Small Business Cybersecurity Self-Assessment Checklist

25 yes/no checks to find the gaps before an attacker does

Sino Technology Solutions | info@sinotechsol.com | sinotechsol.com

---

Why I put this together

A breach doesn't start with the attack. It starts with what you missed.

I've spent 15 years building and securing IT environments where downtime was not an option. The pattern I see over and over is simple: the businesses that get hurt badly are rarely the ones with exotic problems. They're the ones with ordinary gaps nobody checked. A password reused in three places. A backup drive plugged into the same server it was supposed to protect. A firewall that hasn't been updated since it was installed.

This checklist is built to surface those ordinary gaps. It takes about 20 minutes. You don't need to be technical. If you don't know the answer to a question, that is an answer: mark it "No" and move on.

— Eric Bell, Founder and CEO, Sino Technology Solutions

How to use this checklist

1. Answer each question **Yes** or **No**. Be honest. "Mostly" or "I think so" counts as No.
2. Give yourself **1 point for every Yes**.
3. Add up your score at the end and read the scoring guide.
4. For every No, read "What this gap means" in Section 3. That's your to-do list, in plain English.

Section 1: The Checklist

A. Access, Passwords & Multi-Factor Authentication (MFA)

#	Question	Yes	No
1	Is multi-factor authentication (MFA) turned on for email for every user, including the owner?	☐	☐
2	Is MFA turned on for banking, payroll, accounting, and any admin accounts (Microsoft 365 / Google Workspace admin, domain registrar, website)?	☐	☐
3	Does your team use a password manager instead of reusing passwords or keeping them in a spreadsheet, notebook, or browser notes?	☐	☐
4	When someone leaves the company, are their accounts disabled and shared passwords changed the same day?	☐	☐

B. Backups

#	Question	Yes	No
5	Is your critical business data (files, accounting, customer records, email) backed up automatically, without anyone having to remember?	☐	☐
6	Is at least one copy of your backups stored off-site or in the cloud, and **not** permanently connected to the systems it protects?	☐	☐
7	Have you actually restored files from a backup in the last 6 months to prove it works?	☐	☐
8	Do you know how long it would take to get back up and running from your backups (hours, days, or weeks)?	☐	☐

C. Patching & Updates

#	Question	Yes	No
9	Are Windows/macOS and common apps (browsers, Office, PDF readers) set to update automatically on every computer?	☐	☐
10	Is someone responsible for updating firewalls, routers, VPNs, and servers, and do they do it at least monthly?	☐	☐

#	Question	Yes	No
11	Have you retired (or isolated) any computer, server, or device that no longer receives security updates from its manufacturer?	☐	☐

D. Email & Phishing

#	Question	Yes	No
12	Has everyone on your team had phishing awareness training (even a short session) in the last 12 months?	☐	☐
13	Do you have a rule that any request to change bank details, send a wire, or buy gift cards must be confirmed by phone using a number you already have, not one from the email?	☐	☐
14	Is it easy and blame-free for employees to report a suspicious email, and do they know who to report it to?	☐	☐

E. Devices (Laptops, Desktops, Phones)

#	Question	Yes	No
15	Does every work computer have up-to-date antivirus / endpoint protection turned on?	☐	☐
16	Are laptops encrypted (BitLocker on Windows, FileVault on Mac) and phones protected with a passcode?	☐	☐
17	Do everyday users work from standard accounts rather than administrator accounts?	☐	☐

F. Network

#	Question	Yes	No
18	Have the default passwords on your router, firewall, Wi-Fi, printers, and cameras been changed?	☐	☐
19	Is guest Wi-Fi separate from the network your business computers use?	☐	☐
20	Is remote access to your office (VPN, remote desktop) limited, protected by MFA, and not left open to the internet "just in case"?	☐	☐

G. Vendors & Third Parties

#	Question	Yes	No
21	Do you have a list of every outside company that has access to your systems or data (IT provider, software vendors, payroll, cloud apps)?	☐	☐
22	Do you know what security those vendors use, and would they tell you promptly if they had a breach involving your data?	☐	☐

H. Incident Readiness

#	Question	Yes	No
23	Do you have a written, one-page plan for what to do if you're hit by ransomware or an account is compromised, including who to call?	☐	☐
24	Do you know whether you have cyber insurance, what it covers, and what you must do (and not do) to keep a claim valid?	☐	☐
25	Do you keep an offline copy (printed or on a separate device) of key contacts: IT support, bank, insurer, attorney, and key customers?	☐	☐

Section 2: Scoring Guide

Count your Yes answers. Your score: _____ / 25

Score	What it means
21–25: Solid foundation	You've covered the basics many businesses skip. Your next step is verification: are these controls actually working the way you think? A threat assessment tests that.
14–20: Real gaps	You've done some of the right things, but there are openings an attacker could use. Prioritize the "No" answers in sections A (access), B (backups), and C (patching) first.
0–13: High exposure	This is not a judgment, it's a starting point. Several common attack paths are likely open. Start with MFA (questions 1–2) and backups (questions 5–7) this week, then work through the rest.

One rule overrides the score: a "No" on question 1, 6, or 7 is urgent regardless of your total. Unprotected email and backups that can't survive an attack are the gaps that most often turn an incident into a business-ending event.

Section 3: What Each Gap Means (in Plain English)

A. Access, Passwords & MFA

1–2. No MFA on email or financial/admin accounts. A stolen password is all it takes to get in. Your email is the master key: it's where password resets go, where invoices are sent, and where an attacker can impersonate you to your customers and bank. MFA adds a second check, so a password alone isn't enough. Where you can, prefer an authenticator app, a passkey, or a hardware security key over text-message codes; criminals have tools that trick people into handing over one-time codes on fake login pages.

3. No password manager. Reused passwords mean one breach at any website can unlock your business accounts. A password manager lets everyone use long, unique passwords without memorizing them.

4. Accounts left open after people leave. Former employees, or anyone who got hold of their credentials, still have a door into your systems. Make account shutdown part of every offboarding checklist.

B. Backups

5. Backups aren't automatic. Backups that depend on someone remembering eventually stop happening. Usually nobody notices until the day they're needed.

6. Backups are always connected. Ransomware encrypts everything it can reach. A backup drive plugged into the same server gets encrypted along with it. You need at least one copy that's off-site, in the cloud, or disconnected.

7. Backups have never been tested. An untested backup is a hope, not a plan. Restore a few files, or a whole system, on a schedule.

8. Unknown recovery time. If restoring takes two weeks, can the business survive two weeks? Knowing the number lets you decide whether it's acceptable before a crisis decides for you.

C. Patching & Updates

9. Computers and apps aren't auto-updating. Attackers routinely exploit known flaws that already have a fix available. Automatic updates close those holes without anyone having to think about it.

10. Firewalls, VPNs, routers, and servers aren't patched. These devices sit at the edge of your network, facing the internet, and are a favorite target. They often don't update themselves. Someone needs to own this.

11. Out-of-support systems still in use. Once a manufacturer stops issuing security updates, every new flaw stays open forever. Replace these, or at minimum isolate them from the internet and the rest of your network.

D. Email & Phishing

12. No phishing training. Most attacks still start with someone clicking a link or opening a file. Phishing emails are getting more convincing, so short, regular reminders matter more than an annual lecture.

13. No call-back rule for payments. Business email compromise, where a criminal impersonates a vendor or executive to redirect a payment, depends on nobody picking up the phone. A simple verification rule stops it cold.

14. Reporting isn't easy or safe. If people are afraid of looking foolish, they won't report the email they clicked. Early reporting is often the difference between a near-miss and an incident.

E. Devices

15. No endpoint protection. Without it, malicious software can run on a computer with nothing watching or blocking it.

16. Unencrypted laptops and unlocked phones. A lost or stolen device becomes a data breach. Encryption makes the data unreadable without the password.

17. Everyone runs as administrator. If a user with admin rights clicks something malicious, the malware gets admin rights too. Standard accounts limit the damage.

F. Network

18. Default passwords still set. Default passwords for common devices are published online. Leaving them unchanged is like leaving the key in the door.

19. Guests share your business network. A visitor's infected phone, or a curious guest, shouldn't be able to see your file server or accounting system.

20. Remote access left wide open. Remote desktop and VPN services exposed to the internet without MFA are a common way attackers get in. Limit who can use them and protect them with MFA.

G. Vendors

21. No vendor list. You can't manage risk you can't see. Every outside company with access to your systems is a potential path in.

22. Unknown vendor security. If a vendor is breached, your data and your systems can be part of it. Ask what they do to protect you and how they'll notify you.

H. Incident Readiness

23. No incident plan. In the first hours of an attack, people panic, and panic causes mistakes like wiping evidence or paying too quickly. A one-page plan tells everyone what to do and who to call.

24. Unclear cyber insurance. Many policies have conditions, such as requiring MFA or calling the insurer before hiring help. Know them now, not during the incident.

25. No offline contact list. If your email and files are locked, you may not be able to look up your IT provider's, bank's, or insurer's phone number. Keep a copy somewhere an attacker can't reach.

Section 4: Your Next Step

A self-assessment tells you what you *think* is in place. A threat assessment tells you what's *actually* in place.

If this checklist surfaced questions you couldn't answer, or gaps you're not sure how to close, I'm happy to talk it through. Book a free 20-minute security check-in call: we'll go over your results together and I'll tell you honestly where I'd focus first. If it makes sense from there, we can scope a full threat assessment of your environment.

When you work with Sino Technology Solutions, you work with me directly. No layers of account managers, no junior consultants learning on your environment.

Book a free 20-minute security check-in: email info@sinotechsol.com with the subject line "Checklist" and your score, and we'll find a time.

Eric Bell Founder and CEO, Sino Technology Solutions info@sinotechsol.com | sinotechsol.com Tampa Bay, Florida

This checklist is a general self-assessment tool, not a substitute for a professional security assessment or legal/compliance advice.