CGetty
TECHNOLOGIES LLC

VETERAN-OWNED • TRUSTED IT & CYBERSECURITY

Free IT & Cybersecurity Health Check

A 45-question self-assessment for small businesses

What this is

A practical checklist you can run yourself in about 30 minutes to find the gaps in your IT and cybersecurity posture — before someone else does. Built for small businesses, professional services firms, and one-to-fifty-person teams that don't have a dedicated IT or security person on staff.

How to use it

Walk through the seven domains. Check each box that's TRUE for your business today. Be honest — leave a box empty if you're not sure. Tally your score on the last page. Then decide what to fix first.

How to score yourself

Each domain has 6 to 7 yes/no questions. There are 45 total. The math is simple:

1. Check the box if the statement is currently TRUE for your business.
2. Leave it unchecked if it isn't, or if you're not sure.
3. Add up your checks at the end and use the rubric on the last page.

Score Rubric

SCORE	POSTURE	WHAT IT MEANS
38–45	**Mature**	You are in the top tier of small businesses for IT and cybersecurity hygiene. Focus on tabletop exercises, vendor risk, and continuous improvement.
28–37	**Solid**	You have the basics covered, but there are real gaps that an attacker or auditor would find. Prioritize the unchecked items in Domains 1, 3, and 7.
18–27	**At Risk**	You have meaningful exposure. A single phishing click, lost laptop, or fired employee could disrupt the business. Address Identity & Access and Backups first.
0–17	**Critical**	You are operating with significant risk. This is the typical posture before an incident, not after. We strongly recommend an outside review within 30 days.

DOMAIN 01

Identity & Access

Who can sign in, and how protected are those sign-ins?

- ☐ Multi-factor authentication (MFA) is enforced for every email account and business application.
- ☐ MFA is enforced on the owner/admin Microsoft 365, Google Workspace, or QuickBooks account.
- ☐ We use a password manager (1Password, Bitwarden, Dashlane, or similar) — not browser-saved passwords or sticky notes.
- ☐ No employee, contractor, or family member is sharing a single login (no shared passwords).
- ☐ Admin/owner accounts are separate from day-to-day work accounts.
- ☐ When someone leaves, their access to email and apps is removed within 24 hours.
- ☐ We can produce a list of every active user in our email tenant in under 5 minutes.

Checks in Domain 01: ____ of 7

DOMAIN 02

Endpoint & Device Security

Are the laptops, desktops, and phones touching company data actually protected?

- ☐ Every company laptop and desktop has active antivirus or EDR (Defender, SentinelOne, CrowdStrike, etc.).
- ☐ Every device has automatic OS updates turned on and is current within 30 days.
- ☐ Disk encryption (BitLocker on Windows, FileVault on Mac) is enabled on every laptop.
- ☐ Devices auto-lock with a passcode/PIN after 15 minutes of inactivity.
- ☐ Personal phones that access company email require a screen lock and remote-wipe capability.
- ☐ We have an inventory list of every laptop, desktop, and tablet that touches company data.
- ☐ Old or retired devices are wiped before being sold, donated, or recycled.

Checks in Domain 02: ____ of 7

DOMAIN 03

Backup & Recovery

If a laptop dies or ransomware hits tomorrow, what comes back — and how fast?

- ☐ Critical business files (accounting, contracts, client data) are backed up daily.
- ☐ We have at least one backup copy stored in a separate location (cloud, offsite drive, or different account).
- ☐ Microsoft 365 / Google Workspace mail and OneDrive/Drive data is backed up to a third-party tool — not just the platform itself.
- ☐ We have tested a full file restore in the last 90 days.
- ☐ We know our Recovery Time Objective (how long we can be down) and Recovery Point Objective (how much data we can lose).
- ☐ Backups are protected from ransomware (immutable, separate credentials, or air-gapped).

Checks in Domain 03: ____ of 6

DOMAIN 04

Email & Phishing Defense

Phishing is still the #1 way small businesses get breached.

- ☐ Spam and phishing filtering is active and tuned (Microsoft Defender, Google Workspace, Proofpoint, etc.).
- ☐ Our domain has SPF, DKIM, and DMARC records configured (anti-spoofing).
- ☐ External email is visually flagged or banner-tagged so staff can spot impersonation attempts.
- ☐ Staff have received phishing-awareness training in the last 12 months.
- ☐ Staff know exactly who to forward a suspicious email to.
- ☐ Wire transfers, vendor banking changes, and gift-card requests require out-of-band verification (phone call, not just email).

Checks in Domain 04: ____ of 6

DOMAIN 05

Network & Remote Access

How locked-down is the office network — and the way people connect to it?

- ☐ The office router/firewall password has been changed from the factory default.
- ☐ Router/firewall firmware is updated within 90 days of release.
- ☐ Guest Wi-Fi is on a separate network from staff/business Wi-Fi.
- ☐ Wi-Fi uses WPA2 or WPA3 with a strong, non-trivial password.
- ☐ Remote access uses something better than open RDP (VPN, ZTNA, Splashtop, or similar).
- ☐ Smart devices, cameras, and IoT gear are isolated on their own VLAN or guest network.

Checks in Domain 05: ____ of 6

DOMAIN 06

Data Protection & Privacy

Where is your sensitive data, and who can actually see it?

- ☐ We know where client PII, payment data, or PHI lives (which folders, drives, or apps).
- ☐ Sensitive folders use 'least privilege' — only the people who need access have access.
- ☐ We have documented data retention rules (how long files stay, when they're deleted).
- ☐ We have a written privacy notice / privacy policy if we collect data from clients online.
- ☐ Vendors and contractors with access to client data have signed an NDA or DPA.
- ☐ If we handle PHI, we have a HIPAA Business Associate Agreement (BAA) with anyone touching that data.

Checks in Domain 06: ____ of 6

DOMAIN 07

Incident Readiness

When (not if) something goes wrong, do you know what happens in the first 60 minutes?

- ☐ We have a written incident response plan, even a one-page version.
- ☐ We have an after-hours contact list for IT, leadership, and outside counsel.
- ☐ We have cyber liability insurance — and we know our incident reporting hotline.
- ☐ We know which clients/regulators we have to notify if we have a breach.
- ☐ We have a relationship with an outside IT/security firm we can call before an incident — not after.
- ☐ Leadership has done at least one tabletop discussion of a ransomware or data-loss scenario in the last 12 months.

Checks in Domain 07: ____ of 6

Your total score

Add up the checks across all seven domains, then look up where you land on the rubric.

DOMAIN	YOUR SCORE	OUT OF
01 — Identity & Access		/ 7
02 — Endpoint & Device Security		/ 7
03 — Backup & Recovery		/ 6
04 — Email & Phishing Defense		/ 6
05 — Network & Remote Access		/ 6
06 — Data Protection & Privacy		/ 6
07 — Incident Readiness		/ 6
TOTAL		**/ 45**

Where to go from here

Whatever your score, the next step is the same: pick the two or three lowest-scoring domains and fix those first. Most small business breaches we see come from gaps in Identity & Access (Domain 1), Backup (Domain 3), and Incident Readiness (Domain 7). Start there.

Want a second set of eyes?

If you'd like a free 30-minute review of your results — no sales pitch, no obligation — reach out. We'll walk through your unchecked items together and help you sequence the fixes by impact and cost. CGetty Technologies is a Pennsylvania-based, veteran-owned cybersecurity and managed-IT firm built specifically for small businesses without a full-time IT or security team.

CGetty TECHNOLOGIES LLC

Book your free 30-minute review

Email: info@cgetty.com

Web: www.cgetty.com

Pennsylvania-based · Veteran-owned