without this policy: sensitive data is scattered across employee laptops, personal email accounts, USB drives, and consumer cloud services, with no encryption, no backup discipline, and no idea who has access to what.

With this policy: sensitive data is identified, encrypted, backed up, and accessible only to people who need it — and you can recover from incidents because the backups actually work.

Policy Requirements

- ☐ Sensitive data is identified, classified, and inventoried (customer personal information, payment information, healthcare records, financial records, intellectual property, employee personal information).
- ☐ Sensitive data is encrypted at rest on all devices and storage locations (laptops, phones, external drives, cloud storage).
- ☐ Sensitive data is encrypted in transit (HTTPS for web traffic, TLS for email, encrypted protocols for file transfer).
- ☐ Full system backups are performed at least weekly; critical data is backed up daily.
- ☐ Backups are stored in a location physically and logically separate from the primary systems (offsite or cloud).
- ☐ Backup restoration is tested at least quarterly — actual files actually restored, not just the existence of backup files confirmed.
- ☐ Customer data retention is defined: how long it is kept, when it is deleted.
- ☐ Employees are prohibited from storing sensitive business data on personal devices, personal email accounts, or personal cloud storage.
- ☐ Sensitive data is not sent through unencrypted email, consumer messaging apps, or unsecured file sharing.
- ☐ Old devices are securely disposed of (drives wiped or physically destroyed before disposal or resale).
- ☐ A privacy policy is in place, accessible to customers, and compliant with applicable state privacy laws.

Implementation

Control	Free option	Low-cost option	When to upgrade
Disk encryption	BitLocker (Windows Pro and above, included); FileVault (macOS, included)	Same — no upgrade needed	Never for most SMBs — built-in encryption is excellent
Email encryption	Built into Microsoft 365 (Microsoft Purview Message Encryption with E3) and Google Workspace (S/MIME with Business Plus)	Virtru ($5-15/user/month) for any email provider	When sending highly sensitive data routinely, or when recipient encryption is required
Cloud backup	OneDrive, Google Drive,	Backblaze	When data volume

Control	Free option	Low-cost option	When to upgrade
	Dropbox personal tier (limited storage)	($9/month/computer); IDrive ($79/year for 5TB); Veeam Backup for Microsoft 365 ($15-25/user/year)	exceeds free tier; when compliance requires immutable backups
Local backup	External hard drive ($60-150 one-time)	Synology NAS with two drives ($400-800 one-time)	When you need fast restoration or have multiple terabytes of data

> **The 3-2-1 Backup Rule**
>
> Three copies of important data, on two different types of media, with one copy stored offsite. For most small businesses: original data on the working computers, second copy on an external drive or NAS in the office, third copy in cloud backup. The 3-2-1 rule has saved more small businesses from ransomware than any other single practice.

4.5 Incident Response Policy

Why This Policy Exists

Cybersecurity incidents are not rare events that happen to other businesses. They are routine, and the question is not whether you will have one but how you will handle it when you do. The decisions made in the first hour of an incident often determine whether it becomes a contained problem or an existential crisis. A ransomware infection that is isolated within the first hour costs ten times less than one that is allowed to spread for a day. A wire fraud caught within 24 hours is sometimes recoverable; one caught after a week almost never is.

Without this policy: when something goes wrong, the people closest to the problem panic, take actions that destroy evidence, fail to contact the right people, and discover only later that critical decisions were made by whoever happened to be most assertive at the moment.

With this policy: when something goes wrong, there is a clear playbook for the first hour, a clear list of who to call, a clear sequence of actions, and a clear path to controlled escalation.

Policy Requirements

- ☐ A written incident response plan exists, is accessible to the people who would need it, and is reviewed at least annually.

- ☐ Key contacts are documented in writing: IT support, cyber insurance carrier, legal counsel, banking institution fraud line, primary business contacts who would need to be notified.
- ☐ Employees know how to report a suspected security incident (a single point of contact, a single email address or phone number, and clear instructions to report rather than try to fix it themselves).
- ☐ A specific person is designated as the incident response lead for any incident; if that person is unavailable, an alternate is designated.
- ☐ There is a documented procedure for isolating a compromised device from the network (specifically: how to disconnect a computer from Wi-Fi and unplug it from any network cable).
- ☐ Evidence preservation is addressed (do not erase or rebuild affected systems before they have been examined; do not factory-reset compromised devices).
- ☐ Communication procedures are defined for notifying affected customers, partners, regulators (including state breach notification requirements applicable to your business).
- ☐ A post-incident review process is defined to capture lessons and adjust policies.
- ☐ Cyber insurance policy is in place, coverage is understood, and the carrier's incident notification requirements are documented.

The First Hour Playbook

If you discover or suspect a serious cybersecurity incident — ransomware, suspicious activity in your email, suspected wire fraud, unauthorized access — the following sequence of actions is the right starting point for the first hour. Customize the contact information and adapt to your business; print this and post it where it will be findable when needed.

6. If a specific computer is suspected of being compromised, disconnect it from the network — unplug the network cable and turn off Wi-Fi — but do not power it off and do not reboot it (powering off destroys evidence in memory).
7. Notify your designated incident response lead. If the incident affects financial systems or involves a wire transfer, also notify the owner immediately, regardless of time of day.
8. Call your IT provider. Tell them what you have observed and what you have done. Ask them to begin investigation.
9. If you have cyber insurance, call the insurance carrier's incident hotline. Many cyber insurance policies require notification within 72 hours; many also provide free incident response services to policyholders, but only if engaged through the carrier.
10. If financial fraud is involved, call your bank's fraud line. Wire fraud is sometimes reversible if reported within hours; almost never reversible after 48 hours.

11. Do not pay any ransom, do not negotiate with attackers, and do not engage with any communication from attackers without first speaking with your incident response lead, your IT provider, and your insurance carrier or legal counsel.
12. Begin a written log of what you observe and what actions you take. Time-stamp each entry. This log will be invaluable for investigation, insurance claims, and any required notifications.
13. Do not reboot, rebuild, or restore from backup yet. The instinct is to fix it; the right move is to investigate first. Restoring from backup before understanding the incident risks reintroducing the same compromise.

Implementation

Control	Free option	Low-cost option	When to upgrade
Cyber insurance	Not applicable	$1,500-5,000/year for small business policy with $1M coverage	When you have specific industry requirements (healthcare, legal, financial services) or contracts requiring higher coverage
Incident response plan template	FTC Small Business Cybersecurity Planner (free); CISA Cyber Essentials Toolkit (free)	Same — adapted to your business	When you have compliance requirements requiring formal IRP documentation
Incident response retainer	Not applicable	$2,000-10,000/year retainer with cybersecurity firm	When you have regulatory or contractual obligations to demonstrate IR readiness, or when the business is large enough that the time-to-response cost justifies a retainer

> **Cyber insurance is not optional for most SMBs**
>
> A small business policy with $1 million in cyber liability coverage typically costs $1,500-5,000

> per year — less than most businesses spend on general liability. Coverage typically includes incident response services, legal defense, regulatory notification costs, business interruption losses, and ransom payments (with carrier approval). Read the policy carefully: many policies exclude losses where the breach was enabled by lack of MFA, unsupported software, or other named omissions. Use the policy's requirements as a security checklist.

Section 5: Implementation Roadmap

Time required for owner: 30 minutes to read; implementation effort tracked per phase.

Improving cybersecurity does not happen overnight, but it also does not have to take years. This roadmap is structured so that a small business that completes Phase 1 — the first 30 days — is meaningfully more secure than a business that bought enterprise tools and never operationalized them. Phase 2 builds depth over the next 60 days. Phase 3 adds polish and resilience over the following 90 days.

Each control is marked with three indicators:

- Cost: Free / Low-cost / Paid. Free means no cost beyond what your business is likely already paying for (e.g., it is built into Microsoft 365). Low-cost means under $10 per user per month, or a small one-time cost. Paid means more than that.
- Essential star (★): Marked items are the highest-priority controls for micro-businesses (under 10 employees). If you have to choose, do these first.
- Time required: A rough estimate of the owner's time to implement, in addition to the technical setup time.

5.1 The Five Things to Do First

If you do nothing else from this entire framework, do these five things. Together they account for the majority of the protection you can achieve:

1. Enable multi-factor authentication on every email account in the business — every single one, including the accounts of part-time employees and contractors.
2. Enable multi-factor authentication on the accounting software, the CRM, and any cloud service that holds customer or financial data.
3. Confirm that you have backups of the data you cannot afford to lose, and personally test that you can restore at least one critical file from those backups.
4. Establish a verification rule for unusual financial instructions: any wire transfer, any vendor banking information change, any unusual payment instruction received by email must be verified by phone to a known number before action is taken. Communicate this rule to every employee who handles money.

5. Make a list of who you would call if something went wrong: IT provider, cyber insurance, primary bank's fraud line, legal counsel. Put it somewhere you would actually find it during a crisis.

These five actions are within the reach of any small business. They cost between $0 and $200. They take less than four hours of total effort, spread across an afternoon. They prevent or mitigate the majority of the most damaging attacks against small businesses. The rest of this roadmap is the deeper version of these same principles, but if you complete only these five and stop there, you have done more for your business's security than 80 percent of similar-sized businesses have done.

5.2 Phase 1: First 30 Days

Goal: close the highest-impact gaps with free or low-cost controls. Focus on items marked ★ if you have under 10 employees.

Authentication (Week 1)

- ☐ ★ Enable multi-factor authentication on every email account [Free, 2 hours]
- ☐ ★ Enable multi-factor authentication on accounting software [Free, 30 minutes]
- ☐ ★ Enable multi-factor authentication on all other cloud services holding business data [Free, 1-2 hours]
- ☐ ★ Audit all user accounts; disable accounts of former employees, ex-contractors, and unused service accounts [Free, 2 hours]
- ☐ ★ Change all default passwords on routers, network devices, printers, and any IoT devices [Free, 1 hour]

Endpoint Protection (Week 2)

- ☐ ★ Enable automatic security updates on all computers (Windows Update, macOS Software Update) [Free, 30 minutes per computer]
- ☐ ★ Confirm antivirus or endpoint protection is installed and active on every computer (Windows Defender is built-in and adequate for most SMBs) [Free, 30 minutes]
- ☐ ★ Enable automatic screen locking after 10 minutes of inactivity on all workstations [Free, 30 minutes]
- ☐ Enable disk encryption on all laptops (BitLocker on Windows Pro, FileVault on macOS) [Free, 30 minutes per device]

Backup Verification (Week 3)

- ☐ ★ Identify your most critical data (customer records, financial records, intellectual property) [Free, 1 hour]
- ☐ ★ Confirm that backups exist for that data; if not, set up backup immediately [Free to Low-cost, 1-3 hours]
- ☐ ★ Test restoration: pick one critical file, restore it from backup to a test location, confirm it opens and is correct [Free, 1 hour]

Awareness (Week 4)

- ☐ ★ Brief all employees on phishing recognition (15-minute meeting; show actual examples) [Free, 1 hour preparation + 15 minutes meeting]
- ☐ ★ Establish and communicate the wire transfer verification rule [Free, 30 minutes]
- ☐ ★ Establish and communicate how to report a suspected security incident (one named contact, one email address) [Free, 30 minutes]
- ☐ Identify and document the contact information for incident response: IT provider, cyber insurance, bank fraud line, legal counsel [Free, 1 hour]

> **Phase 1 budget reality check**
>
> Total cost for a typical 10-person business completing Phase 1: $0 if you already use Microsoft 365 or Google Workspace and an external hard drive for backup; up to about $200 if you need to purchase a backup drive and a couple of YubiKeys for the owner and bookkeeper. Total time: about 12-16 hours of owner involvement, plus technical setup time. Done in 30 days, this is more cybersecurity work than most small businesses do in years.

5.3 Phase 2: Days 31 to 90

Goal: build the structure that makes Phase 1's controls sustainable, and add the next tier of important controls.

Tools and Infrastructure

- ☐ ★ Deploy a password manager for the organization (Bitwarden Free or Bitwarden Teams); migrate employee passwords into it [Free or Low-cost, 4-8 hours]
- ☐ Set up a VPN for remote access if you have any remote workers (ProtonVPN or built-in Microsoft 365 features) [Free or Low-cost, 2-4 hours]

- ☐ Segment your network: separate guest Wi-Fi from the business network; consider a separate network for IoT devices [Free if your router supports it, 1-2 hours]
- ☐ Enable email security features if you use Microsoft 365 or Google Workspace: anti-phishing, anti-spam, attachment scanning, DMARC/SPF/DKIM (these are settings that prevent attackers from impersonating your domain — see Glossary) [Free, 2-3 hours]

Policies and Procedures

- ☐ ★ Document and adopt the Password and Authentication Policy (Section 4.2) [Free, 2 hours]
- ☐ ★ Document and adopt the Access Control Policy (Section 4.3) [Free, 2 hours]
- ☐ ★ Document and adopt the Data Protection Policy (Section 4.4) [Free, 2 hours]
- ☐ ★ Document and adopt the Incident Response Policy (Section 4.5) [Free, 2 hours]
- ☐ Conduct a formal employee security awareness training session covering phishing, BEC, password practices, and incident reporting [Free, 2 hours preparation + 1 hour session]
- ☐ Implement an offboarding checklist for departing employees (revoke access on day of departure) [Free, 1 hour]

Risk and Asset Management

- ☐ ★ Complete a full asset inventory (Section 3.3 / Appendix D Template 1) [Free, 4-6 hours]
- ☐ ★ Conduct a full risk assessment using the methodology in Section 3 [Free, 3-4 hours]
- ☐ Establish a quarterly backup test schedule [Free, ongoing]
- ☐ Establish a regular access review schedule (monthly recommended for small businesses) [Free, ongoing]

Vendor and Third-Party

- ☐ Inventory all third-party vendors with access to your systems or data [Free, 1-2 hours]
- ☐ Review whether each vendor's access is still needed and whether it should be reduced [Free, 1-2 hours]
- ☐ For any vendor handling sensitive data, request their security practices documentation (most vendors will provide this on request) [Free, 1-3 hours]

Insurance and Continuity

- ☐ Obtain or review cyber insurance: minimum $1 million in coverage for most small businesses; read the policy carefully and use its required controls as a checklist [Paid, $1,500-5,000/year, 2-4 hours to research and obtain]

> **Phase 2 budget reality check**

> Total cost for a typical 10-person business completing Phase 2: $1,500 to $5,000 (cyber insurance is the largest single line item); other items free or low-cost. Total time: about 30-40 hours of owner and IT involvement spread across 60 days.

5.4 Phase 3: Days 91 to 180

Goal: add depth and resilience; address controls that benefit organizations that have completed Phase 1 and Phase 2.

Advanced Detection and Response

- ☐ Implement endpoint detection and response (EDR) — software that watches every computer for suspicious activity, more sophisticated than basic antivirus [Free with Microsoft 365 Business Premium; otherwise Low-cost to Paid, $5-15/user/month]
- ☐ Enable centralized logging for critical systems; review logs at least monthly [Free, 4-6 hours initial setup]
- ☐ Conduct a phishing simulation to measure employee awareness (free options exist via PhishER, KnowBe4 free tier, or via your email provider) [Free or Low-cost, 4-8 hours]

Vulnerability Management

- ☐ Conduct a formal vulnerability assessment (an automated scan of your network and systems for known weaknesses) [Free with tools like OpenVAS for technical users; otherwise hire for $1,500-5,000]
- ☐ Establish a regular patching cadence beyond automatic updates: confirm critical patches are applied within 7 days, important patches within 30 days [Free, ongoing]

Privileged Access

- ☐ Implement privileged access management for administrative accounts (separate admin accounts from regular accounts; use admin accounts only when needed) [Free with Microsoft 365 admin features; otherwise Low-cost]
- ☐ Review who has administrative access; reduce to minimum necessary [Free, 1-2 hours]

Resilience Testing

- ☐ Conduct a full incident response tabletop exercise: walk through how you would respond to a ransomware attack, a wire fraud, and a data breach [Free, 2-4 hours]

- ☐ Conduct a complete restoration test: restore a non-trivial set of files (an entire computer or department) from backup [Free, 2-4 hours]
- ☐ Review and update the incident response plan based on findings [Free, 1-2 hours]

Vendor Risk

- ☐ Review all third-party contracts for security and data handling clauses; renegotiate where critical vendors have weak terms [Free, 4-8 hours]
- ☐ Establish a vendor security questionnaire for new vendors that will handle sensitive data [Free, 2-4 hours]

Compliance and Documentation

- ☐ If your industry has specific compliance requirements (HIPAA, PCI DSS, state privacy law), conduct a gap analysis against those requirements [Free for small-scale assessment; Paid for formal compliance work]
- ☐ Conduct an annual security review and update this framework's adoption [Free, ongoing]
- ☐ Consider a professional cybersecurity audit to validate your security posture, particularly if you have business reasons (customer requirements, M&A activity, insurance requirements) [Paid, $5,000-25,000 depending on scope]

> **Phase 3 budget reality check**
>
> Total cost for a typical 10-person business completing Phase 3: $0 to $5,000 if relying primarily on built-in tools and free assessments; up to $25,000 if engaging external auditors. Most SMBs do not need external audits unless required by customers, regulators, or insurance. Total time: about 20-30 hours over 90 days.

5.5 After Day 180: Maintenance and Continuous Improvement

Completing Phase 3 puts your business at a level of cybersecurity maturity that the vast majority of small businesses never reach. The challenge after Day 180 is maintaining that level. This is what Section 6 (Building the Discipline) addresses in detail: the weekly, monthly, quarterly, and annual practices that keep gaps from reopening over time.

On an annual basis, return to this roadmap. Re-do Phase 1's checks (have any default passwords crept back? are former employees properly offboarded? are backups still working?). Re-do the risk assessment. Adjust policies for changes in the business. The framework is not a one-time project; it is the structure of an ongoing practice.

5.6 Why 30, 90, and 180 Days?

The phase boundaries are chosen deliberately:

Thirty days is the limit of attention for a focused initiative in a small business. Anything that requires more than 30 days of momentum tends to be deprioritized when the next pressing matter arises. Phase 1 is designed to be completable in 30 days because completion in 30 days is realistic; completion in 90 days for the same content tends to mean completion never.

Ninety total days is the time required to actually establish habits, not just install tools. The controls in Phase 2 are not difficult; the difficulty is making them stick. Spending 60 additional days on policy adoption and training builds the patterns that turn Phase 1's controls from technical settings into behavioral norms.

One hundred eighty total days is the time required for at least one full assessment and verification cycle, including a backup test, an access review, and an incident response exercise. Phase 3 is the depth phase: it is where you find out whether the controls you adopted in Phase 1 still work in Phase 3, and where you build the redundancy that allows the system to withstand the inevitable changes (new employees, new vendors, new threats) that will accumulate in the following year.

After 180 days, the business has a working cybersecurity practice. Section 6 explains how to keep it working.

Section 6: Building the Discipline

Time required for owner: 20 minutes to read; 15 minutes per week to practice.

If you have implemented Sections 4 and 5, you have controls in place. The question this section answers is how to keep those controls working over time.

Cybersecurity in small business does not fail because the right controls were never bought. It fails because the right controls were bought, used for a while, and then stopped being maintained. The password manager is purchased and rolled out, and a year later half the employees have stopped using it because it was inconvenient on a particular Tuesday. The backup is set up and works perfectly for six months, until a software update silently breaks it and nobody notices for fourteen months — until the day it is needed. The MFA is enabled on every account, and then a new employee is onboarded with a temporary exception that becomes permanent. None of these failures are technical. All of them are failures of attention.

Enterprises solve this with software — governance, risk, and compliance platforms that track every control, alert on every drift, and produce reports that someone is paid to review. Small businesses do not have those platforms and cannot afford to operate them. What small businesses can afford is rhythm: a small, regular, disciplined practice that catches drift before it becomes failure.

This section gives you that rhythm. It is the most important section of the framework, and it is the part most cybersecurity guides do not include — because it is not a control, it is not a tool, and it is not a product. It is a habit.

6.1 The Weekly 15-Minute Security Review

When: Same time every week. Pick a time. Put it on your calendar. Defend it.

The most important practice in this framework is a 15-minute weekly review by the person responsible for security — typically the owner of a small business, or a designated employee in a slightly larger one. This review does not require expertise. It requires attention.

What to Check

Open each of the following in turn. For each, look at the past week. Note anything that is unusual or that you do not recognize. The full template is in Appendix D, Template 8.

Email administration (5 minutes)

- Sign-in activity for the email system. Most providers (Microsoft 365, Google Workspace) have a sign-in log accessible to administrators. Look for sign-ins from unfamiliar countries, unusual hours for any specific user, repeated failed sign-in attempts, and sign-ins from new devices.
- Forwarding rules. Attackers commonly create email forwarding rules in compromised accounts to silently exfiltrate email. Once a week, check the active forwarding rules across the business. Anything you do not recognize gets investigated.
- New mailbox rules. Beyond forwarding, look for new inbox rules that move messages to the Junk folder, the Archive, or rarely-checked folders. Attackers use these to hide their replies from the legitimate user.
- New OAuth permissions. Look at what third-party applications have been granted access to email accounts. New entries should be expected and explainable.

User accounts (3 minutes)

- Any new accounts created in the past week — were they created by you or with your knowledge?
- Any account changes (password resets, MFA disabled, permissions elevated) — were they expected?
- Any accounts that should have been disabled (former employees, ended contractor engagements) — confirm they are disabled.

Endpoint and update status (3 minutes)

- Software update notifications across the business — are systems applying updates, or are notifications piling up?
- Antivirus or endpoint protection alerts — anything in the past week that warrants follow-up?
- Backup status — did this week's backups run successfully?

Anomaly check (4 minutes)

- Did anyone report anything unusual this week — a strange email, a phishing message, a slow computer, an unexpected pop-up?
- Were there any failed payment transactions, unexpected wire instructions, or vendor change requests this week?
- Did your bank or any vendor send any security notifications you have not yet read?

How to Run the Review

The first time, the review takes 30 to 45 minutes — you are learning where to look and what is normal. By the third or fourth week, it takes 15 minutes. The objective is not exhaustive analysis. It is regular attention. The 15 minutes you spend each week looking at sign-in logs is enough to catch the

unfamiliar foreign sign-in that signals a compromised account, and the difference between catching that on Tuesday and catching it three weeks later is often the difference between a non-event and a wire fraud.

Use Template 8 in Appendix D as your weekly log. Note what you checked, what you saw, and any follow-up needed. Six months from now, the log itself becomes evidence: you have been paying attention, consistently. That evidence matters for cyber insurance claims, customer questionnaires, and your own confidence in your business's security posture.

6.2 The Monthly Access Review

When: First Monday of every month. 30 minutes.

Once a month, take 30 minutes to confirm that the right people have access to the right things. Access drift is one of the most common security failures in small businesses, and a brief monthly review catches it before it becomes severe.

What to Check

Open the Access Review Log (Appendix D, Template 3). For the past month, confirm:

- ☐ Anyone who left the business has had all access revoked: email, file storage, applications, VPN, and any saved credentials in shared password vaults.
- ☐ Anyone whose role changed has had access adjusted: new access granted where needed, old access removed where no longer needed.
- ☐ Any contractors whose engagement ended have had access revoked, including any temporary accounts created for them.
- ☐ Any vendor or third-party access granted in the past month has a defined expiration date and is necessary.
- ☐ All administrative accounts are still required by their current holders.
- ☐ Any shared accounts (which should not exist, but sometimes do) are documented and justified, or are being phased out.

Particular attention to one category: email forwarding to personal email addresses. Employees sometimes forward business email to their personal Gmail or Yahoo addresses to make working from home easier. These forwarding rules survive the employee's departure unless explicitly removed, and they constitute an ongoing data leak.

6.3 The Quarterly Backup Test

When: First week of each quarter. 1 hour.

Once a quarter, actually test that you can restore from backup. Not check that backup files exist. Not confirm that the backup software is running. Test the restoration. Pick a non-trivial set of files — not just one document, but a folder, an entire user's mailbox, or a complete workstation — and restore it to a test location. Confirm the data is intact. Time how long it takes.

Why This Matters

Surveys consistently find that more than half of small businesses with backup systems discover their backups are not actually working only when they need them. The reasons vary: a software update broke the backup agent six months ago and nobody noticed; the backup was only running for some folders, not the ones that turned out to matter; the backup files exist but cannot be opened because the encryption key was on the same computer that the ransomware encrypted. A backup that has not been tested is not a backup. It is a hope.

How to Run the Test

1. Pick what to restore. Rotate quarterly: customer database one quarter, accounting data the next, full mailbox the third, complete workstation the fourth. Cover everything within a year.
2. Restore to a test location, not the original location. The test must not affect production data.
3. Open the restored data. Read a customer record. Open last quarter's tax return. Send yourself an email from the restored mailbox. Confirm it works.
4. Time it. How long did the restoration take from start to functional data? Document this number — it is your real recovery time, which may be very different from what your IT provider has told you.
5. Document the test in Template 4 (Backup Test Log). Date, what was restored, restoration time, anything that did not work, what was fixed.

If the test fails — files are missing, restoration takes 14 hours, the backup itself is corrupted — the test has done its job. You found out today, when there is no urgency, instead of finding out the day a ransomware attack required you to restore everything immediately.

6.4 The Annual Framework Review

When: Same week every year. Block 4 hours.

Once a year, return to this framework. Read it again. Re-do the risk assessment. Update the policies. Confirm that what was true a year ago is still true, and adjust where it is not.

What to Cover

- ☐ Has the business changed? New offices, new employees, new business units, new product lines, new geographic markets — each may carry security implications.
- ☐ Have the systems changed? New cloud services adopted, old systems retired, new vendors integrated.
- ☐ Have the threats changed? Read this year's industry threat reports (Verizon Data Breach Investigations Report, IC3 Annual Report, ISC² Cybersecurity Workforce Study). Note any new attack patterns relevant to your business.
- ☐ Has the regulatory environment changed? New state privacy laws, new sector-specific regulations, new contractual obligations from customers.
- ☐ Has the insurance landscape changed? Policy renewal is the right time to re-evaluate coverage and required controls.
- ☐ Re-do the full risk assessment from Section 3.
- ☐ Update each of the four policies in Section 4 if needed.
- ☐ Adjust the implementation roadmap if any items remain incomplete.

The annual review is also when you should personally re-confirm Phase 1 of the implementation roadmap — not because you do not trust your team, but because Phase 1 is so important that it deserves direct verification by the owner. Has MFA crept off any account? Are former employees actually offboarded? Is the wire transfer verification rule actually being followed?

6.5 Building Habits, Not Projects

There is a particular failure mode common to small business cybersecurity: the security project. The owner attends a webinar, gets concerned, hires a consultant, runs a comprehensive assessment, implements a list of controls, and declares the project complete. A year later, none of the controls are still being maintained, the consultant has moved on, and the assessment report is in a folder no one opens. The business is no more secure than it was before the project, and possibly less, because the project produced false confidence.

This framework is structured to prevent that failure mode. The implementation roadmap in Section 5 is a project; this section is the antidote. Without the rhythm in this section, the controls in Section 4 and Section 5 will degrade over time. The rhythm is more important than the controls.

Calendar Discipline

Put the weekly review on your calendar. Same day, same time, every week. Defend it the way you would 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. Treat it as an obligation.

Put the monthly access review on your calendar — first Monday of every month. Put the quarterly backup test on your calendar — first week of January, April, July, October. Put the annual framework review on your calendar — same week every year, ideally tied to your fiscal year-end or to your insurance renewal date so the timing reinforces the importance.

Five hours a quarter. About 20 hours a year. That is the budget for keeping a small business secure once the framework is implemented. It is not a large investment. It is, however, an investment that has to actually be made — week after week, month after month, year after year.

Involve One Other Person

Habits that depend on one person fail when that person has a difficult month. If only the owner does the weekly review, the practice will fail during the busy season, and may not recover. Involve at least one other person — a designated employee, a co-owner, a trusted contractor — who can do the review when you cannot, and who reads the same logs you read so that two pairs of eyes are watching. The shared practice is much more durable than the individual practice.

This is also a good practice for succession. If the owner steps back from day-to-day operations, sells the business, or simply takes a long vacation, the security practice should continue without interruption. That requires more than one person knowing how it works.

When to Bring in Outside Help

The discipline practice in this section is for ongoing maintenance. There are specific moments when external help is the right investment, even for a small business committed to doing as much as possible internally:

- After a security incident — investigation, recovery, and lessons-learned analysis benefit from outside expertise.
- Before a major business change — acquiring a competitor, expanding into a regulated industry, signing a contract with a major customer who requires a security assessment.
- On a scheduled basis — every 2 to 3 years, an external assessment provides perspective that internal review cannot.
- When a customer or insurer requires it — many B2B contracts now require third-party security attestation.

External help should complement the internal discipline, not replace it. A consultant who comes in once a year and says "things look good" is not a substitute for the weekly review. The weekly review is what keeps things looking good.

6.6 The Bottom Line

This section is about a small commitment, repeated. Fifteen minutes a week, thirty minutes a month, one hour a quarter, four hours a year. Total: about 20 hours over the course of a year, distributed in pieces small enough that no individual session is daunting.

In exchange, the business sustains a level of security that almost no comparable small business sustains. The controls remain in place. The drift is caught. The discipline is the framework's compounding return.

Discipline first. Then even Excel is a good tool. The weekly review, the monthly access review, the quarterly backup test, the annual framework review — these are the discipline. Whatever tools you use to support them — Excel, a notebook, the templates in Appendix D, a more sophisticated platform if you grow into needing one — work because the discipline is there. Without the discipline, no tool helps.

Section 7: Employee and Owner Education

Time required for owner: 45 minutes to read.

More than 80 percent of successful cyberattacks involve a human element — someone clicked a link, used a weak password, was tricked into wiring money, or accidentally sent sensitive data to the wrong person. Technology controls are essential, but they are not sufficient without people who understand what they are looking at.

This section addresses two distinct audiences. The first is your employees, who need practical, repeated education about the threats they face daily — particularly phishing in all its modern forms. The second is you, the owner, who needs a different kind of education: how to make security decisions without becoming a security professional. Both layers are necessary. Most small business cybersecurity guidance covers the first and ignores the second.

7.1 Phishing Recognition

Phishing is the single most common entry point for attacks against small businesses. Train every employee — every one, including part-time staff and contractors with email access — to recognize the warning signs.

Red Flags to Train Every Employee On

- ☐ Sender's email address does not match the claimed organization (e.g., support@amaz0n.net, where the zero replaces the letter o).
- ☐ Urgent or threatening language: "Your account will be closed in 24 hours," "Immediate action required," "Final notice."
- ☐ Requests for login credentials, passwords, or financial information delivered by email.
- ☐ Unexpected attachments, particularly .zip, .exe, .docm, .iso, or .htm files.
- ☐ Links that display one URL but direct to a different one (hover over the link without clicking; the actual destination usually appears at the bottom of the screen).
- ☐ Poor grammar, spelling errors, or unusual formatting (decreasingly reliable as AI-generated phishing improves; absence of errors does not mean an email is legitimate).
- ☐ Unexpected requests that seem out of character for the apparent sender (the CFO never asks for gift cards by email; an unusual request from the CFO is suspicious for that reason alone).

- Requests to bypass normal procedures ("don't tell anyone about this until the deal closes," "I'm in a meeting and can't take a call").
- Offers that seem too good to be true (free gift cards, unexpected refunds, prize notifications).
- Requests to make urgent wire transfers, purchase gift cards, or change vendor bank account information.

The Verification Reflex

The single most important behavioral training you can give employees is the verification reflex: any unusual request involving money, credentials, or sensitive data must be verified through a separate channel before action is taken. "Separate channel" means a phone call to a known number, an in-person conversation, or a message sent via a different system — not a reply to the email itself, which only confirms the request with the same channel that may have been compromised.

This reflex defeats most phishing-initiated attacks against small businesses, including BEC, deepfake-initiated wire fraud, and most variants of impersonation attacks. It costs nothing. It takes less than a minute per occurrence. It must be communicated, modeled, and reinforced until it is automatic.

7.2 Modern Threat Scenarios

The phishing playbook has evolved substantially in the past three years. Train employees to recognize the new variants alongside the classic ones.

AI-Generated Phishing

Phishing emails generated by AI have eliminated the spelling errors, awkward phrasing, and translation artifacts that used to give them away. They can be written in fluent business English, customized to the recipient using publicly available information from LinkedIn or the company website, and produced at scale. The defense is not to look for grammatical mistakes — those are fading — but to look at the request itself: is it consistent with how this sender normally communicates, is it plausible given the context, does it ask the recipient to do something unusual?

A red flag pattern: a perfectly written email asking the recipient to do something they have not done before, on an urgent timeline, with instructions to keep it confidential. The grammar is fine; the social engineering is the giveaway.

Deepfake Voice Calls

Voice cloning technology now requires only a few seconds of source audio to produce a convincing imitation. A podcast appearance, a webinar recording, a video on the company website — any of these provide enough material to clone an executive's voice. Attackers use cloned voices to call

employees with urgent instructions: wire this money, share this credential, take this action immediately.

Defense: a verification rule that applies regardless of how legitimate the voice sounds. "Hi, this is [name], I need you to wire $50,000 to this account today" is the script of a voice impersonation attack against your business. The defense is the same as for written BEC: verify through a separate channel before acting.

Deepfake Video on Conference Calls

This is newer and is documented in cases beginning in 2024. The attacker joins a video call as the impersonated executive, with synthesized video and cloned voice. Image quality is often poor, but in 2026 "poor video quality" is also normal for legitimate calls and does not raise suspicion. The Hong Kong incident at multinational firm Arup in early 2024 cost $25 million via this vector.

Defense: any high-stakes financial decision communicated by video call must be confirmed in writing or by callback to a known number before execution. The video call is no longer a sufficient verification.

QR Code Phishing

Attackers send emails containing a QR code that, when scanned, leads to a credential-stealing site. The technique exploits the fact that QR codes are scanned with personal phones, often bypassing corporate email security and endpoint protection. Common pretexts: "scan to view your secure document," "scan to update your account," "scan to confirm your identity for the conference."

Defense: do not scan QR codes from emails. If an email asks you to scan a QR code to access something, navigate to the source website directly through your browser instead.

Vendor Compromise Cascading

Attackers compromise a vendor or partner you work with, then use the vendor's legitimate email and account to send malicious requests to you. The email is from the real vendor address, the account is the real account, the writing matches the relationship — but the request itself is the attack. Common pattern: "our bank is changing routing — please update the account information for the next invoice."

Defense: any change to vendor banking, payment, or contact information requires verification by phone call to a known number — the verification reflex applied at vendor scale.

7.3 Annual Security Awareness Training Topics

The following topics should be covered with all employees at least once a year, and with new employees during onboarding. Free training materials are available from CISA, the FTC Small Business Cybersecurity Initiative, and many cyber insurance carriers (often included with the policy).

- ☐ How to recognize and report phishing emails (with current real-world examples).
- ☐ Password hygiene: unique passwords, password manager use, why MFA matters.
- ☐ Safe use of company devices: personal use boundaries, BYOD rules, what apps and services are acceptable on a work device.
- ☐ Working from home and remote work security: VPN use, home network security, public Wi-Fi precautions.
- ☐ Social engineering awareness: phone scams, pretexting, vishing, smishing, impersonation by phone or in person.
- ☐ Safe handling of sensitive customer and business data: where it should and should not be stored, how to share it securely.
- ☐ What to do if you suspect a security incident: who to call, what not to do, how to preserve evidence.
- ☐ Physical security: clean desk policy, securing devices when out of the office, tailgating, visitor management.
- ☐ Safe use of public Wi-Fi and cloud storage: when to use VPN, what to avoid.
- ☐ Company-specific policies: review the password, access control, data protection, and incident response policies; confirm understanding.

7.4 Owner Education: Making Security Decisions Without Becoming a Specialist

Most cybersecurity guidance assumes the reader is the IT department or will become it. This framework does not. The owner of a small business has dozens of areas to be moderately competent in — finance, operations, sales, hiring, legal compliance, customer relationships — and security is one more. The goal of owner education is not expertise; it is the ability to make competent decisions on security questions when they arise. This section covers the decisions you will actually face.

Evaluating Vendor Proposals

You will be approached by IT companies, MSPs, cybersecurity firms, software vendors, and insurance providers offering services and products. Many proposals will sound similar. The following questions separate competent providers from sales pitches:

- "What specific risks does this address for our business, and how do you know it is in our top 5 risks?" — Vague answers ("all kinds of attacks," "comprehensive protection") suggest the provider has not assessed your business. Specific answers ("this protects against the BEC attacks that account for the majority of small business losses in your industry") suggest they have.
- "What free or low-cost alternatives exist for what you are proposing, and why is your offering better?" — A competent provider will acknowledge alternatives and articulate the difference. A salesperson will dismiss alternatives. Your most useful tools are often free; if a vendor cannot explain why their paid version is worth more, the answer is usually that it is not.
- "What does success look like in 90 days, and how will we measure it?" — Cybersecurity outcomes are notoriously hard to measure, but a competent provider will define some specific outcomes. A salesperson will speak in vague reassurances.
- "Can I see a sample of the deliverables, with confidential information redacted?" — Reports, assessments, training materials. Quality of work is visible in samples.
- "What certifications and experience do your staff hold, specifically the people who will work on our account?" — Generic firm-level certifications matter less than the experience of the actual people.

Evaluating Cyber Insurance

Cyber insurance is essential for most small businesses. It is also a complex product, and shopping it well saves substantial money and provides better coverage. Read the proposed policy carefully and pay attention to:

- Coverage limits: total policy limit, sub-limits for specific categories (ransomware, business interruption, regulatory penalties, social engineering / wire fraud).
- Sub-limit for social engineering / wire fraud: this is the most commonly used coverage, and it is often capped at $50,000 to $250,000 — well below the total policy limit. If your business handles wire transfers, ensure this sub-limit is adequate.
- Required controls: most policies require specific controls (MFA on email, regular backups, employee training) and exclude losses where these controls were not in place. Use the required controls list as a checklist for your own program.
- Incident response services included: many policies provide free or discounted incident response services through preferred vendors. Some require notification through specific channels for these services to apply.
- Notification timelines: policies typically require notification within 24 to 72 hours of incident discovery. Late notification can void coverage.
- Exclusions: read these carefully. Common exclusions include losses caused by unsupported software, prior incidents, acts of war (sometimes including state-sponsored attacks), and intentional acts by employees.

Get quotes from at least three carriers. Premiums and terms vary widely, and a 30-minute comparison can save thousands of dollars annually.

Responding to B2B Security Questionnaires

If you serve larger customers, you will increasingly be asked to complete security questionnaires before contracts are awarded or renewed. These can be intimidating — they typically run 50 to 200 questions — but the answers are not as complex as the format suggests. The questions fall into a few categories:

- Do you have policies covering the following areas? (Yes — point to your Section 4 policies.)
- Do you have technical controls in place? (Yes for the controls in your implementation roadmap.)
- Do you have insurance coverage? (Yes, with specifics.)
- How do you train employees? (Reference your awareness program.)
- How would you respond to an incident? (Reference your incident response plan.)

If a questionnaire asks about a control you do not have, two responses are appropriate: implement the control if it is reasonable for your business and the customer is important enough to justify it, or honestly note that the control is not in place but explain compensating measures. Honesty is better than fabrication; security questionnaire answers are sometimes audited.

Reading Your Bank's Fraud Notifications

Banks send notifications about suspicious transactions, unusual login activity, and account changes. Many small business owners ignore these as routine. Read them. The bank's fraud team often catches attacks before the business does, and a 30-second response to a notification can prevent a significant loss.

Establish a habit: bank notifications are read on the day they arrive, by you personally if at all possible, and any unusual activity is investigated within hours.

Negotiating with Your IT Provider

If your IT provider is not delivering meaningful cybersecurity services and is presenting themselves as if they are, you have three options:

1. Have an honest conversation: "I want to understand specifically what cybersecurity services we are receiving from you, and what additional services would be available at what cost." A good provider welcomes this conversation; a bad provider becomes defensive.
2. Bring in a separate cybersecurity provider while keeping the IT provider for IT support. The IT and cybersecurity functions are different, and there is no requirement that one company do both.

3. Find a different provider that genuinely does both. Some MSPs do, although they cost more. Use the questions in 7.4 above to evaluate.

When to Pay for Help and When Not To

This framework is designed to be implementable largely without paid external help. There are specific moments when paying for help is the right decision:

- After a significant incident — investigation and recovery should not be the first time you do this kind of work.
- When customer requirements demand specific external attestation (SOC 2, ISO 27001, HIPAA compliance audit).
- When the business reaches a size or complexity where the owner cannot meaningfully oversee security as a part-time activity.
- When a major business change introduces new risk (acquiring a competitor, entering a regulated industry, scaling to multi-state operations).

Outside those moments, the question is not whether you can afford to pay for help; it is whether the help would deliver more value than the equivalent investment in implementing this framework yourself. Most of the time, for a small business, it would not. The framework is the help.

7.5 Quick Reference: Always-Do and Never-Do Lists

Always Do

- ☐ Use strong, unique passwords and a password manager.
- ☐ Enable multi-factor authentication on every account that supports it.
- ☐ Lock your screen when stepping away from your computer.
- ☐ Report suspicious emails to your IT contact before clicking anything.
- ☐ Keep your software and operating system updated.
- ☐ Use the company VPN when working remotely.
- ☐ Verify unusual financial requests through a separate communication channel before acting.
- ☐ Read your bank's fraud notifications the day they arrive.

Never Do

- ☐ Click links or open attachments in unexpected emails without verification.
- ☐ Share your password with anyone, including IT staff (legitimate IT does not need it).
- ☐ Use the same password for multiple accounts.
- ☐ Send sensitive data via unencrypted email or personal messaging apps.

- ☐ Connect to public Wi-Fi without a VPN.
- ☐ Store sensitive business data on personal devices or personal cloud accounts.
- ☐ Disable antivirus or security software, even temporarily.
- ☐ Ignore software update notifications for extended periods.
- ☐ Approve an MFA prompt on your phone that you did not initiate.
- ☐ Take action on an urgent financial request without verifying through a separate channel.

Appendix A: Free-Tier Tools Matrix

This appendix lists tools and services that small businesses can use to implement the controls described in this framework. Every category begins with a free or built-in option that is sufficient for most small businesses. Paid options are listed where they offer real additional value, with explicit guidance on when upgrading is warranted.

Two principles guide this matrix:

- Free is the starting point. Many cybersecurity tools have free tiers that are genuinely usable for small business needs. Bitwarden Free, Microsoft Defender, ProtonVPN, and the security features built into Microsoft 365 and Google Workspace are not crippled marketing versions — they are real tools that real businesses run on.
- Upgrade when you have a reason. Paid tools cost real money and require ongoing attention. Buy them when you have specific needs the free version cannot meet, not because of generic concerns about "protection."

Pricing is approximate as of 2026. Verify current prices before purchase.

A.1 Password Manager

Option	Price	Best for
Bitwarden Free	$0	Most small businesses; unlimited devices, unlimited passwords, sync across devices
Bitwarden Teams	$4/user/month	Businesses needing centralized administration, secure sharing among employees, and admin policies
1Password Business	$8/user/month	Businesses preferring a more polished interface and willing to pay for it
Dashlane Business	$8/user/month	Similar to 1Password; choose based on user interface preference
LastPass Business	$7/user/month	Established option, but consider the company's prior breach incidents when evaluating

> **Recommendation**
>
> Start with Bitwarden Free. Upgrade to Bitwarden Teams when you need centralized administration or to share passwords securely among employees (typically when you grow past 5-7 employees).

A.2 Multi-Factor Authentication

Option	Price	Best for
Microsoft Authenticator	$0	Businesses using Microsoft 365; native integration
Google Authenticator	$0	Businesses using Google Workspace; broad compatibility
Authy	$0	Cross-device synchronization with cloud backup
Duo Free	$0 (up to 10 users)	Businesses wanting more centralized administration than free apps provide
Duo Essentials	$3/user/month	Beyond 10 users, or for businesses needing conditional access policies
YubiKey 5 NFC	$55 one-time per key	Phishing-resistant hardware MFA for high-value accounts (recommended for owner and finance roles regardless of business size)

> **Recommendation**
>
> Use the free authenticator app that matches your email provider. Add YubiKeys for the owner, the bookkeeper, and anyone with access to financial systems — these are the highest-value targets and warrant the strongest protection.

A.3 Endpoint Protection / Antivirus

Option	Price	Best for
Microsoft Defender	$0	Most Windows-based small businesses;

Option	Price	Best for
(built into Windows 10/11)		consistently rates near the top in independent testing
macOS built-in protections (XProtect, Gatekeeper)	$0	Mac-based small businesses; supplement with caution and update discipline
Microsoft Defender for Business (in Microsoft 365 Business Premium)	Included in M365 Business Premium ($22/user/month)	Businesses already paying for M365 Business Premium; provides EDR capabilities
Bitdefender GravityZone Business	$25-40/user/year	Businesses wanting third-party EDR independent of Microsoft
SentinelOne Singularity Control	$45-65/user/year	Businesses with specific compliance or threat-hunting needs
CrowdStrike Falcon Go	$60-90/user/year	Businesses wanting enterprise-grade EDR; usually overkill for SMBs under 50 employees

> **Recommendation**
>
> Microsoft Defender (built into Windows) is genuinely sufficient for the majority of small businesses. The marketing for paid alternatives often overstates the gap; in independent testing, Defender consistently performs at or near the top. Upgrade only with a specific reason.

A.4 VPN for Remote Access

Option	Price	Best for
ProtonVPN Free	$0	Light remote work needs; one device, limited countries
ProtonVPN Plus	$4.99/user/month annual	Most small businesses with remote workers; reliable, privacy-focused
NordLayer	$7-14/user/month	Businesses wanting business-focused VPN with team management

Option	Price	Best for
Built-in Microsoft 365 / Azure VPN	Included in M365	Businesses heavily invested in Microsoft ecosystem
Tailscale (mesh VPN)	Free for personal; $5/user/month for teams	Technical-savvy small businesses; modern alternative to traditional VPN
Cisco AnyConnect	$50-150/user/year	Larger SMBs or businesses with existing Cisco infrastructure

A.5 Email Security

Most small businesses get adequate email security from features built into their email provider. Pay close attention to enabling these — they are commonly disabled by default.

Option	Price	Best for
Microsoft 365 Defender for Office 365 Plan 1	Included in Business Premium	Businesses on M365 Business Premium; adds anti-phishing, ATP attachment scanning, safe links
Google Workspace Standard email security	Included in Workspace Standard	Businesses on Google Workspace; built-in spam, phishing, malware protection
Mimecast Email Security	$3-6/user/month	Businesses needing dedicated email security gateway with archive and continuity
Proofpoint Essentials	$3-5/user/month	Similar to Mimecast; choose based on feature comparison
Avanan / Check Point Harmony Email	$3-5/user/month	Businesses wanting AI-driven phishing detection layered on M365 or Workspace

> **DMARC, SPF, DKIM**
>
> These are three email security settings that prevent attackers from impersonating your business in emails sent to your customers. They are free, take 30-60 minutes of technical setup, and are surprisingly effective at preventing your domain from being spoofed. If your email provider is Microsoft 365 or Google Workspace, they have step-by-step guides for setting them

> up. This is one of the highest-value low-effort items in the entire framework.

A.6 Backup

Option	Price	Best for
External hard drive + manual or scheduled backup	$60-150 one-time	Smallest businesses; works only if discipline is maintained
OneDrive (Microsoft 365)	1TB included with M365 Business Standard ($12.50/user/month)	Businesses on M365; provides versioning and ransomware recovery
Google Drive (Workspace)	Storage included with Workspace plans	Businesses on Google Workspace
Backblaze Personal/Business	$9/month/computer	Continuous cloud backup of computers; simple, reliable
IDrive Business	$79/year for 5TB	Multi-device backup with central administration
Synology NAS (DiskStation)	$400-800 one-time + drives	Local backup with capacity for years of data; pairs well with cloud backup for 3-2-1
Veeam Backup for Microsoft 365	$15-25/user/year	Specifically backs up M365 mailboxes, OneDrive, SharePoint, Teams (M365's own retention is not a true backup)
Datto / Acronis Cyber Backup	$50-200/month for SMB	Businesses needing professional-grade backup with rapid recovery and business continuity features

> **Critical: M365 and Google Workspace are not backups**
>
> Microsoft 365 and Google Workspace retain data for limited periods (typically 30-90 days for deleted items) but they are not designed as backup services. If a user account is compromised and data is destroyed, or if data is accidentally deleted and not noticed for months, the cloud providers' built-in retention may not recover it. For any business serious about data protection, a separate backup tool that creates immutable, independent copies of M365/Workspace data

> is essential. Veeam Backup for Microsoft 365 is the most common choice.

A.7 Document and File Encryption

Option	Price	Best for
BitLocker (Windows Pro and above)	$0 (built-in)	Windows laptop and desktop encryption; default for any business with portable devices
FileVault (macOS)	$0 (built-in)	Mac laptop encryption; same role as BitLocker
7-Zip with AES-256 password	$0	Encrypting individual files or folders for transport
VeraCrypt	$0	Open-source full-disk and container encryption; for technical users
Boxcryptor (now Dropbox)	$10-15/user/month	Encrypted cloud storage layered on Dropbox/Google Drive/OneDrive
Microsoft Purview Information Protection	Included in M365 E3+	Businesses needing data classification, rights management, and data loss prevention at scale

A.8 Cloud Storage with Security

Option	Price	Best for
OneDrive for Business	Included in M365 Business plans (1TB+/user)	M365-based businesses; tight integration, good security defaults
Google Drive (Workspace)	Included in Workspace plans	Workspace-based businesses
Dropbox Business Standard	$15/user/month	Businesses needing simple, reliable file sync; less integrated than M365/Workspace

Option	Price	Best for
Tresorit Business	$14-20/user/month	End-to-end encrypted cloud storage; for businesses with confidentiality requirements (legal, healthcare)
Sync.com	$8/user/month	Lower-cost zero-knowledge encrypted alternative to Tresorit

A.9 DNS Protection

DNS-level filtering blocks employees from accessing known malicious websites — including phishing pages, malware download sites, and ransomware command servers — before any browser or endpoint protection has a chance to. It is one of the highest-value low-effort controls available.

Option	Price	Best for
Quad9 (DNS provider)	$0	Public DNS service that blocks known malicious domains; configure on router
Cloudflare for Families (DNS)	$0	Similar; family-friendly variants available
OpenDNS Home (Cisco)	$0	Configurable filtering with web dashboard
Cisco Umbrella	$2-3/user/month	Business-grade DNS protection with reporting and policy management
DNSFilter	$1-3/user/month	SMB-focused DNS protection with simple administration

> **Recommendation**
>
> Configure Quad9 (9.9.9.9) as your business router's DNS. Free, takes 5 minutes, blocks a large category of malicious traffic before any other security control needs to engage. For businesses wanting more granular control, Cisco Umbrella or DNSFilter provide reporting and policy management at modest cost.

A.10 Network Monitoring and Firewall

Option	Price	Best for
Built-in Windows Defender Firewall	$0	Default workstation firewall; sufficient for most small businesses
pfSense / OPNsense	$0 (open source)	Technical small businesses wanting full firewall control on commodity hardware
Ubiquiti UniFi Dream Machine	$300-500 one-time	Small businesses wanting unified routing, switching, and Wi-Fi management
Fortinet FortiGate (entry SMB models)	$500-1,500 + license	Businesses wanting business-class firewall with reporting
Cisco Meraki MX series	$500-1,500 + license	Businesses wanting cloud-managed firewall; subscription-based

A.11 Phishing Simulation and Security Training

Option	Price	Best for
KnowBe4 Free Phishing Test	$0 (one-time test)	Initial awareness check
FTC Small Business Cybersecurity Initiative training (free)	$0	General awareness training for small businesses
CISA Cyber Essentials Toolkit	$0	Free framework with training resources
KnowBe4 Security Awareness Training	$15-30/user/year	Most popular SMB platform; includes phishing simulations
Hoxhunt	$3-6/user/month	Behavioral training with phishing simulations
Mimecast Awareness Training	Included with Mimecast Email Security	Bundled awareness if already on Mimecast

A.12 Mobile Device Management

Option	Price	Best for
Microsoft Intune (Basic)	Included in M365 Business Premium	M365-based businesses needing mobile device policy enforcement
Google Workspace Endpoint Management	Included in Workspace Standard+	Workspace-based businesses
Jamf Now	$4/device/month	Mac-focused small businesses
JumpCloud	$11-15/user/month	Cross-platform device management for SMBs

A.13 Putting It All Together

For a typical 10-person small business, here is a complete, all-free or low-cost stack that covers the core controls in this framework:

- Email and productivity: Microsoft 365 Business Standard ($12.50/user/month) — includes email, OneDrive, Teams, baseline security
- Password manager: Bitwarden Free or Bitwarden Teams ($4/user/month) — for shared passwords
- MFA: Microsoft Authenticator (free) plus 2 YubiKeys for owner and bookkeeper ($110 one-time)
- Endpoint protection: Microsoft Defender (built into Windows, free)
- Backup: Veeam Backup for Microsoft 365 ($15-25/user/year) plus external hard drive for local backup ($100 one-time)
- VPN: ProtonVPN Plus ($4.99/user/month for those who work remotely)
- DNS protection: Quad9 (free)
- Cyber insurance: $1M policy ($1,500-3,000/year)
- Phishing simulation: KnowBe4 free test or annual paid plan ($150-300/user/year if going with paid training)

Approximate total monthly cost for 10 employees: $200-400. Approximate annual cost including insurance and one-time hardware: $5,000-8,000. This produces a security posture meaningfully stronger than most comparable small businesses, with no enterprise-tier purchases.

Appendix B: Glossary

This glossary translates the technical terms used throughout this framework into plain business language. Every term that appears anywhere in the framework has an entry here. Where useful, business analogies are provided to make concepts concrete.

Terms are listed alphabetically. Cross-references to relevant sections of the framework are noted where applicable.

A

Access control

The set of rules and tools that determine who can use which systems and data. Like the keys in a building — different keys open different doors, and you take keys back when someone leaves. See Section 4.3.

Account takeover (ATO)

An attack in which a legitimate user's account is taken over by an attacker, who then uses the account as if they were the user. The attacker may steal data, send malicious emails to others, or move money. From the system's perspective, the activity looks legitimate because the attacker is using real credentials.

Administrative account / admin account

An account with elevated privileges — the ability to change system settings, create or delete other accounts, install software, or access most data. The most valuable target for attackers. Should be separated from regular daily-use accounts.

Antivirus / endpoint protection

Software installed on each computer that watches for known malicious files and behaviors and blocks them. The basic layer of defense for individual computers.

Application Programming Interface (API)

A way for one piece of software to talk to another. Relevant to security because attackers often exploit poorly secured APIs to extract data or take actions without going through user interfaces.

Asset inventory

A list of everything in your business that has digital value — computers, phones, software, cloud accounts, data. Foundation of risk assessment. See Section 3.3.

Attestation

A formal statement, often from a third party, that confirms certain controls are in place. SOC 2 reports are attestations. B2B customers increasingly require attestation before signing contracts.

B

Backup

A copy of data stored separately from the original, so the data can be restored if the original is damaged or lost. Three rules: three copies, two different media types, one offsite. See Section 4.4.

BEC (Business Email Compromise)

An attack that uses email impersonation or compromise to trick a business into making payments to an attacker. The most expensive cybercrime category by total losses. See Section 2.2.

BitLocker

Microsoft Windows' built-in disk encryption. Available in Windows Pro and above. Encrypts the entire hard drive so data is unreadable if the laptop is stolen. Free.

Botnet

A network of compromised computers controlled by an attacker. Used to send spam, launch DDoS attacks, or relay malicious traffic. Many small business computers are botnet members without anyone noticing.

BYOD (Bring Your Own Device)

A policy where employees use their personal phones, tablets, or laptops for work. Convenient but creates security challenges, since the business has limited control over personal devices.

C

CIS Controls

A widely-used set of cybersecurity best practices published by the Center for Internet Security. Version 8 contains 18 controls organized by implementation priority. This framework references CIS Controls but is not derived from them.

CISA

The Cybersecurity and Infrastructure Security Agency, part of the U.S. Department of Homeland Security. Publishes free cybersecurity guidance, alerts, and resources particularly relevant to small businesses.

CISM, CISSP

Cybersecurity certifications — Certified Information Security Manager and Certified Information Systems Security Professional respectively. Held by experienced security professionals. Useful credentials to ask about when evaluating an IT or security provider.

Cloud service / SaaS (Software as a Service)

Software that runs on a provider's servers rather than on your computers, accessed through a web browser. Microsoft 365, Google Workspace, QuickBooks Online, Salesforce — all SaaS. Convenient but relocates security responsibility to the vendor.

Compromise

A general term for an attacker successfully gaining unauthorized access to a system, account, or network. "Email account compromise" means an attacker has gained control of an email account.

Credential stuffing

An automated attack that takes username/password combinations stolen from one website and tries them on many other websites, exploiting the fact that many people reuse passwords. Defeats easily by MFA and password manager use.

Cyber insurance

Insurance coverage for losses arising from cybersecurity incidents — wire fraud, ransomware, data breach response costs, business interruption. Essential for most small businesses. See Section 4.5.

D

Data breach

An incident in which sensitive data is accessed, copied, or disclosed without authorization. Often triggers legal notification obligations under state and federal law.

Deepfake

Synthetic audio, video, or images generated by AI that imitate real people convincingly. Used in modern social engineering attacks to impersonate executives or known parties. See Section 2.7.

DDoS (Distributed Denial of Service)

An attack that floods a website or network with so much traffic that legitimate users cannot reach it. More commonly aimed at large businesses but occasionally used as extortion against SMBs.

DKIM (DomainKeys Identified Mail)

An email security setting that lets receivers verify that an email actually came from your business's domain. Prevents attackers from impersonating your domain to your customers. Free, and one of the highest-value email security controls. See Appendix A.5.

DMARC (Domain-based Message Authentication, Reporting & Conformance)

An email security setting that tells receivers what to do with emails that fail SPF or DKIM checks (block, quarantine, or allow). Works with SPF and DKIM to prevent domain spoofing. See Appendix A.5.

DNS (Domain Name System)

The system that translates domain names (example.com) into the numeric addresses computers use. DNS-level filtering blocks employees from accessing known malicious domains. See Appendix A.9.

E

EDR (Endpoint Detection and Response)

Software that watches every computer in your business for suspicious activity, like a security camera with an alarm. More sophisticated than basic antivirus — it can detect attacks that have not been seen before by looking at behavior, not just by matching against known malware. See Appendix A.3.

Encryption

Mathematical scrambling of data so it can only be read by someone with the right key. "Encryption at rest" means data is encrypted when stored on a disk. "Encryption in transit" means data is encrypted while being sent over a network. Both are standard requirements for sensitive data.

Executive Order 14028

An executive order issued in May 2021 that establishes federal cybersecurity priorities, including the protection of the broader supply chain that includes small businesses. Frequently cited in U.S. cybersecurity policy.

F

FileVault

Apple macOS's built-in disk encryption. Free, built-in, and the macOS equivalent of BitLocker.

Firewall

A device or software that controls what network traffic can pass into or out of a network. Most small businesses have one in their internet router, plus a software firewall on each computer. The basic layer of network defense.

G

GRC (Governance, Risk, and Compliance)

An umbrella term for the policies, processes, and tools that ensure an organization meets its obligations and manages its risks. Enterprise GRC platforms cost tens of thousands per year. Small businesses do GRC manually using spreadsheets and discipline.

H

HIPAA (Health Insurance Portability and Accountability Act)

U.S. federal law that requires healthcare providers and their business associates to protect patient health information. Carries significant penalties for breaches. Healthcare-related small businesses must understand their HIPAA obligations.

I

IC3 (Internet Crime Complaint Center)

FBI center that collects complaints about internet-based crimes, including cybercrime against businesses. Their annual report is a primary source of statistics on cybercrime trends.

Incident

Any event that disrupts security, regardless of cause or severity. "Security incident" can range from a single suspicious email reported by an employee to a full ransomware infection.

Incident response (IR)

The structured process of detecting, containing, investigating, and recovering from security incidents. See Section 4.5.

Insider threat

Risk from people who have legitimate access to your systems — employees, contractors, vendors. Includes both malicious actions and accidents. See Section 2.6.

ISO/IEC 27001

International standard for information security management systems. Comprehensive but typically too elaborate for small businesses to implement directly. This framework references ISO/IEC 27001 but is not derived from it.

L

Least privilege

The principle of giving each user only the access they need to do their job — no more. The opposite of giving everyone access to everything just in case. Foundation of access control. See Section 4.3.

M

MFA (Multi-Factor Authentication)

Requiring a second proof of identity beyond a password — like using a debit card and a PIN, not just one of them. The most important single security control for small businesses. Defeats the overwhelming majority of automated account compromise attempts. See Section 4.2.

Malware

Any software designed to do harm — viruses, ransomware, spyware, trojans, worms, etc. The umbrella term.

MSP (Managed Service Provider)

An IT company that handles a small business's technology on an outsourced basis — email, computer support, network management. May or may not provide actual cybersecurity services. See Section 4.1.

N

NIST CSF 2.0 (NIST Cybersecurity Framework, version 2.0)

A widely-used cybersecurity framework published by the U.S. National Institute of Standards and Technology. Comprehensive but typically too elaborate for small businesses to implement directly. This framework references NIST CSF but is not derived from it.

O

OAuth

A protocol that lets one application get permission to access another on a user's behalf — "Sign in with Google" type buttons. Convenient and generally secure, but attackers exploit it to gain persistent access; check OAuth permissions in your weekly review (Section 6.1).

P

Password manager

Software that generates, stores, and fills in unique strong passwords for each account, so users can have hundreds of unique passwords without remembering any of them. Foundational tool for small business security. See Appendix A.1.

Patch / patching

Updates released by software vendors to fix bugs and security vulnerabilities. Applying patches promptly is one of the highest-impact security controls. "Unpatched" software is software that has not received available updates.

PCI DSS (Payment Card Industry Data Security Standard)

Industry standard that businesses accepting credit card payments must comply with. Maintained by the major card networks. Failure to comply can result in fines and loss of payment processing privileges.

Phishing

An email designed to trick the recipient into doing something harmful — clicking a malicious link, downloading malware, entering credentials on a fake page, or following a fraudulent instruction. The single most common attack vector. See Section 2.1.

Privileged Access Management (PAM)

The practice of strictly controlling and monitoring administrative accounts. For small businesses, this means separating admin accounts from regular accounts and using admin privileges only when needed.

PII (Personally Identifiable Information)

Information that can identify an individual — name, social security number, address, email, phone, financial information. Subject to varying state privacy laws.

R

Ransomware

Malicious software that encrypts a victim's files and demands payment for the decryption key. Modern ransomware also typically steals data before encrypting and threatens to publish it if the ransom is not paid ("double extortion"). See Section 2.3.

Restoration / restore

The process of recovering data from a backup. "A backup that has not been tested for restoration is not a backup." See Section 6.3.

Risk assessment

The structured process of identifying what your business has, what could threaten it, where you are vulnerable, and where to focus protection. See Section 3.

S

SaaS

See Cloud service.

Security questionnaire (B2B)

A questionnaire from a customer or potential customer asking about your security practices. Increasingly required before contracts are signed or renewed. See Section 7.4.

SIEM (Security Information and Event Management)

Enterprise software that collects and analyzes log data from across an organization's systems. Typically too complex and expensive for small businesses; cloud-based alternatives are emerging.

SOC 2

An auditing standard for service organizations, particularly relevant to SaaS providers. SOC 2 reports describe a vendor's security controls. Increasingly required by enterprise customers. Not typically achieved by small businesses, but small businesses are increasingly asked about it by their customers.

Social engineering

Manipulation of people to take actions or reveal information. Phishing is one form; phone-based vishing, text-based smishing, in-person pretexting are others. The human counterpart to technical attacks.

SPF (Sender Policy Framework)

An email security setting that lists which servers are authorized to send email for your domain. Receivers can check incoming email against this list to detect spoofing. Free; works with DKIM and DMARC. See Appendix A.5.

Spear phishing

Phishing targeted at a specific person, typically using research to make the email convincing. More dangerous than generic phishing because it is customized.

Supply chain attack

An attack that reaches a target through one of the target's vendors, suppliers, or service providers. Common pattern in modern cybercrime. See Section 2.5.

T

TLS (Transport Layer Security)

The encryption that secures most internet traffic, including HTTPS web traffic and most modern email. The current standard replacing the older SSL.

Two-factor authentication (2FA)

An older term for what is now usually called MFA. Same concept: a second proof of identity beyond a password.

V

VPN (Virtual Private Network)

A technology that creates a secure encrypted connection across an unsecured network — typically used for remote employees connecting to the office network or to bypass insecure public Wi-Fi. See Appendix A.4.

Vulnerability

A weakness in a system, application, or process that could be exploited by an attacker. "Vulnerability assessment" is the structured process of finding them.

W

Whaling

Phishing targeted specifically at executives — "big fish." A subset of spear phishing.

Wire fraud

Fraud involving the transfer of money by wire. The endpoint of most BEC schemes. Once money is wired and clears, recovery is difficult; small windows of action immediately after the fraud are critical.

Y

YubiKey

A small hardware device that provides phishing-resistant multi-factor authentication. About the size of a USB drive. Particularly recommended for owner accounts and accounts with access to financial systems. About $55 per device, one-time. See Appendix A.2.

Z

Zero-day

A previously unknown vulnerability that has no patch available. Used in targeted attacks against high-value targets. Rare in small business attacks; not a primary concern for SMB cybersecurity.

Zero trust

A security model that assumes no user or device is trusted by default, even inside the network. Every access is verified. Enterprise concept; small businesses can adopt elements (especially MFA everywhere) without adopting the full architecture.

Appendix C: Industry Incident Cases

This appendix presents 30 industry-specific incident cases, organized by sector. Each case describes a realistic cybersecurity incident that has happened to a small business in that industry. The cases are composite scenarios drawn from documented patterns; specific business names and details have been changed, but the attack mechanisms, business consequences, and preventive measures are accurate.

The purpose of these cases is twofold: to make abstract risks concrete by showing what they look like in your industry, and to translate the controls in this framework into specific business outcomes. Read the cases relevant to your business. They are likely to surface threat patterns and vulnerabilities you may not have considered.

Each case follows the same structure: industry and business size, what happened, how it happened, what it cost, and what would have prevented it (with cross-references to relevant framework sections).

Service Businesses

C.1 Construction / General Contractor (12 employees)

What happened: A small construction company received an email from a roofing subcontractor they had worked with for three years, requesting that the next invoice payment be sent to a new bank account. The bookkeeper updated the wire instructions and processed the next $87,000 payment.

How it happened: The subcontractor's email account had been compromised through a phishing attack on the subcontractor (who did not realize they had been breached). Attackers spent two weeks reading the email exchange between the contractor and subcontractor, learning the relationship, the invoice schedule, and the language used. They sent the bank-change request from the real subcontractor's real account, in language consistent with the relationship.

What it cost: $87,000 wired to attackers, recovered $4,200 through bank fraud cooperation. Cyber insurance covered $50,000 of the loss (sub-limit on social engineering coverage). Total uninsured loss: approximately $32,800. Six weeks of disruption to normal payment cycles while procedures were rewritten.

What would have prevented it: The verification reflex (Section 7.1): a phone call to the subcontractor's known number to confirm the bank change request. Verification rule for vendor banking changes (Section 4.5). Total cost of these controls: zero. Time required: two minutes.

C.2 Automotive Dealership (35 employees)

What happened: An auto dealership's customer database — 14,000 records including names, addresses, social security numbers, financing details — was published on a hacker forum. The first the dealership knew of the breach was a notification from a customer who had received a notification from their identity protection service.

How it happened: An employee fell for a phishing email impersonating the dealership's loan management software vendor. The phishing page captured the employee's credentials, which used the same password as her email. From the email, attackers found the credentials for the customer database in a forwarded message and exfiltrated the data over six weeks.

What it cost: $340,000 in regulatory penalties (violation of state breach notification timing requirements), $180,000 in customer notification costs, $250,000 in legal fees, ongoing identity theft monitoring obligation for affected customers ($2 per customer per month for two years). Reputational damage caused 15% drop in sales for the year following the breach.

What would have prevented it: MFA on email and on the loan management system (Section 4.2). Password manager preventing reuse (Section 4.2). Weekly review catching the unusual data exfiltration in email logs (Section 6.1). Combined cost: under $200/month.

C.3 Automotive Repair Shop (8 employees)

What happened: Ransomware encrypted the shop's diagnostic computers, customer records, and parts ordering system on a Tuesday morning. Operations halted; customers whose vehicles were in the shop could not be billed or contacted.

How it happened: The shop's customer-facing computer (used to print invoices and look up vehicle history) was running an outdated version of Windows that no longer received security updates. Attackers exploited a known vulnerability via a malicious website visited from that computer. Once inside, the attackers spread laterally through the small network because every computer used the same administrative password.

What it cost: 11 days of closure, approximately $42,000 in lost revenue. Recovery cost: $18,000 (paid an IT consultant to rebuild systems from limited backups). $15,000 ransom not paid; data was lost and customers had to be re-contacted manually. Three customers moved to competitors during the closure.

What would have prevented it: Replacing the unsupported Windows computer (~$600). Unique administrative passwords per system (Section 4.2). Working backups tested quarterly (Section 6.3). DNS-level filtering blocking malicious websites (Appendix A.9). Total cost: under $700 plus ongoing free controls.

C.4 Small Medical Practice (6 employees)

What happened: A medical practice received a HIPAA breach notification letter from their state Attorney General after a former employee was found selling patient records on a healthcare data marketplace.

How it happened: The employee was terminated for performance reasons. Her access to the electronic health records system was revoked the day she left, but her access to the practice's cloud-based file storage (where backup copies of patient files were kept) was not. Over the following month, she downloaded several thousand records.

What it cost: $110,000 HIPAA settlement with HHS Office for Civil Rights, $45,000 in legal fees, mandatory three-year corrective action plan, breach notification to 4,800 patients. The practice's medical malpractice insurance premiums increased 35% the following year.

What would have prevented it: Comprehensive offboarding checklist that revokes access to ALL systems (Section 4.3). Monthly access review catching the gap (Section 6.2). Total cost: zero. Time required: one hour for initial setup of offboarding checklist, 30 minutes per month for access review.

C.5 Dental Practice (14 employees)

What happened: Ransomware encrypted the practice's patient management system, X-ray images, and billing records. The practice was unable to schedule appointments or process insurance for 11 days.

How it happened: An office staff member clicked a link in what appeared to be a Microsoft 365 password reset email. The malicious link installed malware that quietly mapped the practice's network for three weeks before launching the encryption. Backups existed but were stored on a network-attached storage device that was also encrypted by the attack.

What it cost: 11-day closure caused approximately $180,000 in lost revenue. Recovery costs: $65,000 (incident response, system rebuild, regulatory consultation). $80,000 ransom paid (under cyber insurance authorization), partial decryption successful. HIPAA breach notification required (4,200 patients). Within 8 months, the senior dentist sold the practice; the operational disruption and post-incident anxiety were factors in the sale decision.

What would have prevented it: MFA on email (Section 4.2) — would have defeated the credential phishing. Backups stored offsite and offline (Section 4.4) — would have allowed recovery without paying ransom. EDR with behavior-based detection (Section 5 Phase 3) — might have caught the network mapping phase. Combined cost: under $300/month for a 14-person practice.

C.6 Mental Health Practice (4 employees)

What happened: A small therapy practice's appointment scheduling system was compromised, and the attackers used it to send fraudulent payment requests to patients.

How it happened: The practice used a small online scheduling vendor whose security controls turned out to be inadequate. Attackers compromised the vendor's system and gained access to the practice's customer information. They then sent emails to patients (using the vendor's email infrastructure, which made them appear legitimate) requesting that copay payments be sent via a payment service.

What it cost: Eight patients sent payments totaling $6,200 to the attackers. The practice covered the losses to maintain patient trust ($6,200 direct cost). State Attorney General investigation, which

concluded with a notification requirement but no fines (the practice's response was deemed appropriate). Significant time investment in patient communication and reassurance.

What would have prevented it: Vendor security review before adoption (Section 5 Phase 2). Quarterly vendor access review (Section 6.2). Patient communication policy specifying that payment requests are never sent by email (Section 4.4). Annual vendor risk reassessment (Section 5 Phase 3).

C.7 Legal Services / Small Law Firm (9 employees)

What happened: A 9-person law firm specializing in real estate transactions lost $124,000 to a wire fraud over a single Friday afternoon, when a buyer's down payment was redirected to attackers.

How it happened: The firm's email had been compromised through credential reuse two months earlier. Attackers monitored email for an active real estate closing, then sent the buyer wire transfer instructions for the down payment. The instructions came from the firm's real email account, with the firm's real signature block, in language consistent with previous communications. The buyer wired the money. The fraud was discovered when the buyer asked for confirmation of receipt.

What it cost: $124,000 wire (recovered $0 — the funds had moved through three banks within two hours). Cyber insurance covered $100,000 of social engineering loss. Bar association investigation, professional liability claim, eventual settlement with buyer for $20,000 (representing the buyer's loss above insurance). Ongoing reputation damage in the local real estate community.

What would have prevented it: MFA on email (Section 4.2). Password manager preventing reuse (Section 4.2). Verification reflex for wire instructions to clients (Section 7.1). Total cost: under $50/month.

C.8 Accounting / Tax Preparation Firm (11 employees)

What happened: During the busy February-April tax season, the firm's primary tax software was inaccessible for three days due to a ransomware attack. About 60 client returns scheduled for filing during that window were delayed.

How it happened: An employee opened a file attached to an email that appeared to be from a client requesting tax document review. The attachment installed malware that propagated through the firm's network and triggered ransomware on Friday evening (timing chosen to maximize damage before discovery on Monday).

What it cost: Three days of operational closure ($85,000 in lost productivity during peak season). $40,000 ransom paid for partial decryption (cyber insurance authorized). Client trust damage: 15 of the affected 60 clients moved their work to other firms within 12 months. Reputation damage in the broader community required two years to recover. Total cost including lost clients: estimated $400,000+ over three years.

What would have prevented it: Email security with attachment sandboxing (Section 5 Phase 2). Employee training to verify unexpected attachments by phone (Section 7.1). Network segmentation to prevent lateral spread (Section 5 Phase 2). EDR (Section 5 Phase 3). Combined cost: under $200/month.

C.9 Real Estate Brokerage (7 agents + admin)

What happened: Over a four-month period, three different commission payments to agents were redirected to attacker-controlled accounts, totaling $43,000.

How it happened: The brokerage admin's email account had been compromised through password reuse from a fitness app breach. Attackers established an automated email forwarding rule that sent her email to an external address. They monitored for commission payment notifications, then intercepted those payments by sending the closing attorneys revised wire instructions before the legitimate ones arrived.

What it cost: $43,000 across three incidents (recovered approximately $8,000 through bank cooperation on the third incident). Cyber insurance covered $35,000. Three separate state regulatory investigations (the brokerage operated in three states), resulting in modest fines. Loss of two agents who blamed the brokerage for the failed commission protections.

What would have prevented it: MFA on email (Section 4.2). Weekly review checking forwarding rules — would have caught the rule within a week of the first incident, preventing the second and third (Section 6.1). Password manager preventing reuse (Section 4.2).

C.10 Professional Services Firm (22 employees)

What happened: The firm's complete client database, including project histories and confidential financial information, was found being offered for sale on a hacker forum.

How it happened: An office manager who had been at the firm for eight years had accumulated extensive system access. Her email account was compromised by attackers via spear phishing. The attackers, operating with her access, downloaded the client database to a personal cloud storage account they controlled, then offered it for sale.

What it cost: Three major clients (representing 35% of revenue) terminated relationships within 60 days of being notified. Estimated $1.2M in lost annual revenue. Legal fees and client communication costs of approximately $80,000. The firm survived but downsized to 14 employees over the following 18 months.

What would have prevented it: Least-privilege access (Section 4.3): the office manager did not need access to the complete client database for her job function. Quarterly access review (Section 6.2). MFA on email (Section 4.2). Combined cost: under $50/month.

C.11 Insurance Agency (8 employees)

What happened: Customer data including drivers' license numbers, social security numbers, and payment information was exfiltrated over a six-month period.

How it happened: The agency's customer relationship management system was accessed via a compromised employee account. The compromised account had MFA enabled, but the attackers used a credential-stuffing attack at a moment when the employee's MFA app had failed and IT had temporarily disabled MFA to troubleshoot. The 'temporary' disable was never re-enabled.

What it cost: Notification to 3,400 customers, $90,000 in legal and notification costs, ongoing identity theft monitoring obligations, state Attorney General investigation. Cyber insurance covered most direct costs but premiums increased 60% on renewal.

What would have prevented it: Process for re-enabling MFA after troubleshooting, with verification (Section 4.3). Monthly access review catching unusual login patterns (Section 6.2). Conditional access policies that require MFA from new devices regardless of state.

C.12 Engineering Firm — Deepfake CEO (40 employees)

What happened: The CFO of a 40-person engineering firm authorized a $290,000 wire transfer for what she believed was a confidential acquisition, based on a Microsoft Teams call from the CEO. The CEO had no knowledge of any of this.

How it happened: The Teams call was a deepfake. The CEO's voice was cloned from a TEDx talk three years earlier; the video was synthesized from his publicly available LinkedIn headshot. The attackers had researched the firm extensively, knew the CEO would be on a flight that day (visible from his social media), and called the CFO with a story consistent with the firm's known interest in expansion.

What it cost: $290,000 wire (recovered $40,000 through international banking cooperation). Cyber insurance covered $200,000. Net loss after insurance: $50,000 plus substantial legal fees and process audit costs. The CFO offered to resign (offer declined). Multiple subsequent client questionnaires now include questions about deepfake protections.

What would have prevented it: Verification rule for high-value wire transfers regardless of how authorization is communicated (Section 4.5). Code-word system for verbal authorizations of large transactions. Written confirmation requirement for wires above a defined threshold. The verification reflex (Section 7.1).

C.13 Marketing Agency (6 employees)

What happened: The agency's email marketing platform credentials were compromised, and attackers used the agency's account to send phishing emails to its clients' customer lists.

How it happened: The agency owner clicked on a phishing email impersonating the email marketing platform's security team. The phishing page captured her credentials. The attackers logged into the real platform and sent phishing campaigns to 30 client customer lists, branding them with the clients' logos.

What it cost: About half the agency's clients terminated their relationships within 60 days. Direct revenue loss: approximately $400,000 over the following year. The agency reduced from 6 employees to 2 within 18 months and pivoted to a different service model. The platform itself was not breached and bore no liability.

What would have prevented it: MFA on the email marketing platform (Section 4.2). Hardware MFA (YubiKey) on the owner's account (Appendix A.2). Weekly review of platform login activity (Section 6.1).

C.14 Photography / Videography Studio (5 employees)

What happened: A photography studio's archive of client photos — over 80,000 images representing 12 years of work — was encrypted by ransomware.

How it happened: An employee's personal device, used for work via BYOD, was infected with malware after she connected to a compromised public Wi-Fi network at a coffee shop. The malware spread to the studio's network when she connected at the office and reached the storage server containing the archive.

What it cost: Backup existed but was 8 months old (the studio had not run incremental backups). Ransom paid: $35,000 for partial decryption (cyber insurance authorized; about 60% of files recovered). Approximately 14,000 client photos permanently lost; client communications and partial refunds totaled approximately $20,000 in additional cost. Two clients filed complaints with state consumer protection agencies.

What would have prevented it: Policy requiring VPN use on public Wi-Fi (Section 4.3, Section 7.3). Regular automated backups (Section 4.4). Network segmentation isolating the archive server (Section 5 Phase 2). Quarterly backup testing would have revealed the missing incremental backups (Section 6.3).

C.15 IT Services Company / MSP (6 employees)

What happened: The MSP's remote management tool — used to support 80+ small business clients — was compromised. Through it, attackers gained access to dozens of client networks simultaneously.

How it happened: An MSP technician's account on the remote management platform was compromised through credential reuse. The technician had MFA on his email but not on the management platform itself.

What it cost: Catastrophic for the MSP: 35 of 80 clients terminated relationships immediately on notification, citing trust loss. Legal liability claims from affected clients totaled over $2M (largely covered by cyber insurance). The MSP closed operations within 18 months. Client losses included real damage — three of those clients suffered ransomware attacks that originated through the compromised access.

What would have prevented it: MFA on the remote management platform (the single most important control for any MSP). Hardware MFA on technician accounts (Appendix A.2). Per-client

credentials rather than shared MSP-wide credentials. Activity monitoring for the management platform (Section 5 Phase 3).

Retail and Hospitality

C.16 E-commerce Retail (12 employees)

What happened: Customer credit card information was stolen from the e-commerce site over a three-month period, affecting approximately 4,200 transactions.

How it happened: Attackers compromised the website's content management system through an unpatched plugin and inserted skimming code that captured payment information at checkout. The retailer used a payment processor but had also chosen to handle some payment data on its own servers (reducing processor fees) — that was the data the skimmer captured.

What it cost: PCI DSS investigation, $145,000 in fines and remediation costs. Customer notification, identity theft monitoring obligations. Loss of credit card processing privileges for 60 days while remediation was verified. Approximately $260,000 in lost revenue during the processing suspension.

What would have prevented it: Patching discipline for website plugins (Section 5 Phase 3). Using only PCI-compliant payment processor (no own-server payment handling). Vulnerability scanning of the website (Section 5 Phase 3). DNS-level filtering on the workstations used for website administration (Appendix A.9).

C.17 Specialty Retail / Jewelry Store (4 employees)

What happened: The store was robbed at gunpoint after attackers had used cyber-reconnaissance to identify when high-value inventory would be on premises.

How it happened: Attackers compromised the store's email and read communications with suppliers about an upcoming high-value shipment. They timed their physical robbery to occur during the 24-hour window when the items were on premises before being placed in the safe.

What it cost: Approximately $140,000 in inventory loss (partially insured). The cyber connection was discovered during the police investigation. Cyber insurance and physical insurance both contested coverage; final settlement after legal proceedings totaled approximately 70% of the loss.

What would have prevented it: MFA on email (Section 4.2). Awareness that physical security and cybersecurity intersect — sensitive operational details (delivery schedules, inventory levels) should be treated as security-sensitive and discussed in secure channels.

C.18 Restaurant (16 employees)

What happened: The restaurant's point-of-sale system was infected with malware that captured credit card information for four months before discovery.

How it happened: The restaurant used an older POS system that connected to the main computer through the office network. The office computer was compromised through phishing. The malware spread to the POS system, which lacked endpoint protection because the POS vendor had said it was 'protected by their proprietary security' (the protection was insufficient).

What it cost: PCI DSS forensic investigation, $90,000 in fines. Card replacement costs charged back: approximately $30,000. Damage to local reputation in a community where word-of-mouth dominates: estimated 12% revenue decline for 18 months following the breach.

What would have prevented it: Network segmentation isolating the POS system from the office network (Section 5 Phase 2). Endpoint protection on all systems regardless of vendor claims (Section 4.4). PCI DSS compliance audit (would have surfaced the network architecture issue).

C.19 Cafe / Bakery (8 employees)

What happened: The cafe's online ordering system began routing customer orders to a competing business across town. Customers paid for orders that never arrived; the cafe lost both the revenue and the customer relationships.

How it happened: The cafe owner's account on the ordering platform was compromised through credential reuse. The attacker (revealed during investigation to be the competing business owner's nephew) modified the routing settings to redirect a percentage of orders.

What it cost: Approximately $14,000 in misdirected orders before the issue was identified, $23,000 in customer goodwill recovery (refunds, free orders, apologies). Local press coverage that ultimately benefited the cafe but caused weeks of stress. Civil suit against the competing business resulted in modest damages.

What would have prevented it: MFA on the ordering platform (Section 4.2). Password manager preventing reuse (Section 4.2). Weekly review checking platform settings for unauthorized changes (Section 6.1).

C.20 Convenience Store / Gas Station (5 employees)

What happened: The store's network was used as a relay for attacks against a Fortune 500 company's vendor portal. The compromise was discovered when the FBI contacted the owner.

How it happened: Default passwords on the store's networked surveillance camera system allowed attackers to gain a foothold on the network. From there, they pivoted through other unpatched devices and ultimately used the network as an attack relay.

What it cost: FBI investigation imposed minimal direct cost on the owner (cooperation was the main requirement), but the network had to be completely rebuilt to satisfy investigators. Estimated $8,000 in direct rebuild costs plus a week of business disruption. The owner subsequently received elevated insurance scrutiny on renewals.

What would have prevented it: Changing all default passwords on every device (Section 4.2). Network segmentation isolating IoT and surveillance devices from the business network (Section 5 Phase 2). Patching discipline for connected devices (Section 5).

Trades

C.21 Plumbing / Electrical / HVAC Contractor (15 employees)

What happened: The contractor's customer scheduling and dispatch system was disabled by ransomware during peak summer service season.

How it happened: An employee opened a malicious attachment in an email that appeared to be from a major equipment supplier. The malware spread through the contractor's network, encrypting both workstations and the central scheduling server. Backups had not been tested; when the contractor attempted to restore, the backup system itself had been broken for 4 months.

What it cost: 9 days of operational disruption during peak season, approximately $130,000 in lost revenue. Recovery and rebuild costs: $45,000. Customer dissatisfaction and one-star reviews on local platforms. Two long-term contracts with property management companies were not renewed, citing reliability concerns.

What would have prevented it: Email security with attachment scanning (Section 5 Phase 2). Tested backups (Section 6.3). Network segmentation (Section 5 Phase 2). EDR (Section 5 Phase 3).

C.22 Landscaping / Lawn Care (22 employees)

What happened: The company's payroll was diverted to attackers for one pay period, affecting all 22 employees.

How it happened: The bookkeeper's email account was compromised. Attackers monitored the email for the payroll cycle, then sent a 'corrected' employee bank account list to the payroll service, replacing all employee accounts with a single attacker-controlled account.

What it cost: $84,000 wired to attackers (recovered approximately $30,000 through fraud cooperation). The company covered the full payroll for affected employees out of cash reserves while pursuing recovery, taking on temporary debt. Cyber insurance covered $50,000 of the social engineering loss.

What would have prevented it: MFA on the bookkeeper's email and on the payroll service (Section 4.2). Verification rule for any change to employee bank accounts (Section 4.5). Payroll service settings requiring multi-step verification for bulk account changes.

C.23 Roofing Contractor (18 employees)

What happened: The contractor's bidding information for several large commercial projects was leaked to a competitor, who underbid them on three consecutive opportunities.

How it happened: The estimator's laptop was stolen from his vehicle (left unlocked) at a job site. The laptop was not encrypted. The thief sold it to a third party who recognized the contractor's branding and offered the data to the competitor.

What it cost: Three lost contracts representing approximately $480,000 in revenue. The owner pursued civil litigation against the competitor (settled for an undisclosed amount). Months of investigation and litigation. The estimator was terminated for the security failure.

What would have prevented it: Disk encryption on all laptops (BitLocker/FileVault, free, Section 4.4). Policy requiring vehicles to be locked and laptops to be removed when unattended. Asset tracking on company hardware (Section 3.3).

Manufacturing and Specialized

C.24 Small Manufacturing / Custom Fabrication (28 employees)

What happened: The shop's CAD designs and proprietary manufacturing processes were exfiltrated and appeared in a competing product six months later.

How it happened: Attackers gained access through a compromised email account (credential reuse) and identified the file server containing design files. Over three months, they slowly downloaded the entire design archive in small batches that did not trigger any volume alerts.

What it cost: Loss of competitive advantage on the affected product line, estimated $1.2M in lost revenue over two years. Patent and trade secret litigation against the competitor cost $180,000 with mixed results. Additional security investments of approximately $40,000 in following year.

What would have prevented it: MFA on email (Section 4.2). Password manager preventing reuse (Section 4.2). Data Loss Prevention (DLP) tools for high-value file servers (Section 5 Phase 3). Logging and monitoring of unusual download patterns (Section 6.1).

C.25 Craft Brewing / Food Production (12 employees)

What happened: The brewery's website and online ordering system were taken offline by a DDoS attack accompanied by an extortion demand.

How it happened: Attackers identified the brewery as a small business unlikely to have DDoS protection. They demanded $10,000 in cryptocurrency to stop the attack. The website hosting provider initially could not absorb the attack volume on the standard hosting plan.

What it cost: 5 days of website and online ordering downtime during the holiday season. Estimated $35,000 in lost online sales. Hosting upgrade and DDoS protection: $4,000. Ransom not paid. Reputational impact was minor as customers understood the situation through clear communication.

What would have prevented it: Cloudflare or similar DDoS protection on the website (often free or low-cost, Appendix A.10). Hosting provider with DDoS resilience built in. Communication plan for handling availability incidents (Section 4.5).

Other Sectors

C.26 Trucking / Logistics Small Fleet (35 employees, 12 trucks)

What happened: The company's fleet management system was compromised, and attackers used it to redirect several high-value cargo shipments to alternate addresses where the cargo was stolen.

How it happened: Attackers gained access through a phishing attack on the dispatch coordinator. The fleet management system did not require MFA. Cargo manifests were modified to show new delivery addresses; drivers, trusting the dispatch system, delivered to the modified addresses.

What it cost: Loss of three cargo shipments totaling approximately $340,000. Customer claims and litigation. Insurance covered most cargo losses but the company's freight broker license was placed under review. Substantial customer trust damage.

What would have prevented it: MFA on the fleet management system (Section 4.2). Verification process for any address changes on active shipments (Section 4.5). Driver training to verify destination changes through dispatch by phone (Section 7.1).

C.27 Religious Organization / Small Nonprofit (4 staff + volunteers)

What happened: A small nonprofit lost $48,000 in its annual giving campaign through wire fraud targeting an elderly donor.

How it happened: Attackers compromised the nonprofit's email and identified communication with a major donor about a planned $50,000 contribution. They sent the donor wire instructions for the contribution, replacing the nonprofit's bank account with their own. The donor wired the money.

What it cost: $48,000 unrecovered (the donor's bank declined to absorb the loss; the nonprofit declined to seek recovery from the donor and absorbed the loss themselves). Cyber insurance was not in place. The nonprofit's executive director resigned over the incident. Multiple board members departed in subsequent months.

What would have prevented it: MFA on email (Section 4.2). Cyber insurance for any organization handling donations (Section 4.5). Verification reflex for wire instructions involving donations (Section 7.1). Cost: under $30/month plus insurance ($800-1,500/year for nonprofit policies).

C.28 Childcare / Educational Services (18 employees)

What happened: Parent payment information and child enrollment records were exposed in a data breach. The breach was discovered when a parent received an identity theft notification linking the source to the childcare provider.

How it happened: The provider used a small enrollment management software vendor whose database was breached. The vendor delayed notification by six weeks while internally investigating. By the time the childcare provider learned of the breach, parents had already begun receiving identity theft notifications from other sources.

What it cost: State Attorney General investigation, $40,000 settlement and notification costs. Significant parent trust damage; estimated 8-12 families withdrew over the following year. The provider sued the vendor for the delayed notification (settlement terms confidential).

What would have prevented it: Vendor security review before adoption (Section 5 Phase 2). Contractual notification timeline requirements with vendors (Section 5 Phase 3). Cyber insurance covering vendor breach (most policies include coverage for breaches at vendors holding your data).

C.29 Fitness Studio / Personal Training (6 employees)

What happened: The studio's customer payment information for monthly memberships was stolen, with about 600 customers affected.

How it happened: The studio's billing was handled through a third-party platform that suffered a breach. Attackers stole stored payment methods for thousands of small fitness businesses, including this one. The studio learned of the breach when chargebacks began accumulating.

What it cost: Approximately $8,000 in chargeback fees and processing costs. Loss of trust required transitioning to a new billing platform mid-year, with associated administrative costs of approximately $5,000. Loss of about 60 of 600 members during the transition. Total estimated impact: $35,000-45,000.

What would have prevented it: Vendor security assessment before adoption (Section 5 Phase 2). Use of payment processors with strong security track records (PCI Level 1 compliance verified). Cyber insurance with vendor breach coverage (Section 4.5).

C.30 Property Management Company (24 employees)

What happened: Tenant rent payments were redirected to an attacker-controlled account for one month, affecting approximately 280 tenants and totaling $340,000.

How it happened: Attackers compromised the property manager's email and identified the monthly tenant statement cycle. They sent updated payment instructions to all tenants on letterhead matching the company's normal communications. About 80% of tenants paid the new account.

What it cost: $340,000 redirected, recovered approximately $90,000. Cyber insurance covered $200,000 social engineering loss. Net loss: approximately $50,000 plus extensive tenant communication, legal review, and administrative cost. Three property owners terminated management contracts citing trust concerns.

What would have prevented it: MFA on email (Section 4.2). Tenant communication policy specifying that payment account information will NEVER change without separate phone notification, communicated to tenants in advance (Section 4.4, Section 7.4). Email security with anti-spoofing (DMARC) preventing the company's domain from being effectively impersonated (Appendix A.5).

C.31 Patterns Across the Cases

Reading these 30 cases produces a few clear patterns:

- Multi-factor authentication on email is the single most frequently cited preventive control. It would have meaningfully mitigated or prevented at least 23 of the 30 cases described above. It is free or near-free. If you do nothing else, do this.
- Backup hygiene — and specifically the testing of backups — is the difference between recovery and existential damage in ransomware cases. Untested backups failed in multiple cases above. Quarterly testing is non-negotiable.
- Wire transfer and payment verification rules — verifying any unusual financial instruction by phone — would have prevented or mitigated at least 8 of the 30 cases. The cost is zero. The discipline is the obstacle.
- Vendor security matters as much as your own. Multiple cases trace to vendor compromises that affected the small business through no direct fault of its own. Vendor due diligence is a real security practice.
- The losses are concentrated in a handful of categories: BEC and wire fraud, ransomware, and data exfiltration. Defending against these three categories well covers the majority of the financial risk.

These patterns are why the implementation roadmap in Section 5 is structured the way it is. Phase 1 is not arbitrary; it is the set of controls that, across hundreds of cases like these, has the highest preventive effect at the lowest cost.

Appendix D: Excel Templates Library

This appendix describes the ten Excel/Google Sheets templates that operationalize the framework. Each template has a specific purpose, a defined update frequency, and a section of the framework that uses it. Together, these ten templates are the working tools of small business cybersecurity — the discipline made tangible.

The templates are described here. Companion .xlsx files are available separately as part of the framework distribution. Each template is also reproducible by any small business willing to set up the column headers themselves; the structure is the value, not any specific implementation.

Two principles for using these templates:

- Keep them in one place. Create a single workbook or shared folder for cybersecurity working documents. Do not scatter them across personal computers. The Templates Library lives where your business records live.
- Update them on the schedule, not when convenient. The discipline is the value. A template updated on schedule for two years is more useful than one updated comprehensively once.

D.1 Template 1: Asset Inventory

Purpose

Single source of truth for everything in the business that has digital value: hardware, software, cloud services, data locations, and accounts. Foundation of the risk assessment process. Used in Section 3.3.

Update frequency

Initial completion: 4-6 hours. Maintenance: 30 minutes monthly during the access review (Section 6.2). Full review annually (Section 6.4).

Structure

The workbook contains five tabs:

- Hardware: Type | Make/Model | Serial Number | Owner | Primary Location | Operating System | Last Patched | Notes
- Software & Cloud Services: Service Name | Vendor | Type | Owner/Admin | License Type | Cost | Renewal Date | Sensitive Data Stored | Notes

- Data Locations: Data Type | Sensitivity | Where Stored | Encryption Status | Backup Location | Retention Period | Notes
- Accounts: System | Username | Owner | Created Date | Last Reviewed | MFA Enabled | Privilege Level | Status (Active/Disabled) | Notes
- Vendors with Access: Vendor Name | Service Provided | Access Type | Access Granted Date | Access Expires | Reviewed Date | Notes

D.2 Template 2: Risk Prioritization Matrix

Purpose

Working tool for risk assessment: identified vulnerabilities mapped against likelihood and business consequence, with priority ratings and remediation status. Used in Section 3.6.

Update frequency

Annual full update during the framework review (Section 6.4). Update individual rows as risks are remediated.

Structure

Single tab with these columns: Risk ID | Description | Affected Assets | Threat Type | Likelihood (Unlikely/Possible/Likely) | Business Consequence (Recoverable/Operational Disruption/Regulatory/Lose Major Customers/Could Close Business) | Priority (Critical/High/Medium/Low) | Owner | Target Remediation Date | Status | Notes

A built-in priority calculation lookup (using INDEX/MATCH or VLOOKUP against the priority matrix) automatically assigns priority based on likelihood and consequence inputs.

D.3 Template 3: Access Review Log

Purpose

Monthly record of access reviews: who has access to what, when last verified, what changes were made. Provides audit trail for cyber insurance, customer questionnaires, and regulatory inquiries. Used in Section 6.2.

Update frequency

Monthly, on first Monday of each month (or other consistent date). 30 minutes per session.

Structure

Two tabs:

- Monthly Review Log: Review Date | Reviewer | Personnel Changes Since Last Review | Account Changes Made | Anomalies Found | Follow-Up Required | Notes
- Detailed Access Audit: System | User | Access Level | Last Verified Date | Reviewer | Status | Notes (used for the systematic verification of access on a rotating quarterly schedule, hitting each system at least once a year)

D.4 Template 4: Backup Test Log

Purpose

Quarterly record of actual backup restoration tests: what was restored, how long it took, what worked, what did not, what was fixed. Used in Section 6.3.

Update frequency

Quarterly, in the first week of each quarter.

Structure

Single tab: Test Date | Tester | What Was Restored | Restoration Method | Time to Restore | Restoration Successful (Yes/No/Partial) | Issues Encountered | Resolution | Next Test Target | Notes

Quarterly test targets rotate: customer data → accounting data → email mailbox → complete workstation, repeating annually.

D.5 Template 5: Incident Response Contact List

Purpose

Pre-prepared, accessible list of who to call when something goes wrong. Used in Section 4.5.

Update frequency

Quarterly verification (call each number to confirm it still works), and immediately whenever a contact changes.

Structure

Single tab, formatted as a printable reference card:

- Internal incident response lead: Name, mobile, alternate phone
- Backup incident response lead: Name, mobile, alternate phone
- Owner (if not the IR lead): Name, mobile

- IT support / MSP: Company, account number, support phone, after-hours phone, account manager email
- Cyber insurance: Carrier, policy number, claims hotline, claims email, incident response services number
- Primary banking institution: Name, account numbers, fraud hotline (24-hour line, not the regular customer service)
- Secondary banking: same as above
- Legal counsel: Firm, attorney name, phone, email
- Cybersecurity consultant (if engaged): Name, firm, phone, email
- State Attorney General consumer protection / breach notification: state-specific contact
- FBI Internet Crime Complaint Center (IC3): ic3.gov for filing reports
- CISA: 1-888-282-0870 for federal cybersecurity reporting

This list is printed and posted in at least two physical locations in the business: the owner's office and the workspace of whoever handles money. It is also stored in a location that does not require access to the compromised systems (a printed copy in a fire-safe, a copy on a personal phone, a copy with the legal counsel).

D.6 Template 6: Vendor Security Assessment

Purpose

Quick evaluation form for new vendors that will handle business data. Surfaces vendor security practices before signing. Used in Section 5 Phase 2 and Section 6.4.

Update frequency

Completed for any new vendor before contract execution. Annual review of existing vendors during the annual framework review.

Structure

One tab per assessment. Standard sections:

- Vendor identification: name, services provided, contract value, data they will handle, criticality
- Compliance attestations: SOC 2 (with date), ISO 27001 (with date), HIPAA-relevant business associate agreement (yes/no), PCI compliance level
- Security controls: MFA available for our accounts, encryption (in transit and at rest), backup practices, breach notification commitments

- Access management: how does our access work, can we control who at our company has access, what happens if our admin leaves
- Incident history: any breaches in the last 5 years, how were they handled
- Termination provisions: data return on termination, data deletion verification, retention obligations
- Score and decision: green/yellow/red rating with rationale, owner approval, contract date

D.7 Template 7: Employee Training Tracker

Purpose

Record of who has been trained on what and when. Required for cyber insurance attestation, customer questionnaires, and regulatory compliance in some industries. Used in Section 7.3.

Update frequency

Updated whenever training is delivered. Reviewed quarterly.

Structure

Two tabs:

- Training Roster: Employee Name | Hire Date | Initial Training Date | Last Annual Training | Phishing Simulation Results (date, click rate) | Specialized Training (HIPAA, PCI, etc.) | Notes
- Training Calendar: Date | Topic | Audience | Materials Used | Completion Status | Notes

D.8 Template 8: Weekly 15-Minute Review Log

Purpose

Brief log of each weekly security review: what was checked, what was observed, what required follow-up. The most important template; the discipline made visible. Used in Section 6.1.

Update frequency

Weekly. Same time every week. 15 minutes.

Structure

Single tab with these columns: Week | Reviewer | Email Admin Findings | User Account Findings | Endpoint/Update Findings | Anomaly Findings | Follow-Up Items | Status of Last Week's Follow-Up | Notes

Many weeks the entire row will read "nothing unusual." That is the correct outcome and worth recording. The pattern of weeks with nothing unusual interspersed with occasional findings is the signature of a disciplined practice.

D.9 Template 9: Phishing Incident Log

Purpose

Record of phishing attempts that employees report — what was received, what action was taken, whether it was a true threat. Surfaces patterns over time. Used in Section 7.1.

Update frequency

Updated whenever a phishing email is reported. Reviewed quarterly to identify patterns and inform training.

Structure

Single tab: Date Reported | Reporter | Apparent Sender | Subject Line | Email Pretext (claim being made) | Determination (legitimate / spam / phishing / advanced phishing) | Action Taken (deleted / reported to provider / forwarded to IT) | Lessons / Pattern Notes

Quarterly pattern analysis is valuable: are particular vendors being impersonated repeatedly? Are particular employees being targeted? Are tactics evolving? These patterns inform security awareness updates.

D.10 Template 10: Policy Acknowledgment Tracker

Purpose

Record of which employees have read and acknowledged each business policy, with date. Required for many cyber insurance policies and provides employer protection in case of disputes.

Update frequency

Updated whenever an employee acknowledges a policy. Reviewed quarterly to confirm all current employees have current acknowledgments.

Structure

Cross-reference table: Employee Name (rows) × Policy Name (columns). Each cell contains the date the employee acknowledged that policy. Empty cells indicate gaps to fill.

Policies tracked include the four core policies in Section 4 (Password & Authentication, Access Control, Data Protection, Incident Response), plus any business-specific policies (acceptable use, BYOD, social media, others).

D.11 Putting the Templates to Work

These ten templates produce, between them, the entire artifact set of a working small business cybersecurity program. Together they answer every question a cyber insurance carrier, customer security questionnaire, or regulatory inquiry will ask:

- "What systems do you have?" → Asset Inventory (Template 1)
- "What risks have you identified, and how are you mitigating them?" → Risk Prioritization Matrix (Template 2)
- "How do you manage access?" → Access Review Log (Template 3) and the Access Control Policy
- "How do you handle backup?" → Backup Test Log (Template 4) and the Data Protection Policy
- "How would you respond to an incident?" → Incident Response Contact List (Template 5) and the Incident Response Policy
- "How do you assess third-party risk?" → Vendor Security Assessment (Template 6)
- "How do you train employees?" → Employee Training Tracker (Template 7) and the awareness program
- "How do you maintain ongoing security?" → Weekly 15-Minute Review Log (Template 8)
- "How do you handle phishing?" → Phishing Incident Log (Template 9) and the awareness program
- "How do you ensure policy compliance?" → Policy Acknowledgment Tracker (Template 10)

A small business that maintains these ten templates with discipline is a small business with a working cybersecurity program. The templates are simple. The discipline is the work.

Appendix E: Plain-Language Threat Catalog

This appendix catalogs the threats your business might encounter. Section 2 of this framework provides deep narrative coverage of the seven most common categories; this catalog is the encyclopedic reference, with shorter, structured entries for every threat category — including categories not covered in Section 2.

Read Section 2 to understand. Use this appendix to look up specific threats when something happens or when you need a quick reference. Each entry has the same structure: what the threat is, how you would recognize it, and what to do if it happens.

Email-Based Threats

E.1 Phishing (General)

What it is

An email designed to trick the recipient into clicking a malicious link, opening a malicious attachment, or sharing sensitive information. Generic phishing is sent to many recipients and is somewhat opportunistic — the attacker hopes a small percentage will fall for it.

How to recognize it

Sender address that does not match the apparent organization; urgent or threatening language; requests for credentials or sensitive data; unexpected attachments; links to unfamiliar websites.

What to do if it happens

Do not click. Do not reply. Forward the email to your designated security contact. Delete it after reporting. If you already clicked, change the affected password immediately, run a full antivirus scan, and notify IT support.

E.2 Spear Phishing

What it is

A phishing attack specifically targeting one person, usually researched in advance using publicly available information (LinkedIn, company website, social media). Far more convincing than generic phishing.

How to recognize it

Email is highly personalized — uses your name, references your role or recent activity, mentions specific colleagues or projects. May reference real but publicly available information.

What to do if it happens

Same as phishing — do not click, report it. Spear phishing succeeds on familiarity; the personalization is meant to lower defenses. Verify any unusual request through a separate channel before acting.

E.3 Whaling

What it is

Spear phishing aimed specifically at executives — CEOs, CFOs, owners. Particularly dangerous because executives often have privileged access and are also impersonated in BEC schemes.

How to recognize it

Email targeting an executive; references high-stakes business matters (acquisitions, legal issues, board concerns); often appears to come from another executive or a board member.

What to do if it happens

Same as spear phishing. Executives should be especially cautious of urgent confidential requests via email — these are precisely the patterns whaling attacks exploit. Verify through phone calls to known numbers.

E.4 Business Email Compromise (BEC)

What it is

An attack in which the attacker impersonates a legitimate business email account (compromised or imitated) to commit fraud — typically wire transfer fraud or vendor impersonation.

How to recognize it

Unusual financial instruction received by email; changes to vendor or customer banking information; urgency or confidentiality emphasized; requests to bypass normal procedures.

What to do if it happens

Do not act based on the email alone. Call a known phone number for the apparent sender to verify. If the fraud has already occurred, contact your bank immediately — wire fraud is sometimes recoverable in the first few hours.

E.5 Email Account Takeover

What it is

When an attacker gains control of a legitimate email account through stolen credentials, malware, or social engineering. Subsequent attacks (BEC, fraud, data theft) often run through the compromised account.

How to recognize it

Unusual sign-in alerts; emails sent from your account that you did not write; emails missing from your sent folder; password change you did not initiate; new forwarding rules you did not set up; complaints from contacts about strange messages.

What to do if it happens

Change the password immediately. Enable MFA if not already enabled. Review and remove any unauthorized forwarding rules. Notify contacts. Investigate what the attacker did while in control. Engage IT support and consider engaging cybersecurity professional.

E.6 Wire Fraud / Invoice Fraud

What it is

A subset of BEC focused specifically on intercepting or redirecting financial transactions — fraudulent invoices, altered banking instructions, fake vendor changes.

How to recognize it

Vendor sends new banking information by email; invoice arrives from a vendor whose payment cycle does not match; urgent payment requests with new details; invoices for amounts inconsistent with normal patterns.

What to do if it happens

Verify any banking change by phone to a known number. Establish a written policy that banking changes are never made based on email alone. If the fraud has occurred, contact bank fraud line within hours — speed matters.

E.7 Vendor Email Impersonation

What it is

An attack that uses a compromised vendor's email account or a similar-looking address to impersonate a vendor and commit fraud against the vendor's customers.

How to recognize it

Email appears to be from a real vendor but contains unusual requests, banking changes, or urgent payment demands. The email may come from the vendor's actual address (compromised account) or a near-miss imitation.

What to do if it happens

Verify with the vendor by phone using a known number — not a number provided in the suspect email. If the vendor's email is compromised, they need to know.

Malware Threats

E.8 Ransomware

What it is

Malware that encrypts your files and demands payment for the decryption key. Modern ransomware also typically steals data before encrypting and threatens to publish it.

How to recognize it

Files become inaccessible with strange extensions (.locked, .encrypted, .crypt); ransom notes appear on screens; systems stop functioning normally; unusual network activity may have been noticed in the days or weeks before the encryption (the dwell period).

What to do if it happens

Disconnect affected systems from the network immediately (do not power them off). Do not pay or negotiate without consulting your insurance carrier, legal counsel, and incident response firm. Engage incident response professionals. Restore from offline backups after the environment has been investigated and cleaned.

E.9 Banking Trojans

What it is

Malware specifically designed to steal banking credentials and intercept financial transactions. Often spreads through phishing or malicious websites.

How to recognize it

Browser slowness specifically when banking; unexpected prompts on banking sites; reports from your bank about unusual activity; antivirus alerts referencing banking trojans (Emotet, TrickBot, IcedID, others).

What to do if it happens

Disconnect the affected computer from the network. Do not log into any financial accounts from that device. Engage IT support to clean or replace the system. Change all banking and financial credentials from a known-clean device. Notify your bank and watch for fraudulent transactions.

E.10 Keyloggers

What it is

Software that records keystrokes — typically used to capture passwords and other typed sensitive information. Often part of a broader malware infection.

How to recognize it

Often invisible to the user. Detected by endpoint protection software or by indirect signs (account compromises traced back to a specific computer, accounts being accessed without other explanation).

What to do if it happens

Disconnect the computer from the network. Run thorough antivirus scan; if confirmed, the safest response is to wipe and rebuild the computer rather than attempt cleaning. Change all credentials that were typed on the affected computer, from a known-clean device.

E.11 Spyware

What it is

Software that monitors user activity and reports it to the attacker — keystrokes, screenshots, files, communications, browsing history.

How to recognize it

Antivirus alerts; unusual computer behavior (slowness, unexpected pop-ups); webcam light activating without explanation; mysterious increase in network activity.

What to do if it happens

Same as keyloggers — wipe and rebuild the affected system. Treat any data that may have been on the computer as compromised.

E.12 Cryptominers (Cryptojacking)

What it is

Malware that uses your computer's processing power to mine cryptocurrency for the attacker. Less directly damaging than other malware but indicates that your system has been compromised.

How to recognize it

Computer noticeably slower than normal; fans running constantly even when computer appears idle; battery draining quickly on laptops; high electricity bills; CPU usage extremely high without explanation.

What to do if it happens

Treat as any other malware infection — disconnect, scan, clean or rebuild. Crypto-mining infection is often a sign that other malware is present, even if cryptomining is the only thing visible.

Authentication Attacks

E.13 Password Reuse / Credential Stuffing

What it is

Automated attacks that test passwords stolen from one website's breach against thousands of other websites and services. Succeeds against any account where the same password was reused.

How to recognize it

Sign-in attempts from unfamiliar locations; login alerts; account lockouts; eventual successful access by an attacker.

What to do if it happens

Change the password immediately. Enable MFA. Use a unique password for every account going forward. Use a password manager. Check haveibeenpwned.com to see if your email address has appeared in known breaches.

E.14 Brute Force Attacks

What it is

Automated attempts to guess passwords by trying many possibilities against a single account. Most modern systems have protections (account lockouts, rate limits) but brute force attacks still succeed against systems with weak controls or against accounts with very weak passwords.

How to recognize it

Many failed login attempts; account lockout notifications; sign-in attempts at unusual hours.

What to do if it happens

If the account is locked, follow the recovery process. Use a strong password (12+ characters, mixed character types) and enable MFA when restoring access. Consider whether the targeted account holds anything sufficiently valuable that the attacker invested in trying.

E.15 Password Spraying

What it is

An attack pattern that tries one common password ("Spring2024!", "Welcome1", "Password123") against many user accounts at the same organization. Avoids account lockouts because each account only sees one or two failed attempts.

How to recognize it

Pattern of failed login attempts spread across many accounts; the same source IP attempting access to multiple accounts; the failed attempts may not trigger lockouts because each individual account has only one or two failures.

What to do if it happens

Detected primarily through centralized log analysis. If your organization has been targeted, all employees should be required to change passwords (in case any were using the spray candidate). Implement password complexity requirements that exclude common passwords. Enable MFA universally.

E.16 Session Hijacking

What it is

Stealing the active session token (the cookie that keeps you logged in) rather than the password itself. If successful, the attacker can use the application without needing the password or MFA.

How to recognize it

Activity in your account that you did not initiate; signed-in sessions you do not recognize.

What to do if it happens

Sign out of all sessions on all devices (most major platforms have this option). Change the password. Re-enable MFA if it was somehow bypassed. Investigate how the session token was stolen — usually through malware, browser compromise, or unencrypted network traffic.

E.17 MFA Fatigue / MFA Bombing

What it is

An attacker, having stolen a password, repeatedly triggers MFA prompts on the legitimate user's phone, hoping the user will eventually approve one to make the prompts stop.

How to recognize it

Multiple MFA prompts that you did not initiate; prompts at unusual hours; persistent prompts that keep returning even after dismissing them.

What to do if it happens

Never approve an MFA prompt you did not initiate. Many such prompts mean your password is compromised — change it immediately. Notify IT support so the source can be investigated. Train every employee on this specific pattern.

Social Engineering Threats

E.18 Pretexting

What it is

Creating a false context (a pretext) to manipulate someone into providing information or taking an action. The attacker poses as a credible person or authority — a vendor, a regulator, an IT support technician, an executive — to elicit cooperation.

How to recognize it

Caller or sender claims authority and asks for information that would normally require formal verification; pressure to act quickly; resistance to verification questions.

What to do if it happens

Verify before acting. The legitimate caller will not be offended by verification; the fraudulent caller will be. If in doubt, hang up and call back through a known number.

E.19 Vishing (Voice Phishing)

What it is

Phishing conducted by phone — typically a call claiming to be from your bank, the IRS, Microsoft, or a vendor, asking for sensitive information or directing actions.

How to recognize it

Caller asks for passwords, account numbers, or remote computer access; claims urgent issue requiring immediate action; pressures you to stay on the line and not consult others.

What to do if it happens

Hang up. Call back through a number from official sources (the back of your bank card, the company's website you navigated to independently). Legitimate organizations do not call demanding sensitive information.

E.20 Smishing (SMS Phishing)

What it is

Phishing conducted via text message — links to phishing sites, fake delivery notifications, fraudulent bank alerts.

How to recognize it

Unexpected text with a link; claims package delivery, account problem, prize won; pressure to click a link immediately.

What to do if it happens

Do not click links in unsolicited texts. Verify through official channels (the courier's website, the bank's app) by navigating directly, not through the text's link. Delete the text.

E.21 QR Code Phishing (Quishing)

What it is

Phishing through QR codes that lead to phishing sites. Often sent in emails or printed on physical materials. The QR code obscures the actual destination URL.

How to recognize it

Unsolicited email or printed material with a QR code; claims of a discount, document, or login that requires scanning the code.

What to do if it happens

Do not scan QR codes received in unsolicited emails or unfamiliar contexts. If you must scan, preview the URL before opening it. Verify legitimacy through official channels.

E.22 Deepfake Voice or Video Impersonation

What it is

AI-generated synthetic audio or video used to impersonate a real person. Increasingly used in social engineering — particularly executive impersonation in BEC schemes.

How to recognize it

Unusual voice or video communication from an executive, family member, or trusted contact requesting urgent action; some hint of unusual quality or context (poor connection, claimed disruption); the request is unusual or high-stakes.

What to do if it happens

Verify through a different channel. A callback to a known number defeats deepfake voice and video. For high-stakes financial requests, written verification is appropriate.

E.23 Tailgating (Physical Social Engineering)

What it is

Physically following an authorized person into a restricted area without proper credentials. Often combined with social engineering (carrying boxes, claiming forgotten badge).

How to recognize it

Unfamiliar person at the door asking to be let in; person without visible badge or credentials; person presenting a plausible story to bypass security.

What to do if it happens

Do not let strangers into restricted areas, regardless of their story. Direct them to the appropriate reception or access procedure. Train all employees that politeness does not override security.

E.24 Baiting

What it is

Attacks that exploit curiosity or greed — USB drives left in parking lots labeled "Confidential Salaries," too-good-to-be-true offers, free WiFi networks designed to capture connections.

How to recognize it

Unusual physical objects (USB drives, CDs) found in places they should not be; offers that seem too good to be true; suspicious wireless networks in business contexts.

What to do if it happens

Do not plug in unknown USB devices. Do not connect to unfamiliar wireless networks for business purposes. Treat unsolicited offers with skepticism.

Network and Web Threats

E.25 Man-in-the-Middle Attacks

What it is

An attacker intercepts communication between two parties — typically by joining the same network or controlling a network device along the path.

How to recognize it

Often invisible. Indirect signs: certificate warnings on websites, unexpected redirects, application connection errors that resolve when changing networks.

What to do if it happens

Use VPN on public networks. Pay attention to certificate warnings — do not bypass them. Use HTTPS-Everywhere or similar tools to ensure encrypted connections. Avoid sensitive activity on networks you do not control.

E.26 DNS Hijacking

What it is

Manipulation of DNS records to redirect traffic — typing your bank's address but reaching an attacker's server. Can occur at the device level (malware), router level (compromised router), or server level.

How to recognize it

Familiar websites appear different than expected; certificate warnings; redirects to unexpected destinations; antivirus alerts about DNS settings being changed.

What to do if it happens

Use trusted DNS services (Quad9, Cloudflare for Families). Pay attention to website appearance and certificate validity. Investigate any unexpected DNS changes; consider router security if it persists.

E.27 Drive-by Downloads

What it is

Malware that installs automatically when you visit a compromised website, often without any explicit interaction. Less common with modern browsers but still occurs against unpatched systems.

How to recognize it

Unexpected file downloads when visiting websites; antivirus alerts during browsing; system slowness or unusual behavior after visiting a particular site.

What to do if it happens

Keep browsers and operating systems patched. Use endpoint protection. Avoid suspicious websites; treat browser warnings seriously. If suspected, isolate the affected device and run thorough antivirus scans.

E.28 DDoS Attacks (Distributed Denial of Service)

What it is

Flooding a website or service with so much traffic that it cannot serve legitimate users. Aimed at extortion, competitive sabotage, or activism. Less common against small businesses but occurs.

How to recognize it

Website or service becomes unreachable or extremely slow; volume of traffic from many IP addresses; explicit ransom or extortion demands sometimes accompany the attack.

What to do if it happens

Engage your hosting provider or content delivery network — most modern hosts have DDoS protection capabilities. Cloudflare and similar services offer DDoS mitigation. Do not pay extortion demands.

Insider and Access Threats

E.29 Malicious Insider

What it is

An employee, contractor, or vendor with legitimate access who deliberately uses that access to harm the business — typically by stealing data, sabotaging systems, or facilitating external attacks.

How to recognize it

Unusual access patterns (downloading large amounts of data, accessing systems outside normal scope); coincidence with employee dissatisfaction or imminent departure; signs of preparation (creating backup channels, copying credentials).

What to do if it happens

Engage HR and legal counsel before taking any action. Preserve evidence. Restrict access through normal HR processes if possible. For active incidents, contain damage by limiting access; investigate carefully.

E.30 Accidental Insider (Mistake)

What it is

Harm caused by employees through error rather than malice — sending sensitive data to the wrong recipient, leaving a laptop in a taxi, choosing a weak password, falling for a social engineering attack.

How to recognize it

Reports from external parties about receiving unintended communications; lost or stolen devices; admissions from employees about mistakes.

What to do if it happens

Address calmly. The most important thing is that the employee felt safe reporting the mistake (the no-blame culture). Investigate the impact, mitigate where possible, and adjust controls or training to reduce recurrence. Do not punish the report.

E.31 Privilege Escalation

What it is

An attacker who has gained limited access exploits a vulnerability or misconfiguration to gain higher-level access — turning a regular user account into an administrator, for example.

How to recognize it

Often invisible during the attack itself; detected by reviewing logs (account elevations, new admin assignments, configuration changes) and by noticing the consequences (unauthorized actions taken with elevated permissions).

What to do if it happens

Investigate to determine the scope of access gained. Reset all elevated credentials. Patch the vulnerability or correct the misconfiguration that enabled the escalation. Treat all systems the elevated account could reach as potentially compromised.

Supply Chain Threats

E.32 Vendor Compromise

What it is

Your business is harmed because a vendor with access to your systems or data is compromised. The attacker uses the vendor's access to reach you.

How to recognize it

Reports from the vendor of their own breach; unusual activity in your systems traced to vendor access; communications that appear to be from the vendor but contain unusual requests.

What to do if it happens

Restrict vendor access until the vendor has completed their incident investigation and remediation. Investigate your own systems for any access that occurred during the vendor's compromise period. Adjust contractual security requirements with the vendor going forward.

E.33 Software Supply Chain Attack

What it is

Malware delivered through a compromised software update from a legitimate vendor. The 2020 SolarWinds attack is the most famous example; smaller-scale incidents occur regularly.

How to recognize it

Endpoint protection alerts following a software update; unusual behavior shortly after applying a routine update; explicit notifications from software vendors of compromised releases.

What to do if it happens

Disconnect affected systems if active compromise is suspected. Engage incident response. Apply vendor-provided patches or removal tools. Investigate scope of access during the compromise period.

E.34 Service Provider Compromise

What it is

Your IT support provider, MSP, or other service provider is compromised, exposing all of their customers — including you.

How to recognize it

Notifications from the service provider of a breach; unusual activity in your systems traced to administrative tools; coordinated incidents affecting multiple businesses served by the same provider.

What to do if it happens

Engage incident response. Investigate scope. Reset all credentials that the provider had access to. Reassess your relationship with the provider — service providers that suffer security incidents demonstrate either capability gaps or resource constraints that may continue.

Data and Physical Threats

E.35 Data Exfiltration

What it is

Unauthorized removal of data from your systems — typically by attackers after a successful intrusion, or by malicious insiders.

How to recognize it

Unusual outbound network traffic; large data downloads or transfers; accounts accessing data outside their normal scope; eventual appearance of stolen data on hacker forums or in third-party hands.

What to do if it happens

Engage incident response. Investigate scope of data taken. Notify affected parties as legally required. Strengthen access controls and monitoring to detect future exfiltration earlier.

E.36 Data Extortion (Without Encryption)

What it is

Attackers steal data and threaten to publish it unless paid — without encrypting your systems. Increasingly common as ransomware groups have shifted toward this model.

How to recognize it

Demand for payment to prevent data publication; the attacker may show samples of stolen data to prove the claim; no operational impact (your systems still work) but significant data exposure threat.

What to do if it happens

Engage incident response, legal counsel, and cyber insurance. Do not pay or negotiate without professional guidance. Notify regulators and affected parties as legally required, regardless of payment decision.

E.37 Device Theft

What it is

Physical theft of laptops, phones, or external drives — from offices, vehicles, hotels, or in public.

How to recognize it

Missing device; reports from employees of stolen property; evidence of break-ins or unauthorized access to physical spaces.

What to do if it happens

Treat all data on the device as potentially compromised. Use device management tools to remote-wipe if possible. Change credentials that were stored on or accessible from the device. File police reports. Apply lessons to prevent recurrence (cable locks, hotel safes, never leaving devices in vehicles).

E.38 Physical Break-In

What it is

Unauthorized physical access to your office or other facilities, with theft or compromise of computer systems.

How to recognize it

Evidence of forced entry; missing or moved computers; unfamiliar devices left behind; alarm system events; signs of network intrusion that begin shortly after physical access.

What to do if it happens

Treat all systems in the affected location as potentially compromised. Engage IT support and possibly incident response. File police reports. Investigate whether the physical break-in was opportunistic theft or targeted access (which suggests further sophistication).

E.39 Hardware Tampering

What it is

Modification of hardware to insert malicious capability — keyloggers, hardware skimmers on payment terminals, modified network devices.

How to recognize it

Visual signs of tampering on devices; payment skimmers physically attached to card readers; unfamiliar devices on the network; antivirus or behavioral detection alerts of unusual activity.

What to do if it happens

Daily inspection of payment terminals. Tamper-evident seals on critical devices. Replacement of suspect hardware. For high-stakes environments (financial services, point-of-sale-heavy retail), consider tamper-detection technology.

Modern and Emerging Threats

E.40 AI-Generated Phishing

What it is

Phishing emails written by generative AI — grammatically correct, fluent, often personalized, indistinguishable from professional human writing.

How to recognize it

The defenses based on writing quality (poor grammar, awkward phrasing) no longer apply. Recognition is procedural: any unusual request is verified through a separate channel, regardless of how legitimate the email appears.

What to do if it happens

Same as any phishing — do not act, verify through known channels, report. Train employees that the era of recognizing phishing by writing errors is ending.

E.41 SIM Swapping

What it is

An attack where the attacker convinces a mobile carrier to transfer your phone number to a SIM card they control. Defeats SMS-based MFA and enables account takeovers.

How to recognize it

Sudden loss of cell phone service; texts and calls stop arriving; account password reset notifications you did not request; unusual financial activity.

What to do if it happens

Contact your mobile carrier immediately to recover the number. Change passwords on all financial and email accounts that may have been targeted. Report to law enforcement. Migrate from SMS-based MFA to app-based or hardware MFA going forward.

E.42 Cryptocurrency Theft

What it is

Theft of cryptocurrency holdings from business or personal wallets. Particularly relevant for businesses that hold cryptocurrency or accept cryptocurrency payments.

How to recognize it

Unauthorized transactions in cryptocurrency wallets; phishing emails impersonating cryptocurrency platforms; access from unknown locations; recovery phrase compromise.

What to do if it happens

Cryptocurrency transactions are generally irreversible. Move remaining funds to a new wallet immediately. Investigate compromise scope. For business-held cryptocurrency, hardware wallets and multi-signature arrangements are essential.

E.43 Prompt Injection (AI Tool Compromise)

What it is

If your business uses AI tools (chatbots, AI assistants, automated email handlers), attackers may inject malicious prompts that cause the AI to take harmful actions or reveal sensitive information.

How to recognize it

Unexpected actions by AI tools; data leakage through AI responses; AI tools providing assistance to unauthorized parties.

What to do if it happens

Audit AI tool usage and controls. Limit what business processes AI tools can access. Treat AI-generated outputs with appropriate skepticism. Stay current on prompt injection developments as the field evolves rapidly.

E.44 Cloud Misconfiguration Exposure

What it is

Sensitive data exposed through misconfigured cloud storage, databases, or APIs. Frequently the cause of large breaches; often discovered by security researchers before attackers, but exploited when found by attackers first.

How to recognize it

Notifications from researchers or law enforcement of exposed data; sudden unexpected access patterns to cloud resources; data appearing in third-party hands.

What to do if it happens

Engage cloud expertise immediately to identify and close the misconfiguration. Investigate scope of exposure (often through cloud provider logs). Notify affected parties as legally required. Implement automated configuration scanning to prevent recurrence.

Closing

This concludes the SMB Cybersecurity Framework. It is not the last word on cybersecurity for small businesses — the threat landscape evolves, the tools improve, the practices refine — but it is enough to begin.

Begin with the five things in Section 5.1. Add the discipline in Section 6. Adopt the policies in Section 4 over your first 90 days. Do the risk assessment in Section 3. Train your employees with Section 7. Use the appendices when you need them. In a year, you will have a working cybersecurity practice that puts your business among the best-protected small businesses in the country.

That is the offer. Take it.

Discipline first. Then even Excel is a good tool.

© 2026 Iurii Zhurov · SMB Cybersecurity Advisors LLC · Palm Harbor, Florida

This framework is freely available for use by U.S. small and medium-sized businesses.
Reproduction and distribution for non-commercial purposes is permitted with attribution.