SENTRY
CONSULTING GROUP

SECURITY-FIRST MANAGED IT
Fairfax, VA · DC / MD / VA · Veteran-Owned

FREE SELF-ASSESSMENT

The Small-Business IT & Cybersecurity Readiness Checklist

15 questions to gauge whether your technology would hold up to a real threat, an auditor, or a cyber-insurance review. Answer each honestly with a yes or no.

Accounts & Access

- ☐ **Multi-factor authentication (MFA) is on for every email and remote-access account.**
  A stolen password alone shouldn't be enough to get in. This is the single highest-impact control.
- ☐ **Admin accounts are separate from everyday accounts and limited to who truly needs them.**
  If an everyday account is compromised, the attacker shouldn't inherit the keys to everything.
- ☐ **When someone leaves, their accounts, email, and access are shut off the same day.**
  Every departure is a security event. "We'll get to it" is how data walks out the door.

Devices

- ☐ **Every computer runs managed endpoint protection (EDR) that someone actively monitors.**
  Antivirus that no one watches is a smoke alarm with the battery out.
- ☐ **Laptops and mobile devices are encrypted, so a lost device isn't a reportable breach.**
  Encryption turns a stolen laptop into a hardware cost instead of an incident.
- ☐ **Operating systems and software are patched on a defined schedule, not "whenever."**
  Most breaches exploit known holes that a patch had already closed.

Data & Backup

- ☐ **Critical data is backed up automatically, and the backups are monitored for success.**
  Backups that quietly fail are worse than none, because you think you're covered.
- ☐ **A test restore has actually been performed in the last 90 days.**
  A backup you've never restored is a hope, not a recovery plan.
- ☐ **You know where your sensitive data lives (client records, PHI, financials) and who can access it.**
  You can't protect, or prove you protect, data you haven't mapped.

Email & Threats

- [ ] **Advanced email security filters phishing and business-email-compromise (BEC) attempts.**
  Email is the front door for the large majority of attacks and fraud.
- [ ] **Any change to vendor banking or payment details is verified by phone to a known number.**
  This one habit stops most wire-fraud losses, no technology required.
- [ ] **Staff get security-awareness training and know how to report a suspicious message.**
  Your people are either your weakest layer or your first line. Training decides which.

People, Process & Readiness

- [ ] **IT support comes from a consistent team that knows your environment, with defined response times.**
  Rotating, anonymous help desks don't know your systems and can't move fast when it counts.
- [ ] **Your environment is documented, not living in one person's head.**
  Networks, accounts, vendors, and procedures should survive any one person leaving.
- [ ] **You could produce evidence of your security controls tomorrow if an auditor, cyber-insurer, or client asked.**
  Doing the work isn't enough; being able to prove it is what passes audits and wins contracts.

How did you score?

13–15 yes: Strong. You're operating at a level most small businesses aren't, and you can likely prove it. Keep the evidence current.

8–12 yes: Real gaps. You're exposed in specific, fixable places, and probably can't fully document what you do have.

7 or fewer: At risk. A single incident, audit, or insurance review could hurt. Worth addressing soon, not someday.

Not sure how you scored, or where to start?

Sentry Consulting Group is a veteran-owned, security-first managed IT provider in Fairfax, VA, serving small businesses across the DC/MD/VA corridor. Our free assessment reviews your environment, identifies the gaps, and tells you exactly what it would take to close them, with no obligation.

Book your free assessment: calendly.com/jcoppo-sentryconsulting/30min