IronRoot
Risk Consultants

Top 10 Security Risks
Small Businesses Ignore (And Pay For)

A plain-English guide to the security and compliance gaps that catch small businesses off guard -- and what you can do about each one.

1

No Multi-Factor Authentication on Email

THE RISK

Business email is the #1 target for attackers. Without MFA, a stolen or guessed password gives an attacker full access to your inbox, contacts, cloud files, and a master key to every other account that uses that email for password resets.

REAL-WORLD EXAMPLE

A 12-person accounting firm lost access to their entire Microsoft 365 environment after an employee's password was phished. The attacker forwarded all incoming email to an external address for six weeks — accessing client financial data the entire time.

WHAT TO DO

Enable MFA on every email account and cloud service today. Use an authenticator app (not just SMS). Takes under 30 minutes in Microsoft 365 or Google Workspace. This is the single highest-ROI security action available.

*** CRITICAL**

2

Backups That Have Never Been Tested

THE RISK

Having a backup is not the same as having recovery. Most small businesses discover their backups are incomplete, corrupted, or misconfigured only when they desperately need them — after ransomware, hardware failure, or accidental deletion.

REAL-WORLD EXAMPLE

A dental practice paid $35,000 to a ransomware group because their cloud backup had been failing silently for four months. Their IT provider had set it up correctly at first, but a software update broke the backup job and no one noticed.

WHAT TO DO

Test your backups now. Pick 3 random files and restore them. Schedule a full restore test annually. Backups should be: automated, off-site or cloud, encrypted, and include all critical data including email.

*** CRITICAL**

3

Former Employee Accounts Left Active

THE RISK

When someone leaves — voluntarily or not — their login credentials don't automatically disappear. Without a formal offboarding process, ex-employees can retain access to email, CRM, project tools, file storage, and financial systems for months or years.

REAL-WORLD EXAMPLE

A marketing agency discovered that a former account manager terminated 14 months earlier still had active access to their HubSpot and Google Drive. He had downloaded the client list and taken it to a competing firm.

WHAT TO DO

Build an offboarding checklist tied to HR. On the last day: disable email, revoke cloud access, change shared passwords. Quarterly: run an access review for all active accounts and verify each maps to a current employee.

* HIGH

4

No Written Incident Response Plan

THE RISK

When a breach or ransomware attack happens — and for most businesses it's when, not if — you'll have minutes to hours to respond correctly. Every delay costs money. Without a plan, you're improvising in a crisis.

REAL-WORLD EXAMPLE

A law firm that suffered ransomware wasted 48 hours trying to reach their IT vendor, unsure who was responsible for the decision to restore vs. pay. By the time they engaged incident response professionals, the attacker had already exfiltrated several years of case files.

WHAT TO DO

Write a one-page plan: who do you call first (IT, legal, cyber insurance, law enforcement)? What do you isolate and how? Where are your backups? Run a tabletop exercise with your team once a year. Keep a printed copy off-site.

* HIGH

5

Employees Using Personal Email for Business

THE RISK

When employees use Gmail, Yahoo, or personal accounts for client communications or sensitive data — even occasionally — that data falls outside your security controls, retention policy, legal hold capability, and compliance obligations.

REAL-WORLD EXAMPLE

A financial advisor used his personal Gmail to send a client's tax documents 'just this once.' Two years later, during a regulatory audit, he couldn't produce that record. The fine for the missing client communication exceeded $15,000.

WHAT TO DO

Publish a clear policy: no client data or business communications via personal accounts. Make your business email easy enough to use that there's no reason not to. Consider MDM for company phones to enforce this on mobile.

*** MEDIUM**

6

Vendors with Access and No Security Review

THE RISK

Most small businesses have 10-30 vendors with some form of access to their systems or data — IT support, payroll, CRM, cloud storage. Each vendor is a potential entry point. Vendors get breached too — and their breach becomes your breach.

REAL-WORLD EXAMPLE

The 2013 Target breach started with an HVAC vendor's compromised credentials. The same pattern plays out for small businesses every week: a shared IT support login, an unsecured API key, a payroll vendor's compromised database.

WHAT TO DO

List all vendors with access to your data or systems. For each: (1) confirm they use MFA, (2) limit access to only what they need, (3) ensure your contract requires breach notification. Ask critical vendors for their SOC 2 report.

*** HIGH**

7

Unpatched Software and Devices

THE RISK

Every unpatched vulnerability is an open window. Attackers actively scan for systems running known-vulnerable software. Many devastating ransomware attacks exploited vulnerabilities that had been patched months before — the victims just hadn't updated.

REAL-WORLD EXAMPLE

A healthcare clinic's Windows 7 workstation — used only to run a specialty medical device — was compromised through a known vulnerability. Because it shared a network with their main systems, the attacker pivoted to the EHR and encrypted patient records.

WHAT TO DO

Enable automatic updates for all operating systems and major applications. Build a quarterly review of anything that cannot auto-update (medical devices, legacy systems). Replace or isolate systems that no longer receive security patches.

*** HIGH**

8

No Cybersecurity Awareness Training

THE RISK

Your employees are your biggest attack surface — not because they're careless, but because attackers specifically target them. Phishing, business email compromise, and social engineering attacks are constantly evolving. One click can give an attacker a foothold in your network.

REAL-WORLD EXAMPLE

An accounting firm's bookkeeper received a convincing email appearing to come from the owner, requesting an urgent wire transfer for a client matter. Without training to spot the red flags, she processed $47,000 to a fraudulent account.

WHAT TO DO

Provide security awareness training at onboarding and at least annually. Run quarterly phishing simulations. Train specifically on wire fraud and business email compromise, not just malware.

*** HIGH**

9

Data You Didn't Know You Were Responsible For

THE RISK

Many small businesses handle regulated data without realizing it: health information (HIPAA), payment card data (PCI DSS), financial records (GLBA), or children's data (COPPA). Ignorance is not a defense. Regulators don't credit businesses for not knowing the rules applied to them.

REAL-WORLD EXAMPLE

A yoga studio that stored client credit card numbers in a spreadsheet — because the owner didn't realize they were subject to PCI DSS — faced a $25,000 fine and mandatory forensic audit after a breach.

WHAT TO DO

Take 30 minutes to map what data you collect: Do you hold health info? Card numbers? Data about children? Financial records? If yes — research the applicable regulation and seek advice. Two hours of consulting is a fraction of the cost of non-compliance.

*** MEDIUM**

10

No Cyber Liability Insurance — Or the Wrong Kind

THE RISK

A standard general liability or BOP policy typically does NOT cover cyber incidents. Many business owners assume they are covered until the moment they need to file a claim. Cyber incidents — even small ones — can cost tens of thousands in incident response, legal fees, and notification costs.

REAL-WORLD EXAMPLE

A professional services firm spent $68,000 on forensic investigation, legal counsel, client notification letters, and credit monitoring after a modest breach. Their insurer denied the claim because the incident fell under their data breach exclusion.

WHAT TO DO

Review your current insurance policies — specifically ask your broker: does this cover cyber incidents, ransomware, and data breach notification costs? If not, get a standalone cyber liability policy. Premiums typically run $1,500-$5,000/year for small businesses.

*** MEDIUM**

Know Your Gaps -- Before an Attacker Does.

IronRoot Risk Consultants helps small businesses build practical, affordable security and compliance programs.

chris@ironrootrisk.com | ironrootrisk.com