

THE BUSINESS LEADERS SERIES

Cybersecurity for Business Leaders

SMB EDITION

CYBER RISK, PROTECTION, AND PRACTICAL STEPS

FOR SMALL-BUSINESS OWNERS AND THE PEOPLE WHO RUN THEM

*Your MSP is the program.
If they are weak, you are weak.*

Make them show you the proof.



THIS GUIDE · 3 OF 6 IN THE SERIES

J.W. WALKER · [JEREMYWALKER.US/RESOURCES](https://jeremywalker.us/resources) · WITH IDEAL TECHNOLOGYS

Cybersecurity is no longer an IT problem. It is a governance responsibility. When a ransomware attack locks your core systems or a vendor breach exposes customer data, you don't face an IT failure. You face a business failure: regulatory scrutiny, legal liability, and the erosion of customer trust. This guide is written to help you govern that risk in plain business terms, without needing to become a technical expert.

TWO PRINCIPLES THAT SHOULD GUIDE EVERYTHING

Before the domains, the controls, and the checklists, two ideas should shape how you and your leadership team read everything that follows. Get these two right and the rest becomes judgment. Get them wrong and no amount of tooling will save you.

Compliance is a floor, not a ceiling. Passing a compliance audit or an insurance security questionnaire means you cleared a minimum bar, not that your business is secure. A business with a clean audit or insurance review can still be breached tomorrow. Compliance confirms baseline adequacy; it does not confirm safety. Govern to your actual risk, and let compliance follow as a byproduct, never the other way around.

Govern the risk you cannot delegate. Leadership does not manage firewalls or read scan results. But leadership owns the decisions management cannot make alone: what risk the business will accept, whether findings are actually being resolved, whether the program is funded, and whether the reporting it receives is appropriate and honest. Those cannot be handed to IT. They are the substance of governance.

Five Things This Week

Do not try to build a whole program from this guide in one sitting. Do these five things first. They close the holes that actually take small businesses down, and everything else in this guide builds from here. [2]

- 1. **Turn on MFA everywhere money, email, or customer data lives.** Microsoft 365 or Google, banking, payroll, accounting, and your password manager. If a system cannot do multi-factor authentication, that system is now a risk item, not a convenience.
- 2. **Pin down your backups, in writing, with your MSP.** Ask where the backups are, whether they are offline or immutable, when they were last actually restored, and the real restore time for the systems that take payment and run payroll.
- 3. **Protect the owner personally.** Freeze your credit at Equifax, Experian, TransUnion, and ChexSystems, then lock your mobile-carrier account with a PIN and port-out protection. You are a target because of your role.
- 4. **Write the money rule on one page.** Send it to anyone who can move funds: no payment-detail change, no new vendor account, no urgent wire, without a callback on a number you already have. Voice is not verification.
- 5. **Compare your insurance application to your MSP contract.** Highlight every control the insurer requires and every security obligation the MSP claims. The gaps between those two documents are your real to-do list.

Then use the rest of this guide to tighten what those five exposed.

WHAT'S IN THIS GUIDE

Start Here: Five Things This Week	The five actions that close the holes that take small businesses down
Your MSP Is the Program	Why your managed provider is the real security program, and how to govern it
The Minimum Viable Program	The whole program for a business under fifty people, on one page
1. Cybersecurity as a Leadership Issue	Why cyber risk is now a leadership responsibility, and what that means

2. The Threat Landscape	The attacks businesses actually face today
3. AI and Emerging Threats	Deepfakes, AI fraud, and governing the AI your staff already uses
4. The Security Landscape	The core security domains in plain English
5. Identity Is the Control Plane	Why identity, not the firewall, is where the fight happens
6. Data Protection and Customer Trust	Where customer data lives and how to protect it
7. Vendor and Third-Party Risk	Governing every other vendor beyond your MSP
8. Resilience, Backups, and Continuity	Recovering when, not if, something goes wrong
9. The Risk Management Process	How to right-size risk management for a small business
10. Testing, Audits, and Assessments	What each review tells you, and what it does not
11. The Numbers Worth Watching	The few numbers an owner should actually watch each quarter
12. Questions to Ask Quarterly	A repeatable governance cadence
13. The First 90 Days	A checklist for new leaders and annual review
14. Your People Are Under Attack Too	Personal security for owners and executives

Your MSP Is the Program

For most small businesses the managed IT provider is not one vendor among many. They hold the keys. They have administrative access to your systems, they manage your backups, and they get the after-hours call. If they are weak, you are weak. If they are breached, you are breached. And no examiner or regulator is checking them for you. Treat the MSP relationship the way you would treat a controller who also has the checkbook: with clear rules, real proof, and no blind trust.

Why an MSP, and How to Know Yours Is Good

For most small businesses, a managed provider is the better model, and it is worth being honest about why. A single in-house IT person is one human being with one set of skills, one calendar, and one point of failure; when they are on vacation, sick, or simply out of their depth on security, you are exposed. A capable MSP gives you a team instead of a person: security, backup, cloud, and compliance expertise that no single generalist carries, coverage that does not take a day off, and buying power that makes good tooling affordable at your size. For most businesses under fifty people, that is more protection per dollar than hiring the equivalent in-house, if the provider is a good one.

The catch is the flip side: a weak MSP is more dangerous than no MSP, because you believe you are covered when you are not. “We have IT people” is not the same as “we are secure.” That is the entire reason the rest of this section exists. If you use an MSP, and most small businesses should, do not take the protection on faith. Hold them to the standards below, ask the questions, and make them show you the proof. A good provider will welcome it. A weak one will get uncomfortable, which tells you what you need to know.

Put This in the Contract, or Do Not Sign

- **MFA and unique logins for every technician.** No shared “support” account that everyone uses.
- **Fast written notice of any security incident,** at the MSP or in your environment, quick enough to meet your state and insurance clocks. Do not accept “promptly.”
- **Your data, logs, and documentation are yours** and transferable to you if the relationship ends.
- **A named restore-time target** for the systems that take payment and run payroll.

- **The right to see proof** on a fixed cadence: backup-test results, the list of who has admin access, and open critical findings.
- **No silent subcontracting** of your environment to another party.

Ask This Every Quarter

These belong in a real quarterly business review, not a friendly vibe check. If your provider cannot answer them without reaching for a sales slide, you do not have a security partner. You have a break-fix shop with a security line item.

- Show me the last successful restore. What was in scope, how long did it take, and what failed?
- Who at your company currently has admin access to us, and when did you last review that list?
- What critical patches are open on our systems right now, and why?
- What would you do in the first four hours if our email or our backups were hit?
- What are you seeing in businesses like ours that we have not addressed yet?
- If we parted ways in 30 days, what would we not have?

The Minimum Viable Program

If you have fewer than about fifty people, this is the program. Everything else in this guide is improvement, not the floor. The work splits cleanly into what you own and what your MSP owns, and it ends in four simple documents.

What You Own

- The risk you will not accept. For example: no shared admin passwords, no untested backups, no vendor with admin access and no contract notification clause.
- Who can move money, and the callback rule that governs it.
- What happens in the first 24 hours of an incident: who calls the MSP, who calls counsel, who calls the insurer, and who talks to customers.
- A quarterly review of open findings, backup tests, and who has vendor access.

What Your MSP Owns (and Must Prove)

- Identity: MFA on every privileged and remote account, admin accounts kept separate from daily-use accounts, and departing staff removed within 24 hours.
- Devices: endpoint protection on every machine that touches business data, and patching on a defined schedule.
- Email and collaboration security.
- Backups that meet a stated recovery target, with a restore test at least twice a year and the results in writing.
- Monitoring, and a defined path to reach someone after hours.
- A current list of who has admin access, including the MSP's own technicians.
- Incident notice to you fast enough that you can meet your insurer and state deadlines.

The Artifact, Not the Binder

You do not need a forty-page policy set to start. You need four living documents: a one-page incident card with names, numbers, and authority; a vendor list showing who has access to what; an open-findings list with owners and dates; and proof of your last successful backup restore. If those four do not exist, you do not have a program. You have a vendor.

1. Why Cybersecurity Is a Leadership Responsibility

In most organizations, cybersecurity was historically treated as an IT concern. That era is over.

When a ransomware attack locks your core business systems, you cannot serve customers, invoice, or make payroll, and every day of downtime is money you do not get back. When a business email compromise redirects a wire, the money is often gone before you notice. When a vendor breach exposes customer data, you face legal liability, notification costs, and lasting damage to the trust that defines your relationship with your customers. For a small business, any one of these can be an existential event, not a line item. This is not an IT problem. It is a business survival problem.

A Note on Scope

This is a guide to cybersecurity and information security governance. Fraud is a related but distinct discipline, with its own controls, its own regulatory framework, and often its own team. The two intersect constantly: a compromised credential, a convincing deepfake, or an unpatched system is frequently the on-ramp to a fraud loss. This guide addresses those cyber weaknesses and the points where they open the door to fraud, but it does not attempt to cover bookkeeping controls, positive-pay, or a formal fraud process as disciplines in their own right. Those are major domains that deserve their own dedicated treatment.

Cybersecurity now touches every dimension of how a business operates:

- **Customer trust.** A data breach or extended service disruption is a direct betrayal of the relationship customers place in you. Trust, once damaged, is hard to rebuild.
- **Operational resilience.** Cyber incidents are now among the most likely causes of extended service outages. Business continuity and cybersecurity are the same conversation.
- **Regulatory posture.** Cybersecurity is now a front-and-center concern for regulators, insurers, and the larger customers who vet their vendors. Depending on your industry you may face HIPAA, GLBA and the FTC Safeguards Rule, PCI DSS, or state privacy law, and nearly every business faces state breach-notification requirements. Material incidents increasingly must be reported, on tight timelines, to affected people and sometimes regulators.
- **Financial exposure.** Ransomware payments, recovery costs, regulatory fines, legal fees, and forensic investigations represent material financial risk. Cyber insurance coverage depends on having adequate controls in place.
- **Vendor risk.** Your risk does not stop at your front door. It extends through every third-party vendor, cloud provider, and software vendor with access to your systems or customer data.

The Leadership Role

Leadership's job is not to manage firewalls, select security tools, or interpret vulnerability scan results. Those responsibilities belong to management and technical staff. Leadership's job is to govern.

- Confirm that management has a funded, effective, and improving security program.
- Understand the business's material cyber risks in plain business terms.

- Ensure identified findings are tracked and resolved, not just reported.
- **Establish risk appetite and set the boundaries of acceptable risk.**
- Ask meaningful questions and expect straight, honest answers.
- Treat cyber risk with the same seriousness you already apply to cash flow, customer trust, and insurance.

Governance Principle

A leadership team that receives a clean audit report then moves on has not governed cybersecurity. Governance means ongoing oversight, informed funding decisions, and accountability for unresolved risks.

Does Your Leadership Need Cyber Fluency?

You do not need every leader to be technical, and you should be wary of any guide that tells you otherwise. But an ownership or leadership group with no one who can engage credibly with a security report is a leadership group that cannot tell the difference between reassurance and genuine progress.

You do not need to become technical. You do need one person who is not selling you the stack to tell you whether a security report is real progress or just reassurance. That can be you, once you have read this guide, a fractional advisor, or your counsel. Governing only through the provider who implements your controls is how programs look fine on paper and fail in the actual incident. If your business has a formal board, as many nonprofits and investor-backed companies do, that oversight belongs there too.

2. The Threat Landscape Facing Small Businesses

Small businesses are not too small to be targeted. They hold customer data, employee records, payment information, and access to money, which is exactly what attackers want. The following are some of the most significant categories of risk in the current environment.

Business Email Compromise (BEC)

BEC is one of the highest-dollar fraud categories facing businesses of any size. Attackers compromise or impersonate an executive's email account and use it to authorize fraudulent wire transfers, redirect payroll, or manipulate vendors into changing payment instructions.

These attacks frequently succeed not because of technical failures but because an employee followed an instruction without independent verification. No firewall stops a convincing email from a spoofed address. [8]

Ransomware

Ransomware attacks encrypt your systems and data, rendering them unusable until a ransom is paid or backups are restored. Modern ransomware operators also steal data before encrypting it, threatening to publish sensitive customer and employee information unless paid, a tactic called double extortion. Recovery, even with backups, can take days to weeks and is expensive. Ransomware attacks on critical vendors have cascaded into simultaneous service outages across dozens of businesses at once.

Phishing and Spear Phishing

Phishing delivers malicious links or attachments via email, tricking employees into surrendering credentials or installing malware. Spear phishing is the targeted version, crafted for a named individual using researched details about their role and relationships. Finance teams, HR staff, executives, and system administrators are common targets. A single successful phishing attack is frequently the entry point for a larger breach.

Credential Theft and Account Takeover

Stolen usernames and passwords are traded widely on criminal markets. When employees reuse passwords or fail to use multi-factor authentication, attackers can access systems without exploiting any technical vulnerability. They simply log in. Customer accounts face the same threat: attackers test stolen credential lists against login portals at scale, then drain accounts, make fraudulent purchases, or take over the account entirely.

Supply Chain Compromise

When a cloud provider, managed service provider, or software vendor is compromised, the impact extends to every business they serve. Businesses without visibility into vendor security posture often do not learn about a vendor compromise until the damage is already spreading through their own systems.

Insider Risk

Not all risk comes from outside. Employees with privileged access can intentionally or accidentally expose data, modify records, or facilitate fraud. The risk is elevated during transitions: departing employees, disgruntled staff, or contractors with excessive access. Insider risk requires access controls, separation of duties, monitoring, and a formal offboarding process that revokes access immediately upon departure.

Cloud Misconfiguration

As businesses move systems and data to cloud platforms, improperly configured storage, permissions, or access controls can expose customer data to anyone on the internet. Many significant data exposures have resulted from misconfigured cloud settings, not external attacks.

Cyber-Enabled Payment Fraud

Payments fraud is its own discipline, but much of it now arrives through a cyber door. ACH origination, wire transfers, card processing, and mobile payment platforms are all targeted for direct financial gain, and the entry point is frequently a compromised credential, a spoofed email, or a socially engineered customer service interaction rather than a flaw in the payment rail itself. This guide addresses that cyber on-ramp. The broader payments-fraud program, including transaction monitoring and recovery, sits alongside it as a distinct discipline.

Key Insight

Many successful breaches begin with a compromised credential, a clicked phishing link, or an exploited vendor rather than a technically sophisticated exploit. Human behavior and access management are where a large share of attacks start.

3. Artificial Intelligence and Emerging Threats

Artificial intelligence is transforming cybersecurity from both sides. Defenders use AI to detect threats faster and process security signals at scale. Attackers use AI to conduct more convincing, more targeted, and more scalable attacks. Business leaders need to understand three dimensions: the threats AI enables against your organization, how AI is reshaping fraud and account takeover, and how to govern the AI tools your own staff is already using.

AI-Enabled Threats Against Your Business

Deepfake voice and video. AI voice-cloning tools can replicate a person's voice from as little as a few seconds of recorded audio, often sourced from a voicemail, a public video, or a social media clip. Attackers use cloned voices to impersonate executives, owners, or customers themselves. Fraud scenarios now include a cloned "CFO" calling an employee to authorize an urgent wire transfer after hours, a "board chair" or investor calling the CEO during a sensitive decision window, and fake customer voices used to bypass telephone authentication at customer service lines. Deepfake video is advancing at similar speed and is already appearing in fraud attempts against businesses of every size.

Owner and Leadership Awareness

Your voice may be a target. Recordings from public presentations, recorded calls, or social media can be harvested to create convincing audio impersonations. Any owner or executive with a public profile should treat unusual verbal requests for action or money as suspect until independently verified.

AI-generated phishing at scale. Traditional phishing emails were often identifiable by poor grammar or awkward phrasing. AI-generated phishing can eliminate many of those signals, producing grammatically perfect, contextually aware messages that reference a recipient's actual job title, colleagues, recent work, or organization-specific terminology scraped from public sources. What once required a skilled operator hours to craft can now be produced in seconds across thousands of targets at once. The human filters trained on "bad grammar" and "suspicious links" are increasingly insufficient on their own.

AI-assisted attack tooling. Attackers are beginning to use AI to speed up parts of their work, from writing convincing lures to helping analyze targets. The practical takeaway for leaders is not a specific technique but a direction: the time between when a weakness becomes known and when it is used may continue to shrink, which raises the value of testing and patching on a disciplined cadence.

AI in Fraud and Account Takeover

Invoice and payment-change fraud. AI makes impersonation fraud far more convincing. Attackers use it to generate flawless invoices, spoof a supplier requesting a change to payment details, or impersonate an executive authorizing a payment. The classic small-

business version is the fake vendor-banking-change email: a message that looks exactly like your real supplier, asking you to update the account their payments go to. The money then flows to the attacker.

Cyber-enabled account takeover. Automated credential-stuffing and related techniques let attackers test large volumes of stolen credentials against login portals and work around some traditional controls. Where a compromised credential leads to a drained account or a fraudulent payment, a cyber weakness has become a fraud loss. The defense is the same one that matters everywhere else in this guide: strong identity controls, MFA, and monitoring.

Social engineering of customer service staff. Customer service employees field calls daily requesting account changes, password resets, and transfers. AI voice impersonation means the caller may not be who they claim to be, even if they sound exactly right. Staff must be trained on verification procedures that do not rely on voice recognition or caller familiarity alone. Secure callbacks to registered numbers, step-up authentication, and other independently verified controls are stronger than knowledge-based questions alone.

Governing Your Own AI Tool Usage

Many employees are already using AI tools in their daily work, whether formally sanctioned or not. Staff use consumer AI assistants to draft customer communications, summarize documents, analyze spreadsheets, and answer operational questions. The governance question is not whether AI is being used. It is whether its use is visible, controlled, and consistent with customer privacy obligations.

Shadow AI and data exposure. When employees enter customer data, internal policies, account details, or financial records into public AI tools, that information may be used to train external models, retained by the provider, or exposed in ways that violate customer privacy, regulatory requirements, or contractual obligations. This risk is largely invisible without a policy framework defining what may and may not be used with AI systems.

A governance framework for AI tool usage should address:

- Which AI tools are approved for use, and by which roles.
- What categories of sensitive data may be used only in specifically approved AI environments, and what data or uses are prohibited entirely.

- How AI-generated content is reviewed before use in customer-facing work, or anything that affects a person.
- How AI vendors are subject to third-party risk review, the same as any other technology vendor.
- Who maintains the approved tool list and reviews new tools before use.
- How employees report accidental disclosure of restricted data through AI tools.

Regulatory expectations for AI. There is no separate AI rulebook for small business. The rules you already live under still apply: privacy, consumer protection, employment and hiring law, and your contracts with larger customers. The exposure is concrete. If your staff paste customer data into a public AI tool, you may have just handed that data to a third party in violation of your obligations. If AI influences a hiring, pricing, or customer decision you cannot explain, you do not have a defensible position. The whole program at this size is three things: a short policy, a list of approved tools, and a human who owns the output.

Leadership Question

Ask your technology and compliance teams: What AI tools are employees using today? What customer data may have passed through those systems? Do we have a policy that governs this, and have employees been trained on it?

4. The Security Landscape in Plain English

A mature security program covers many domains. Leaders do not need to understand how each technology works. They need to understand what each domain protects and what questions to ask about it.

Identity and Access	Controls who can log in to what, with what permissions. Weak identity controls are involved in a large share of breaches. The most important domain.
Endpoint Security	Protection on laptops, desktops, servers, and mobile devices. Unmanaged or unprotected devices are a primary attack surface.

Email Security	Filtering of malicious messages before they reach employees. Phishing remains one of the most common attack delivery methods.
Network Security	Firewalls, segmentation, and traffic monitoring. Limits how far an attacker can move once inside.
Cloud Security	Securing data and systems hosted in cloud platforms. Configuration errors are a leading cause of cloud incidents.
Data Protection	Encryption, classification, and access controls on sensitive data. Protects customer information at rest and in transit.
Application Security	Security in the software and web applications the business runs. Poorly secured apps are common targets.
Backup and Recovery	The ability to restore systems and data after an incident. Backups are only valuable if tested and confirmed to work.
Vendor Security	Oversight of third-party security posture. Your risk extends to every vendor with access to your systems or data.
Monitoring and Detection	The capability to detect threats in near-real time. Undetected threats cause far more damage over time.
Incident Response	A defined process for identifying, containing, investigating, and recovering from an incident.
Governance and Policy	The policies, training, risk management, and accountability that tie all other domains together.

5. Identity Is the Control Plane

Many leaders still think of the firewall as the center of security. In modern environments, identity is often where the fight starts and ends.

When an attacker steals valid credentials and uses them to log in, there is no attack for a firewall to block. The attacker looks exactly like a legitimate user. Defense shifts to strong identity controls, behavioral monitoring, and meaningful access limitations.

Multi-Factor Authentication (MFA)

Multi-factor authentication requires something you know (a password) plus something you have (a phone or hardware token) or something you are (a biometric). Even if an attacker has a stolen password, MFA makes that password alone insufficient in most cases. For a business, MFA should be required for all administrative and privileged accounts, all remote access, email and collaboration platforms, core business systems and financial systems, any system containing customer data, and vendor and third-party access accounts.

Leadership Question

What percentage of accounts require MFA today, especially privileged accounts and remote access? What is the target coverage and the timeline to reach it?

Privileged Access Management

Privileged accounts, those with administrative rights or the ability to modify security configurations, are the highest-value targets for attackers. A compromised admin account can disable security controls, delete backups, and move freely across the network. Leaders should confirm that privileged accounts are inventoried and reviewed on a schedule, that administrative access uses separate accounts from day-to-day use, that access is granted on a least-privilege basis, that privileged sessions are logged, and that access is revoked immediately when employees change roles or leave.

Password Management and Account Lifecycle

Password reuse is one of the most exploitable behaviors in any organization. When employees use the same password across work and personal accounts, a breach of any one becomes a credential the attacker can test against all the others. Password managers and long, unique passwords meaningfully reduce this risk. Equally important is lifecycle management: without a formal offboarding process, former employees retain access long after they leave. Regular access reviews should verify that every account is tied to an active, authorized person with a current business need.

6. Data Protection and Customer Trust

Customer data is the most sensitive asset a business holds. Social Security numbers, account numbers, payment details, employee records, and personal information are exactly what identity thieves and fraudsters want. Leaders need to understand where that data lives, who can access it, how it is protected, and what happens if it is exposed.

Where Customer Data Lives

Customer data rarely lives in one place. It may reside in your core business system, your accounting or payment platform, email archives, document management systems, scanned records, cloud storage, backups, and on employee devices. Vendors you share data with may hold copies you no longer track. A meaningful data inventory answers: What sensitive data do we have? Where does it live? Who has access? How long do we retain it? How is it destroyed when no longer needed?

Encryption, Retention, and Destruction

Encryption converts data into an unreadable format without the appropriate key, and should apply both at rest and in transit across databases, file shares, email, mobile devices, and backups. Equally important, data you no longer need is still a liability: retaining data beyond its required period increases the scope of any breach without providing value. A formal retention schedule defines how long each record type is kept and how it is securely destroyed, including paper records, hard drives, archived backups, and decommissioned systems.

Regulatory Requirements and Customer Notification

Businesses are subject to overlapping data protection requirements, and for most small businesses the practical picture is simpler than it sounds. Two things now govern almost everyone. First, state data breach notification laws: nearly every state requires you to notify affected people, and sometimes regulators, when personal data is exposed, with specific timelines. [4] Second, cyber insurance, which has become the de facto regulator of small business security. Insurers increasingly require multi-factor authentication, backups, endpoint protection, and employee training as conditions of coverage or of paying a claim. On top of that universal baseline, regulated industries carry added obligations: HIPAA for anyone handling health information, the Gramm-Leach-Bliley Act and the FTC Safeguards Rule for financial services and many firms that handle consumer financial data [3], PCI DSS for anyone accepting

card payments, and state or professional rules for fields like legal and accounting. Know which of these apply to you, because a single documented information security program can satisfy most of them at once. [5]

Data Governance Question

Do we have a current data inventory? Do we know where customer PII lives across all systems and vendors? When did we last review our retention practices and confirm that data destruction is actually occurring on schedule?

7. Vendor and Third-Party Risk

No business is an island. Beyond your MSP, covered on its own earlier in this guide, you rely on cloud providers, software vendors, payment processors, and your accounting and payroll platforms. Each has access to your systems, your data, or both, and each is a door. When any of them has a security incident, you may have one too, whether or not anyone attacked you directly. This section is about governing that wider set of vendors.

Why Vendor Risk Is the Central Story

This is not a peripheral concern; it is a large and growing source of real incidents. Industry reporting consistently finds that a large share of breaches trace back to a third party rather than to the business itself, and the pattern is the same everywhere: an attacker compromises a vendor, a managed service provider, or a piece of shared software, and every customer of that vendor is exposed at once. [1] The concentration risk is real and concrete: when a single provider that serves thousands of small businesses is breached, thousands are breached with it. You inherit the security of every vendor you rely on.

There is a hard truth small-business owners should sit with plainly. No regulator is checking your vendors for you. A large bank has examiners who scrutinize its critical technology providers; a five-to-fifty-person business has no one performing that oversight on its behalf. Your cloud provider, your payment processor, and your software vendors are all doors into your business, and verifying their security is entirely your responsibility. In practical terms: vendor oversight is not optional or someone else's job. It is yours, and it is one of the highest-value things you can do to reduce real risk.

Your Notification Clock Can Start at Your Vendor

You likely have notification obligations of your own, and they can start with a vendor's breach. State breach-notification laws, your cyber insurance policy, and your contracts with larger customers can all require you to report an incident within a defined window, often as little as 72 hours, once you know or reasonably should know it occurred. A vendor that sits on bad news for a week can quietly put you behind your own deadline. That is why your contracts with critical vendors should obligate them to notify you promptly of any security incident: their delay becomes your liability. Notification timelines in vendor contracts are not a nicety; they are a control.

Components of a Mature Vendor Risk Program

- **Vendor inventory.** A current list of all vendors with system or data access, classified by criticality. An inventory you cannot maintain is not a real inventory.
- **Due diligence.** Security assessments before onboarding, including review of SOC 2 reports, penetration test results, security questionnaires, and insurance coverage.
- **Contractual controls.** Security requirements, incident notification timelines, audit rights, and breach response obligations must be present in contracts, not assumed.
- **Ongoing monitoring.** Periodic reviews at intervals appropriate to vendor risk, not just at contract renewal. A high-risk vendor reviewed only every three years is not meaningfully monitored.
- **Concentration risk. When multiple critical functions depend on a single vendor or technology stack, that concentration warrants additional oversight and contingency planning. This is acute for small businesses, where one MSP, one cloud platform, or one payment processor often carries several critical functions at once.**

Vendor Risk Reality

An attacker who compromises your payroll platform, your accounting software, or a payment processor can reach your data and your money without ever attacking you directly. Because no regulator examines your providers for you, responsibility for effective due diligence and ongoing oversight remains with the business. Vendor oversight is not optional. It is a fundamental component of your security program.

8. Resilience, Backups, and Continuity

Resilience is the ability to withstand disruption and recover with acceptable speed. In a cybersecurity context, it means being able to detect an incident, contain the damage, restore systems and data, and resume customer service within a timeframe that customers and regulators can accept. A common failure mode is not the absence of backups. It is the presence of backups that have never been tested and fail when they are needed most.

Backup Fundamentals

- **Recovery Point Objective (RPO).** How much data can the business afford to lose? If the last backup ran 24 hours ago, a ransomware attack today means 24 hours of transactions are potentially gone. Backup frequency should be designed to meet a defined RPO.
- **Recovery Time Objective (RTO).** How long can operations be disrupted before the impact becomes unacceptable to customers and regulators? The RTO drives investment in redundancy, failover, and recovery infrastructure.
- **Offline and immutable backups.** Backups stored only on the same network as primary systems can be encrypted or deleted by ransomware. Critical backup strategies should include offline, segregated, or immutable copies that an attacker with ordinary production access cannot modify or delete.
- **Backup testing.** A backup that has never been tested has not been proven to work. Restoration tests must run on a regular schedule, cover all critical systems, and be reported to leadership. A failed restoration test for a critical system should be treated as a critical finding.

Business Continuity and Incident Decision-Making

Business continuity planning defines how the business operates when primary systems are unavailable: which customer-facing services must be maintained and at what minimum level, manual procedures for serving customers, taking payment, and continuing critical work when systems are down, communication protocols for customers and regulators, and clear decision authority. When an incident occurs, decisions must be made quickly and with incomplete information. Who has authority to disconnect systems? Who authorizes a forensic firm? Who notifies affected customers, regulators, and your insurer? Who communicates to customers? These questions must be answered before an incident, not during one. Incident response plans

should be reviewed annually, and contact information and escalation paths verified whenever they change.

The Ransom Payment Decision

One incident decision deserves its own attention because it carries legal exposure leadership must understand in advance: whether to pay a ransom. This is not simply a financial or operational choice. Paying certain sanctioned threat actors can itself be a violation of federal law, and regulators have made clear that a payment made without appropriate diligence can create liability on top of the incident. [7] The decision should never be made in the heat of an attack by whoever happens to be available. No ransom decision should be made without legal counsel and sanctions screening; both are non-negotiable before any payment, not optional steps.

Before an incident, leadership should confirm who holds authority to authorize or refuse a payment, that legal counsel and sanctions screening are part of any payment decision, and that procedures exist for appropriate engagement with law enforcement.

Leadership Question

When were our backups last tested? Were all critical systems included? What were the results? How long would it actually take to restore full operations after a ransomware event, and who has authority over the decisions we would face in the first 24 hours?

9. The Risk Management Process

Cybersecurity risk does not manage itself, but a small business does not need a corporate risk department to handle it. Read the next three sections for the logic, then right-size them: if you have an MSP and fewer than fifty people, the Minimum Viable Program earlier in this guide is your version of all of it. The formal process below is what you grow into, not what you start with. It must still be identified, evaluated, prioritized, and actively managed, just at a scale that fits your business. [6]

Step 1: Define Risk Appetite

Risk appetite is the amount and type of risk leadership is willing to accept in pursuit of the business's mission. It is a governance decision made by ownership and senior leadership, not a

technical determination made by IT. For cybersecurity, risk appetite statements set the boundaries within which management operates, for example: the business will not accept unencrypted customer PII on any production system; will not operate core business systems without tested, offline backups meeting a defined RTO; and will not onboard a vendor with privileged access that has not completed a security review within the past 12 months. Without a stated appetite, there is no consistent basis for prioritizing investment or knowing what requires escalation to ownership. It should be reviewed and formally approved at least annually.

Governance Connection

Risk appetite translates leadership's values into operational guidance. When management accepts a risk or defers a control, that decision should trace back to a documented risk appetite position, not informal judgment.

Step 2: Identify Critical Systems and Assets

Not all systems are equal. Before risk can be meaningfully assessed, the business must identify what matters most: the systems, data, and processes whose failure or compromise would cause the greatest harm. Core business systems, payment and financial systems, customer data repositories, identity and authentication systems, network infrastructure, backup systems, and critical vendor connections form the backbone of that inventory. It is the foundation for everything that follows, and risk assessments, continuity plans, and security investment should all flow from a clear understanding of what the business cannot afford to lose.

Step 3: Assess the Risks

Risk assessment evaluates the likelihood and potential impact of threats against each critical asset, producing a prioritized view of where the greatest risk exists. A meaningful assessment considers the threat sources that could cause harm, the vulnerabilities they could exploit, the likelihood of the threat being realized given current controls, and the operational, financial, regulatory, and customer-trust impact if it were. Risk assessments should be kept current, revisited as part of the annual information-security program review, and updated after significant changes: new systems, new critical vendors, major technology transitions, or material incidents.

Step 4: Maintain a Risk Register

A risk register is a living document recording identified risks, their current ratings, assigned ownership, planned treatments, and resolution status. It is the operational artifact that connects assessment findings to active management. Each entry should capture a plain-language description, a likelihood and impact rating, a named risk owner, a treatment plan, a current status with target dates, and the residual risk remaining after controls are applied.

Governance Use

The risk register is one of the most important documents leadership should review regularly. It shows not just what risks exist, but whether management is actively addressing them, who owns them, and whether residual risk is within the leadership-approved appetite.

Step 5: Treat the Risks

For each risk, management selects a treatment. Mitigate: implement controls that reduce likelihood or impact, the path for most high-priority cyber risks. Transfer: shift financial impact through insurance or contract, though cyber insurance requires specific controls and does not cover all losses. Accept: formally decide not to invest further, typically when mitigation cost exceeds expected loss, with the acceptance documented, owned, and revisited. Avoid: eliminate the activity or asset creating the risk entirely.

Step 6: Monitor and Report to Leadership

Risk management is not an annual event. Threats emerge, vendors change, systems are added and retired, and staff turn over. Leadership should receive a regular cyber risk update covering the status of the highest-rated risks, any new risks identified, progress on active mitigation with items at risk of missing targets, a summary of incidents and near-misses, and any risks where the leadership-approved acceptance posture should be reconsidered.

Risk Appetite vs. Risk Reality

One of the most important governance questions is whether current residual risks are within the leadership-approved appetite. If open risks exceed the stated appetite, that gap should trigger escalation for additional mitigation, funding, or formal acceptance at the level authorized by the business's governance framework.

10. Testing, Audits, and Assessments

Businesses are subject to a range of security reviews. Understanding what each one is, and what it is not, prevents leaders from mistaking compliance activity for security assurance.

IT Controls Audit	Evaluates controls against a defined scope and set of criteria. May include testing of technical controls, but it is not adversarial testing against a live attacker.
Risk Assessment	Identifies and prioritizes major cyber risks by likelihood and impact. The output is a prioritization, not a certification.
Vulnerability Scan	An automated check for known technical weaknesses: missing patches, misconfigurations, known flaws. Produces a list of potential issues; does not validate or exploit them.
Vulnerability Assessment	Takes scan output further with human validation, context, and prioritization by severity and business impact. Separates real risk from scanner noise. Still stops short of exploitation.
Penetration Test	Simulates a real attacker attempting to breach systems. Demonstrates what an attack could achieve, within a defined scope and timeframe.
Social Engineering Test	Tests human susceptibility to phishing, pretexting, and vishing. Reveals training and process gaps.
Architecture Review	Evaluates whether the overall system design creates unnecessary risk. Particularly useful before major changes.
Configuration Review	Checks whether systems are configured against a prescriptive security benchmark such as the CIS Benchmarks. Distinct from a vulnerability scan and more rigorous.

Tabletop Exercise	A discussion-based simulation of an incident. Tests whether decision-making, communication, and escalation work in practice.
Compliance Examination	A regulator, auditor, or insurer review of minimum standards. Meeting those standards is a floor, not a ceiling.

Critical Limits Every Leader Should Understand

- **A clean audit does not prove security.** An audit evaluates controls against a defined scope and criteria. Even a thorough one is not the same as adversarial testing: passing it means you met the criteria examined, not that your defenses would hold against a determined attacker probing for the gaps the audit did not look at.
- **A vulnerability scan is not a penetration test.** A scan identifies known vulnerabilities. A penetration test actively attempts to exploit them. Very different levels of assurance.
- **A penetration test does not equal a mature program.** Surviving a scoped simulation means you passed that simulation, not that the broader environment is secure.
- **A tabletop exercise does not prove recovery readiness.** Unless the action items it surfaces are completed and validated, it identifies gaps without closing them.
- **Meeting a compliance or insurance standard is the minimum, not the goal. Compliance confirms baseline adequacy. A business with a clean audit or insurance review can still be successfully breached.**

Testing Principle

Testing is only valuable if findings are acted on. Ask how many findings from the most recent penetration test or risk assessment remain unresolved, and why. The age of open findings is often more telling than the findings themselves.

11. The Numbers Worth Watching

Security metrics for leadership should be meaningful, actionable, and honest. At your size, five numbers are enough, and three of them are proof your MSP should already be showing you every quarter. If every metric trends green every quarter, ask what is being measured.

MFA Coverage (%)	What percentage of accounts require multi-factor authentication, especially privileged accounts? One of the highest-impact controls against credential-based attacks.
Privileged Account Review	When were privileged accounts last inventoried and reviewed? Are all tied to current, authorized individuals?
Critical Patch Compliance (%)	What percentage of systems have critical patches applied within the required window? Unpatched flaws are among the most exploited vectors.
Open High-Risk Findings	How many findings from recent assessments remain unresolved, and how long have they been open? Age matters as much as count.
Backup Test Results	When were backups last tested across all critical systems? What were the results? Any failures?
Reporting Integrity Honest security reporting shows a mix of progress and problems. A set of numbers with nothing in the red or yellow columns every quarter is a signal that the reporting framework needs to be challenged, not that the business has no security challenges.	

12. Questions Leadership Should Ask Quarterly

These questions create a repeatable governance cadence. They do not require technical expertise to ask, but the answers reveal whether the security program is functioning, improving, and honestly reported. Ask them consistently, and expect the answers to change.

- What are our top cyber risks right now, and what is the status of efforts to address them?
- What changed in our environment this quarter? New systems, new vendors, significant configuration changes, or staff changes in security-sensitive roles?
- Where are we taking risk on purpose this quarter, such as a system without MFA, a vendor with admin access, or an untested backup, and is that still acceptable to you?

- What findings from our last assessment, audit, or penetration test remain unresolved? What is preventing resolution?
- When were our backups last tested? Were all critical systems included? What were the results?
- What is the status of our critical vendor reviews? Are any high-risk vendors overdue?
- Are privileged accounts controlled? When were they last reviewed and reduced to the minimum necessary access?
- What would cause the greatest harm to customers if it failed or was compromised today?
- What does our MSP need from us, a decision, a spend, or access removed, that is currently stuck on our side?
- Have we had any security incidents, near-misses, or threat intelligence updates leadership should understand?
- What AI tools are employees using, and are customer data or sensitive records being handled appropriately within them?

Asking Better Questions

Security briefings that consist entirely of status updates create a false sense of progress. Owners who ask what is not going well, what is overdue, and what management is worried about get more honest and more useful reporting.

13. The First 90 Days: A Leader Checklist

For new owners, executives, or leaders, and as an annual baseline review for all leaders, the following confirms that foundational oversight is in place and the business's security program is visible at the governance level.

Risk and Assessments

- Confirm a current risk assessment exists. Review the top findings and their status.
- Review all open findings from recent audits, assessments, and penetration tests, and how long each has been open.
- Review the open-findings list. Confirm every item has an owner and a target date.

Identity and Access

- Validate that MFA is enabled for all administrative, remote access, and cloud platform accounts.
- Confirm privileged accounts have been reviewed within the past 90 days.
- Ask when the last access review was conducted, particularly for staff who changed roles or departed.
- Confirm a formal onboarding and offboarding process exists for system access.

Resilience and Backups

- Confirm backups exist for all critical systems and are stored offline or in immutable storage.
- Ask when backups were last tested, what was included, and what the results showed.
- Review the business continuity and incident response plans. Confirm they are current, tested, and understood.
- Confirm you know your breach-notification obligations under state law, your insurance policy, and your key contracts, and who is responsible for meeting them.

Vendors

- Review the vendor inventory. Confirm it is current and covers all vendors with system or data access.
- Identify any critical vendors overdue for a security review and ask why.
- Confirm contracts with critical vendors include security requirements, breach notification timelines that let you meet your own reporting obligations, and audit rights.
- Ask whether any critical service relies on a single vendor without a documented contingency.

Governance and Insurance

- Confirm leadership receives a meaningful cyber risk report at least quarterly.
- Review cyber insurance coverage. Confirm limits, exclusions, and required controls are understood and met.
- Schedule a tabletop exercise within 90 days if one has not occurred in the past 12 months.
- Confirm legal counsel is identified for cyber incident response before an incident occurs, and that the ransom-payment decision authority is defined.

AI and Emerging Technology

- Ask whether a formal AI usage policy exists and whether employees have been trained on it.
- Confirm vendor-provided AI tools have been reviewed under the third-party risk program.
- Ensure owner and leadership awareness of deepfake voice and video risks, and that verification procedures exist for unusual financial requests.

14. Your People Are Under Attack Too

See also: *Personal Cybersecurity for Business Leaders*, the dedicated guide in this series at jeremywalker.us/resources, covers this in depth and is built to share with staff, boards, and families.

Attackers do not only target systems. They target employees, owners, executives, key staff, and their families. A compromised personal email account can be used to launch attacks against the business. An owner or executive who falls for a deepfake voice scam can inadvertently authorize a fraudulent transaction. Personal security is now part of organizational resilience. The following is recommended for every owner, executive, and their household.

Protect Your Identity

- Freeze your credit with all three major bureaus (Equifax, Experian, TransUnion) and with ChexSystems. A freeze is free, can be temporarily lifted, and prevents new accounts from being opened in your name.
- Monitor your credit reports through AnnualCreditReport.com for accounts or inquiries you do not recognize.
- Set fraud and transaction alerts on all personal bank, investment, and credit card accounts.

Secure Your Accounts and Devices

- Enable MFA on every personal account, including ones that seem low value; attackers use them to pivot to higher-value targets.
- Use a password manager for strong, unique passwords, and never reuse them across work and personal use.
- Secure your personal email first. It is the master key to resetting almost every other account.

- Keep devices patched and enable full-disk encryption and remote wipe. For sensitive work away from home, prefer your own cellular connection or personal hotspot over unfamiliar Wi-Fi. A patched device using encrypted connections is what actually keeps you safe on an untrusted network; use a VPN where your organization requires one, but do not treat it as a substitute for the basics.

Guard Against SIM Swapping

SIM swapping is a fraud technique where an attacker convinces your mobile carrier to transfer your phone number to a SIM they control, giving them your text-based authentication codes. Add a port-out PIN or account passcode with your carrier, be alert to unexpected loss of cell service, and move critical two-factor authentication off SMS onto an authenticator app or hardware token where possible.

Be Skeptical of Unusual Requests

- Verify any unusual financial or authorization request through a separate, independently confirmed channel. Do not use the phone number or email the request came from.
- Remember that voice can be convincingly cloned from a small amount of audio. Urgent calls from executives or owners requesting money or sensitive information should always be verified through a second channel.
- Talk to family about scams, particularly voice impersonation and scams that target older relatives.

Reduce Your Digital Footprint

- Review your public social media presence. Details about your role, relationships, travel, and routines fuel targeted social engineering.
- Be aware that people-search sites and data brokers aggregate significant personal information; opt-out services can reduce this over time.
- Consider what is publicly visible on LinkedIn, association websites, and company materials. Attackers research targets before they make contact.

Leadership Reality

Owners and executives are high-value targets. Personal digital hygiene is also organizational security. The time you invest in protecting yourself is time invested in protecting the business and the people who run it.

Closing: Security Is an Operating Discipline

Cybersecurity is not a product you purchase, a project you complete, or an audit you pass once a year. It is an operating discipline, practiced continuously, improved over time, and governed with the same seriousness you already apply to cash, insurance, and customer trust.

The businesses that weather incidents best are not the ones with the most sophisticated tools or the largest IT departments. They are the ones with clear governance, honest reporting, tested plans, documented risk appetite, accountable ownership, and leadership that takes the subject seriously before something goes wrong.

Strong cybersecurity governance does not require every leader to become a technical expert. It requires asking the right questions, demanding honest answers, ensuring findings get resolved, requiring that risk is owned and tracked, and treating security investment as the operational necessity it has become.

The threat environment will keep evolving. AI-enabled attacks, more sophisticated fraud, and vendor compromise events will continue to affect businesses of every size. A business's response is not to chase every trend or acquire every tool. It is to build the governance structures, recovery capabilities, and repeatable habits that make the organization resilient to whatever comes next.

A closing reminder on scope: the ground this guide covers is cybersecurity and information security governance. Payments fraud, chargebacks, and stolen wires are their own disciplines, closely connected to what is here but broader than it. Strong cyber governance closes many of the doors that fraud walks through, but it does not replace a dedicated fraud program. Treat them as partners, not substitutes.

Your customers trust you with their data and their business. Security is how you protect that trust.

Sources and References

The facts and statistics in this guide are drawn from public, reputable sources. Requirements evolve and vary by state and industry, so confirm current obligations with your own counsel, your insurer, or the relevant regulator before relying on any specific point for a compliance decision.

[1] Verizon Data Breach Investigations Report (annual). Widely cited industry analysis consistently finding that a large share of breaches involve small businesses and third-party or supply-chain factors.

[2] Cybersecurity and Infrastructure Security Agency (CISA), Cybersecurity resources for small and medium businesses (cisa.gov). Practical, free guidance on baseline protections.

[3] Federal Trade Commission, Cybersecurity for Small Business and the FTC Safeguards Rule (ftc.gov). Guidance on protecting customer data and the security-program requirements for covered financial businesses.

[4] State data breach notification laws (all 50 states). Each state sets its own definition of covered data and notification timeline; consult counsel for the states where your customers reside.

[5] Applicable sector regulations, including the HIPAA Security Rule (health), the Gramm-Leach-Bliley Act and FTC Safeguards Rule (financial), and PCI DSS (card payments). Confirm which apply to your business with counsel.

[6] NIST Cybersecurity Framework 2.0 and NIST AI Risk Management Framework (nist.gov). Voluntary, widely recognized frameworks for organizing security and AI risk management at any size.

[7] U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. Warns that making or facilitating ransom payments to sanctioned actors can carry federal sanctions exposure.

[8] FBI Internet Crime Complaint Center (IC3), annual Internet Crime Report (ic3.gov). Documents business email compromise and payment-fraud losses across businesses of all sizes, and has warned of AI-enabled and deepfake-assisted fraud.

About the Author

J.W. Walker has spent his career in information security across commercial and government environments. He has sat in the tester's chair, built a company from the ground up through exit, and serves as CTO of an information security firm. Today he advises owners and leaders on security strategy, governance, and the decisions that decide whether a program actually works. He writes plain-language guides that help owners and leaders make confident decisions about security and risk without needing to become technical experts.

For more from the author, visit jeremywalker.us/resources. For an independent read on your program, start at jeremywalker.us/cyber-advisory.

About This Guide and Its Partners

This guide is a collaboration between J.W. Walker and Ideal Technologys, written to give small-business owners a clear, honest picture of cybersecurity without the jargon or the sales pressure.



J.W. Walker writes plain-language guides for business leaders at jeremywalker.us/resources. Ideal Technologys provides managed IT, cybersecurity, cloud, and backup services to businesses across Tampa Bay and beyond. Contact them at idealtechnologys.net. Because Ideal sells those services, the questions in this guide about your provider are written to work on them, too.

Full disclosure from J.W.: I back people I trust, and only people I trust. I receive a referral fee from Ideal Technologys. Nothing up front. I'm paid each month you stay with them, and not a dollar after you leave. If you work with them through me, I will be your advocate for the life of the relationship. If they ever stop deserving your business, I'll tell you to leave and lose the fee. That's the deal.

Last reviewed: October 2026. Regulatory positions and standards evolve; confirm specific requirements with counsel or your regulator before relying on them.