Prevvi

MANAGED IT & AI SOLUTIONS
CAMBRIDGE, MA

The 11-Point Small Business Cybersecurity Checklist

Small businesses get breached by boring things: an unpatched firewall, a reused password, a convincing invoice email. Boring attacks have boring, affordable defenses. These are the eleven controls that matter, ordered by what the 2026 breach data actually says.

Why this matters: in the **Verizon 2026 Data Breach Investigations Report**, about **96% of ransomware victims were small and mid-sized businesses**. Attackers do not pick targets; their scanners do.

- [ ] **01 Patch on a schedule, not a mood**
  Automate and verify OS, browser, firewall, and VPN updates. Unpatched vulnerabilities are the #1 way attackers first get in (31% of breaches, Verizon DBIR 2026).

- [ ] **02 Multi-factor authentication, everywhere**
  Turn on MFA for email, banking, VPN, and every admin account. It blocks over 99.2% of account-compromise attacks (Microsoft). Prefer app or hardware keys over SMS.

- [ ] **03 Endpoint detection and response (EDR)**
  Go beyond antivirus: EDR watches for attacker behavior and can isolate a machine automatically at 3 a.m.

- [ ] **04 Backups you have actually restored**
  Follow the 3-2-1 rule (three copies, two media, one offsite and immutable). Test a restore quarterly and time it. 66% of ransomware victims recover via backups (Sophos 2026).

- [ ] **05 Email security beyond the spam filter**
  Add advanced filtering, link and attachment scanning, and publish SPF, DKIM, and DMARC so criminals cannot spoof your domain. Email starts about half of ransomware incidents.

- [ ] **06 A password manager for the whole team**
  Make the secure path the lazy path. Paired with MFA it closes most of the credential attack surface.

- [ ] **07 Least privilege and no shared admin accounts**
  Day-to-day work in standard accounts; admin rights in separate, monitored accounts used only when needed. Keep the blast radius small.

- [ ] **08 Security awareness training that is not a checkbox**
  The human element was present in 62% of breaches (DBIR 2026). Short, regular, specific, with simulated phishing and instant feedback.

- [ ] **09 An offboarding process that runs the same day**
  End access the hour employment does: email, VPN, cloud apps, and shared credentials. Orphaned accounts are also audit findings.

- [ ] **10 A one-page incident response plan**
  Write down who to call, what to disconnect, how to communicate if email is down, and where the cyber-insurance policy lives. The average US breach costs $10.22M (IBM 2025).

- [ ] **11 Mobile device management (MDM)**
  The phones are part of your network. Require screen lock, device encryption, remote wipe, and enforced updates. Most business plans already include the tooling.

If you can only do three this quarter

01
Patching
Closes vulnerability exploitation, 31% of initial access.

02
MFA
Closes credential abuse, 39% of breaches overall.

04
Tested backups
Makes ransomware survivable, 48% of all breaches.

Everything else on the list makes you harder to hit. These three make you survivable.

One more blind spot: your vendors

The DBIR 2026 found third-party involvement in 48% of breaches, and 55% among small businesses specifically. Your bookkeeper's remote-access tool and your website contractor's admin login are part of your attack surface. Ask every vendor with access which of these eleven controls they run, including your IT provider.

Sources

Verizon, 2026 Data Breach Investigations Report
Microsoft, mandatory MFA documentation (99.2% figure)
CISA, Implementing Phishing-Resistant MFA
Google Cloud / Mandiant, M-Trends 2026
Sophos, State of Ransomware 2026
Veeam, ransomware trends (backups targeted in 93%+ of attacks)
US-CERT / CISA, Data Backup Options (the 3-2-1 rule)
NIST SP 800-124 Rev. 2, mobile device security
IBM, Cost of a Data Breach Report 2025
FTC, Cybersecurity for Small Business

Want to know which of the eleven you are missing?
Book a free assessment and we will walk your environment against this exact list. No scare tactics.

prevvi.com
+1 (617) 676-0012
info@prevvi.com