The Small Business Security Playbook

A Four-Category Framework for Owners Without an IT Team

Sylvan Press

Sylvan Press

Field-tested, plain-English references for the people who do the work and stand behind their call.

Contents

The Small Business Security Playbook

A Four-Category Framework for Owners Without an IT Team

Published by Sylvan Press, the security imprint of Sylvan Assurance, LLC — Vermont, USA.

ISBN (paperback / hardcover / ebook): to be assigned prior to publication.

Print and ebook ISBNs are registered through Bowker before release.

First edition, 2026.

Disclaimer. This book provides general guidance and recommended security and compliance practices, not legal, financial, or professional advice, and it does not create any advisory or consulting relationship between the author, the publisher, and the reader. Every recommendation is optional — a widely accepted way to reduce a common risk — and the reader decides which to adopt, adapt, or decline. Following this guidance reduces exposure to common risks but does not guarantee any particular outcome and does not prevent any particular breach, incident, or loss. Where this book refers to laws, regulations, standards, or commercial products, it does so for general awareness only; confirm specific obligations with qualified counsel, and note that product references are illustrative and do not constitute endorsement.

Sylvan Press — sylvanassurance.com

Preface

If you own a small business, you have probably been told you should care about security — and you have probably not yet worked out what to do about it. You do not need more advice. You need a framework you can actually execute: a small, ordered set of things to do that moves the business from *aware-but-overwhelmed* to *defended-where-it-matters*, using time and tools you can actually afford. This book is that framework, built for a non-technical owner to implement across a year of focused work plus a light sustaining cadence thereafter.

It started as a series of conversations. Friends running small businesses — a consulting firm, a clinic, an e-commerce shop, a freelance design practice — would ask for some time to talk about security. They had been told they should be doing something. They were not sure what. The literature aimed at them was either intimidatingly technical or contemptuously dumbed-down, and the frameworks they kept hearing about — NIST, ISO, the various compliance regimes — were built for organisations with security staff. Small businesses do not have security staff.

The frameworks here come from more than two decades of professional security practice inside a top-25 global company — across network security, corporate information security, computer security incident response, and a product security incident response team (PSIRT): handling vulnerabilities in software and hardware products, receiving reports from researchers, triaging them, coordinating fixes with

engineering, managing disclosure, and navigating the inevitable mess when something goes wrong. The work is mostly invisible. When a PSIRT is doing well, disclosures come out cleanly, fixes ship on schedule, and the public never knows there was a problem. When it is doing badly, the company turns up in the news.

Across those conversations, a pattern emerged. The same things that go wrong at enterprise scale were going wrong at small businesses, with the same root causes — credentials reused across services, accounts that should have been deactivated but were not, backups that had never been tested, software unpatched for years — and the same kinds of consequences. The difference was not the attacks. The enterprise had a team to absorb the work. The small business had the owner. This book is the longer version of those conversations: the patterns from years of incident-response work, applied at the scale and budget a small business can sustain.

It is worth being honest about what the book does not do. It does not turn anyone into a security professional. It does not eliminate the possibility of incidents. It does not substitute for legal counsel in regulated industries, for incident-response specialists in serious situations, or for the deeper work a business needs as it grows. The case studies are composites, fictionalised to make specific points without identifying any specific business; the framework is grounded in real work, real incidents, and real remediation.

How to Use This Book

The book is organised to support several different reading patterns. Choose the one that matches your situation.

Reading path 1: Cover-to-cover, for first-time readers. If you have not engaged with small business security in any structured way before, read the book straight through. Part I (Chapters 1, 2, 3) is foundational; Part II (Chapters 5 through 8) is the framework itself; Part III (Chapters 9 through 12) is practitioner tools; Part IV (Chapters 13 through 15) covers solo operators, tabletops, and training; the closing chapter addresses sustaining the practice over time. Chapter 4 introduces the three recurring case-study businesses that appear throughout the rest of the book.

Reading path 2: Skip to the category that matches your current gap. If you have already started thinking about security and know roughly where your weaknesses are, start in Part II with whichever chapter addresses your priority. Chapter 5 is Identity and Access Management — the highest-return category for most small businesses. Chapter 6 is Data Classification and Retention — the right starting point for regulated businesses. Chapter 7 is Backup and Disaster Recovery — appropriate for businesses with operational continuity concerns. Chapter 8 is Vulnerability and Patch Management — the right priority for businesses with substantial software surface. You can return to Part I for the framing if needed.

Reading path 3: Right-now triage. If something has just happened

or might be happening, skip to Chapter 11 (The First 48 Hours). It is the chapter you reach for during an incident. After the incident is resolved, the rest of the book covers what to do so that the next one — if there is one — is smaller and more contained.

Reading path 4: Starting from scratch. If the question is *where do I begin?*, Chapter 9 (Your First Five Fixes) is a triage list of the five concrete actions that produce the most security return for the least time invested. Read it first, do the five fixes, and then return to the rest of the book for the broader framework.

A note on the case studies. Three fictional businesses appear throughout the book as recurring case studies: Acme Pro Services (a 22-person consulting firm), Brightside Commerce (a 7-person e-commerce shop), and Cedar Clinic (a 4-person medical practice). They are introduced in Chapter 4 and revisited across the framework chapters. None of them is meant to represent the reader's specific business; parts of each will sound familiar.

A note on what is fresh writing versus established standards. The framework in this book is grounded in standards including the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), ISO/IEC 27001 (jointly published by the International Organization for Standardization and the International Electrotechnical Commission), and various regulatory and incident-response practices. The specific synthesis — the four-category structure, the maturity model, the recurring case studies, the practitioner tools — is original to this book. Readers familiar with the underlying standards will recognise the conceptual roots; readers unfamiliar with the standards do not need to engage with them to use the framework.

A note on terms. Acronyms are expanded on first appearance in each chapter. A glossary of terms appears as part of Appendix A. Technical jargon is kept to a minimum throughout; where it is unavoidable, the meaning is given in plain language at first use.

A note for readers outside the United States. The framework itself is jurisdiction-neutral; the regulatory examples lean American because the case-study businesses are. Chapter 12 covers how to work out which regimes apply to your business — including the European Union's General Data Protection Regulation (GDPR) and UK GDPR

— wherever it is based.

A note on what the book does not advise. This book provides general guidance, not legal, financial, or compliance advice. Specific situations — particularly those involving regulated data, active incidents, or contractual obligations — may require professional counsel. The book is explicit about where those boundaries lie.

The work begins in Chapter 1.

About This Book

This book is produced by **Sylvan Assurance, LLC**, as part of the Sylvan Press security imprint.

The framework presented in this book provides general guidance and recommended security practices for small or medium-sized businesses (SMBs), drawn from widely recognised security standards and frameworks, professional incident response experience, and observed patterns across small business security incidents. It is **not** a professional security audit, a penetration test, a certification, or legal advice, and it does not create any advisory or consulting relationship between the author, the publisher, and the reader.

Every recommendation in this book is **optional** — a widely accepted way to reduce a common risk. The reader decides which recommendations to adopt, adapt, or decline. Following this guidance reduces exposure to common attack patterns and improves the defensibility of a small business's security posture, but it **does not guarantee security and does not prevent any particular breach, incident, or loss**. Responsibility for the security of the business, its systems, and its data remains with the operator of the business.

Where this book refers to laws or regulations, it does so for general awareness only. Specific obligations should be confirmed with qualified legal counsel.

Where this book references commercial products or services by name, those references are illustrative. The author and publisher have

no commercial relationship with any of the products mentioned, and inclusion does not constitute endorsement.

The first chapter begins on the next page.

1 The Drowning Owner

If you are reading this book, you have probably been told too many times that you should be doing something about cybersecurity. You have probably not done very much about it.

This is not a moral failing. It is a structural problem.

Small-business owners are besieged by security advice. Vendors want to sell them software. Insurance brokers want them to qualify for coverage. Clients want them to sign clauses they only partially understand. And the headlines pile up about other small businesses that did not take security seriously enough and no longer exist.

The advice is contradictory. The vocabulary is intimidating. The recommended next steps usually require either an internal IT team you do not have or a budget you cannot justify.

The natural response, after enough of this, is to do nothing. Not because you do not believe security matters. Because the path from where you are to "doing security properly" looks impossibly steep. Each individual recommendation makes sense in isolation. Together they sum to a security programme you cannot run. It would require hiring someone. Or buying tools at price points that feel disproportionate for a business of your size. Or spending six months on a compliance project that pulls you away from the work that actually makes the business run.

This book exists for the readers who are drowning in security advice and have not done very much about it. It is not going to solve every

problem. It is not going to make you a security expert. What it will do is give you a small, ordered set of things to do. It will explain why each of them matters. And it will give you a sustainable practice for doing the work as a normal part of running your business — not as a periodic special project.

The framework was designed for a specific kind of business. Three to fifty employees. No internal IT staff. Sensitive data of some kind: client information, financial records, employee files, or any of the things small businesses inevitably accumulate. And owners who have been told they need to do something about security without ever being shown what *something* concretely means.

1.0.1 What this book is, and is not

This book is a practical framework for small-business security. It is structured around four categories of work. Each category is applied at a level of process and detail that small businesses can actually sustain. The framework is designed for a non-technical owner to implement across a series of focused work sessions, with maintenance that fits inside a quarterly calendar.

The book is not a textbook on cybersecurity. The technical depth is deliberately limited. Enough to make decisions. Not enough to substitute for specialised expertise.

The framework references underlying standards. The most common ones are two widely used security standards, the NIST CSF and ISO/IEC 27001. You do not need to study them. The framework does not assume you have a Chief Information Security Officer (CISO). It does not assume you have anyone whose job title contains the word "security."

The book is not a sales tool for a particular set of products. The recommendations name specific tools where useful. The tools are interchangeable with similar alternatives. The framework holds together regardless of which specific tools you choose.

The book is not a substitute for legal counsel, professional incident response, or specialised compliance work in highly regulated industries. The framework reduces the surface area of work in these spe-

cialised areas considerably. It does not eliminate the need for outside help where outside help is appropriate. The book is explicit about where those boundaries lie.

Finally, the book is not a thorough programme. Securing a small business completely is not possible. Security is a matter of degree, not a binary state. The framework is intended to reduce the most common attack paths. It is intended to improve the business's defensibility when something goes wrong. It does not produce perfect security, and it does not claim to.

1.0.2 Why "do everything" is a trap

The single most common path to small-business security failure is the attempt to do everything.

Owners read about security and become convinced they need to address all of it at once. They commit to a thorough programme. They start implementation. Within three weeks, the programme collides with the actual operational demands of running the business. Something has to give. Usually the security programme is what gives. The business reverts to where it was before the attempt began — with the additional weight of having tried and failed.

The trap is not that the thorough programme was unrealistic in its individual components. Most of the components are reasonable. The trap is that small businesses do not have the operational slack to run multiple unrelated initiatives at once. Sequencing matters more than scope. Pacing matters more than ambition. A small business that implements three controls thoroughly over six months ends up in a better position than one that attempts twenty controls and finishes none of them.

The framework in this book is designed to be sequenced. Each chapter builds on the previous ones. The recommended work is bounded by sections that can be completed in distinct sessions of focused work. It is not a continuous programme that has to be sustained indefinitely.

Once the initial implementation is complete, the maintenance fits inside the normal rhythms of the business. Quarterly access re-

views. Annual recovery tests. Event-triggered updates when something changes.

This is the right pacing for almost every small business. It is slower than what enterprise security programmes target. It is also vastly more likely to actually happen — which is the variable that matters.

1.0.3 The Operational Resilience frame

The framework is organised around a concept called *operational resilience* rather than around *security* as it is commonly understood.

The distinction matters. Security, in its strict sense, is about reducing the likelihood of bad things happening. Attackers getting in. Data being stolen. Systems being disrupted. Operational resilience is broader. It includes the prevention work. It also includes the work of continuing to operate when things do go wrong, recovering quickly from disruptions, and limiting the consequences of incidents the prevention work fails to stop.

For a small business, operational resilience is a more useful frame than security alone. Three reasons.

First, the work that produces operational resilience also produces security as a side effect. A business with strong backups, clear data inventories, and tested incident response capability is harder to harm. It is harder to attack for many of the same reasons. The relationship runs in both directions.

Second, the operational resilience frame matches how small business owners actually think about risk. Owners are not worried, in their gut, about whether their security controls are technically up to enterprise standards. They are worried about whether the business continues to function when something happens. Whether the storefront stays up during the holiday season. Whether client data does not disappear. Whether the business survives an incident if one occurs. The resilience frame addresses those questions directly.

Third, the resilience frame produces better priority-setting than a security-only frame. When the question is "what should we focus on?", the resilience answer is usually clearer than the security answer. The most valuable work to do is the work that reduces the worst plausible

consequence of the most likely failure modes. That framing produces a natural sequence. Pure security framing tends to produce sprawling lists.

The four categories are Identity and Access Management, Data Classification and Retention, Backup and Disaster Recovery, and Vulnerability and Patch Management. Each contributes to both preventing incidents and limiting their consequences when prevention falls short.

1.0.4 The four categories at a glance

The framework's four categories address distinct failure modes. Together, they account for the bulk of incidents that affect small businesses.

Identity and Access Management addresses the question of who can reach what. The single largest cause of small-business breaches is account compromise. Credentials get stolen through phishing. They get reused across services that have since been breached. They belong to accounts that should have been deactivated when an employee left. Identity and Access Management (IAM) is intended to close these paths through Multi-Factor Authentication (MFA — the second step at sign-in, like a code on your phone, that a stolen password alone cannot pass), controlled access privilege, and disciplined offboarding.

Data Classification and Retention addresses the question of what data you hold. How sensitive each piece is. What regulations apply to it. How long you keep it. Most small businesses have not deliberately decided any of this. Data accumulates by accident. The classification work makes the surface visible and the regulatory exposure tractable. The retention discipline reduces the volume of sensitive data the business holds at any moment. That reduces both the consequences of breaches and the surface area of ongoing regulatory obligation.

Backup and Disaster Recovery addresses the question of whether the business continues to operate when something goes wrong. The failure could be a ransomware attack, a hardware crash, a cloud service outage, or an environmental event. The difference between a survivable incident and an existential one is usually the quality of the backup strategy and the discipline of having actually tested recovery.

Vulnerability and Patch Management addresses the question of keeping the holes in your software closed as they are discovered. Most successful attacks that do not involve credential compromise involve unpatched flaws in software the business is running. The discipline is straightforward. Inventory what you have. Watch for disclosed vulnerabilities. Apply patches on a defined cadence. The work requires sustained attention. The absence of that attention is what most small businesses get caught on.

The four categories interact. Identity and Access Management controls who can reach the data classified in Data Classification and Retention. Data Classification informs the priorities of Backup and Disaster Recovery. Vulnerability and Patch Management protects the systems where the data lives and the credentials operate. A weakness in any one category undermines the others. Strength in all four typically produces a system more reliable than the sum of the individual controls.

1.0.5 What is not in the framework

The framework deliberately leaves several things out — network architecture, formal penetration testing, EDR and SIEM tooling (the enterprise-grade software that watches each computer for break-ins and collects logs at scale), sophisticated threat modelling, and the specific demands of regulated-industry compliance (HIPAA, PCI DSS, GDPR, and the like; Chapter 12 covers how to tell which regimes apply to you). Each is either lower-value per unit of effort at this scale, or out of scope for a non-technical owner working in focused sessions. Chapter 2 sets out the full list and the reasoning behind each exclusion.

The boundary is drawn at one line: the work has to be implementable by a non-technical owner working in focused sessions. Everything inside that boundary is the framework. Everything outside is appropriate but separate.

1.0.6 What you will be able to do by the end of this book

Before the capability list, the honest bottom line: implementing this framework costs a typical small business 80–150 hours of focused work

in the first year — spread across twelve months, an hour or three a week alongside running the business, not a season you must somehow clear — then 20–30 hours a year to sustain, plus $500–$2,000 a year in tools. That is the price of everything on the list below.

A reader who has worked through this book and implemented the framework will, by the end, be able to:

- Maintain a current inventory of every service the business uses, who has access to each, and at what level
- Have MFA enabled on every service that supports it, with the strongest method available
- Use a password manager consistently across the team, with no reused passwords on services that matter
- Run a documented offboarding process within twenty-four hours of any departure
- Maintain a data inventory that maps every category of sensitive data to its location, who has access, and how long it should be retained
- Have a clear sense of which regulations apply to the business, what notification windows exist, and what specific obligations are operational
- Operate with three copies of business-critical data, on two different storage media, with at least one offsite and one immutable — a copy that cannot be changed or deleted, even by someone holding valid credentials
- Have a tested recovery process with a known recovery time
- Receive and triage vulnerability disclosures on a monthly cycle, applying critical patches within 72 hours
- Have a documented incident response plan with the right contacts pre-identified
- Run quarterly tabletop exercises to maintain incident-response muscle memory
- Provide annual security awareness training to staff
- Carry cyber insurance with terms aligned to the business's exposure (or have made a deliberate decision not to)

This list is not exhaustive. The framework produces second-order ef-

fects that are difficult to enumerate in advance. Better organisational practices. Clearer vendor management. More defensible answers to client security questions.

The list is also not free. Implementing the framework takes work. The book is structured to make the work as efficient as possible. It is still work.

The same accounting, with the detail: the 80–150 first-year hours are focused effort, not calendar time — spread across twelve months, they sit alongside running the business rather than on top of it. Sustaining work runs 20–30 hours per year thereafter, mostly in quarterly and annual cycles. Tool spending is modest — typically $500–$2,000 per year, depending on the business's size and risk profile.

For most small businesses, that is the right amount of investment. Less than that produces inadequate protection. More than that produces compliance theatre without proportional benefit.

The rest of the book is the framework itself. Chapter 2 explains why these specific four categories were chosen. Chapter 3 introduces the maturity model used to assess each category. Chapter 4 introduces the three businesses — Acme, Brightside, and Cedar — that appear as recurring case studies. The work begins in earnest in Part II.

Most readers will not implement the framework cover-to-cover in a single push. The framework rewards working through it sequentially. It also tolerates picking and choosing once the foundation is in place. The best reading strategy is to work through Chapters 2 and 3 fully, then choose one category from Part II as the first implementation target. Read the rest of the book at whatever pace makes sense as the work progresses.

There is no rush. There is also no time like now.

You've just read Chapter 1 of

The Small Business Security Playbook

The full book runs 339 pages across 16 chapters,
with a complete back-of-book index.

Published by Sylvan Press, the book imprint of Sylvan Assurance — field-tested, plain-English references for the people who do the work.

Scan to see the full book — and where to buy it.
sylvanassurance.com/go/smb-security-playbook

Not ready for the full book? See where you stand first — free, a few minutes:

sylvanassurance.com/go/free-smb-security-assessment