



Cybersecurity Best Practices Checklist

2026 edition // for small and mid-size businesses in North Georgia

Cybersecurity used to be the lock on your front door. Today it is the lock, the alarm, the cameras, the fence, and the dog. Attackers are faster, cheaper, and better organized than they were five years ago, and small businesses are now the preferred target because the defenses are thinner and the payoffs are still worth the effort. The good news: the fundamentals still work, you just have to do them all.

This checklist walks through the essentials, updated for the threats that actually matter in 2026. Print it, mark what is in place, and bring the gaps to your next IT review.

\$16.6B

U.S. cybercrime losses in 2024, up 33%
year over year

88%

of SMB breaches involve ransomware

\$1.1B

lost to AI deepfake fraud in the U.S. in
2025

Why this matters now

The FBI logged \$16.6 billion in reported cybercrime losses in 2024, a one-year jump of 33 percent. Business email compromise alone, where an attacker impersonates a vendor or executive to reroute a payment, accounted for \$2.77 billion of that total. Ransomware remains the single biggest threat to small and mid-size businesses: 88 percent of SMB breaches involve ransomware, and the median ransom demand is now \$115,000.

Two things have changed since the last version of this checklist. First, AI has put convincing phishing, voice cloning, and fake video calls within reach of any criminal with an internet connection. Second, most breaches no longer start inside your company. They start with a vendor, a SaaS tool, or a cloud account that shares access into your environment.

¹FBI IC3 2024 Annual Report.

²Verizon 2025 Data Breach Investigations Report, SMB snapshot.

³Industry reporting on AI-enabled fraud, 2025 (U.S.).

The 2026 Checklist

Eleven sections. If your team can check every box, you are ahead of most businesses in the region. If you cannot, the gaps below are the shortest path to fewer incidents and a lower insurance premium.

1. Identity: passwords, MFA, and passkeys

- ✓ **Require a password manager:** Every employee gets a company-provisioned password manager. This is non-negotiable in 2026. Re-used passwords are the starting point for credential-stuffing attacks.
- ✓ **Enforce phishing-resistant MFA:** Multi-Factor Authentication (MFA) adds a second check beyond the password. Not all MFA is equal: SMS codes and push prompts can be stolen or fatigued. CISA, the U.S. cyber agency, recommends phishing-resistant MFA using passkeys or FIDO2 security keys, which bind the login to a specific device and cannot be handed over to an attacker.
- ✓ **Move to passkeys where supported:** Microsoft 365, Google Workspace, and most major business apps now support passkeys. They are faster for users and resistant to phishing. Start with admin accounts and any app that holds money or customer data.

2. Modern endpoint protection (EDR, not just antivirus)

- ✓ **Deploy business-grade EDR on every device:** Endpoint Detection and Response (EDR) is the modern replacement for antivirus. It watches behavior, not just known bad files, and can roll back a ransomware attack in progress. Every laptop, desktop, and server needs it, including personal devices used for work.
- ✓ **Monitor 24/7:** Attackers do not keep business hours. Most successful ransomware attacks start late on a Friday or over a holiday weekend. If no one is watching the EDR alerts at 2 a.m., the tool is only doing half its job.

3. Patch and update management

- ✓ **Automate updates everywhere possible:** Operating systems, browsers, Microsoft 365 apps, line-of-business software, and firmware on firewalls and switches. Exploitation of unpatched software is now the number-two way attackers get in.
- ✓ **Set a maximum patch window:** Critical vulnerabilities get patched within 7 days. Everything else within 30. If a vendor cannot tell you when a patch was last applied to a given device, that is a finding.

4. Security awareness and AI phishing defense

- ✓ **Train quarterly, not annually:** AI-written phishing emails no longer have the typos and awkward grammar that used to give them away. Training has to keep up. Short, frequent lessons beat the one-hour yearly module.
- ✓ **Simulate phishing and voice cloning:** Send test phishing emails monthly. Add a quarterly voice-cloning drill, where a leader's voice is simulated asking for a wire transfer or password reset. Deepfake-enabled CEO fraud reportedly targets roughly 400 companies per day, and a convincing voice clone can be built from three seconds of audio.
- ✓ **Create a "call back on a known number" rule:** Any request for money, credentials, or gift cards that arrives by email, text, or voice has to be verified through a second channel using a phone number the employee already has. This one rule stops most BEC and deepfake attacks cold.

5. Secure network access

- ✓ **Segment the network:** Office Wi-Fi, guest Wi-Fi, production machines, and IoT devices (cameras, printers, badge readers) should be on separate network segments. A compromised printer should not be able to reach your accounting server.
- ✓ **Retire legacy VPNs in favor of zero-trust access:** A Virtual Private Network (VPN) that grants a remote worker full network access once they log in is a 2015 design. Modern Zero-Trust Network Access (ZTNA) grants only the specific apps a user needs, and re-checks identity and device health on every connection.
- ✓ **Keep firewalls current and monitored:** A firewall with an expired license is a \$3,000 paperweight. Licenses, firmware, and rules get reviewed at least twice a year.

6. Backup and ransomware recovery

- ✓ **Follow the 3-2-1-1-0 rule:** Three copies of your data, on two different media, with one copy off-site, one copy immutable (cannot be altered or deleted by an attacker), and zero errors on your last test restore. Cloud backups alone do not meet this standard if the attacker has your admin credentials.
- ✓ **Test restores on a schedule:** A backup you have never restored is a hope, not a plan. Restore at least one critical system quarterly and time how long it takes.
- ✓ **Assume the attacker has been inside for weeks:** Modern ransomware groups dwell in a network for a median of several weeks before triggering encryption, long enough to corrupt recent backups. Keep backup history long enough to recover a clean version.

7. Least-privilege access control

- ✓ **Grant the minimum access needed, and nothing more:** Sales does not need access to payroll. The receptionist does not need domain admin. Review access quarterly and after every role change or departure.
- ✓ **Separate admin accounts from daily-use accounts:** IT staff, including outside partners, log in daily with a standard account and only elevate to an admin account when a task specifically requires it. This single change blocks a large share of ransomware blast-radius.
- ✓ **Off-board within 24 hours:** When someone leaves, access is revoked the same day, including email, file shares, SaaS apps, VPN, and any personal device that had company data on it.

8. Secure email

- ✓ **Configure SPF, DKIM, and DMARC:** These three email authentication standards make it dramatically harder for an attacker to send email that looks like it came from your domain. Most small businesses have SPF partially configured and the other two set to "none." That is not protection.
- ✓ **Use an advanced email security tool:** The spam filter that ships with Microsoft 365 or Google Workspace is a good start and not the end. A layered email security product catches impersonation, malicious links that activate after delivery, and AI-generated phishing.
- ✓ **Encrypt sensitive email and attachments:** If you send Protected Health Information, financials, or legal documents, use a HIPAA-compliant or encrypted email solution. Regular email is a postcard.

9. Incident response and cyber insurance

- ✓ **Write the plan before you need it:** A one-page incident response plan covers: who declares an incident, who is called first (IT partner, insurer, attorney, leadership), what systems get isolated, what regulators or customers get notified, and who talks to the press. Keep a printed copy off the network.
- ✓ **Run a tabletop exercise annually:** Gather the response team for 90 minutes, walk through a realistic ransomware scenario, and find out where the plan breaks. Cheaper than finding out during a real incident.
- ✓ **Carry cyber insurance, and understand the controls it requires:** Most cyber insurers now require MFA on email and remote access, EDR on all endpoints, tested offline backups, and proof of security awareness training before they will issue or renew a policy. Your renewal questionnaire is a useful checklist on its own.

10. Vendor and supply chain risk

- ✓ **Inventory every vendor with access to your data:** Accounting software, MSP, payroll provider, CRM, marketing tools, shop-floor systems. If a vendor has a login into your environment or holds your customer data, they are in scope. The Verizon 2025 Data Breach Investigations Report found that third-party involvement in breaches doubled year over year.
- ✓ **Review vendor security at least annually:** Ask each vendor for a SOC 2 report or a short security questionnaire. The ones who refuse tell you something important.
- ✓ **Limit and log vendor access:** Vendors log in with their own named accounts, with MFA, with just-in-time access where possible, and the sessions are recorded. No shared "support@" logins.

11. Physical security

- ✓ **Encrypt every device:** Full-disk encryption (BitLocker on Windows, FileVault on Mac) on every laptop, desktop, and phone. A stolen but encrypted laptop is a nuisance. A stolen unencrypted laptop is a data breach.
- ✓ **Control facility access and review it:** Badge or keypad access on sensitive areas (server closet, records room, shop floor with networked machines). Review the access list quarterly. Pull the log after every employee departure.

2026 threat radar: what to watch for

Even with the fundamentals in place, these are the patterns most likely to bite a business in our region in 2026:

- **AI voice and video impersonation:** A call or video meeting from "the owner" asking for a wire or a password reset. Assume it is fake until verified on a known number.
- **MFA fatigue and push-bombing:** A flood of MFA prompts late at night, hoping an exhausted employee taps "Approve." Phishing-resistant MFA makes this impossible.
- **Third-party compromise:** A vendor gets breached, attackers use their access to reach you. Vendor access reviews catch this.
- **Shadow AI and data leakage:** An employee pastes customer data into a free AI tool. IBM's 2025 Cost of a Data Breach Report tied ungoverned AI use to an extra \$670,000 per breach on average.
- **Unusual login activity:** Logins at 3 a.m., from new countries, or from new devices. EDR and identity monitoring should flag these in real time.

Why business owners partner with an MSP

Keeping all eleven of these controls running, 24 hours a day, across a growing business is a full-time job. It is several full-time jobs once you add a security operations center, a patch cycle, an EDR console, and a backup schedule. A Managed Service Provider (MSP) takes that work off the business and runs it for a flat monthly fee.

PeachByte is North Georgia's managed IT partner for businesses that want to stop thinking about IT. Founded in 2022 and based in Adairsville, we manage 200+ endpoints across the region and respond in minutes, not hours. One partner, one bill, one phone number for workstations, servers, email, cybersecurity, backups, vendor coordination, and the AI tooling that is starting to run alongside all of it.

Your next step

Start with a free IT review: a 60-minute walk-through where we benchmark your environment against the checklist above and hand you a written roadmap of what to fix first. No pressure, no sales pitch, and the findings are yours to keep whether or not we work together.

Book a free strategy call at peachbytesolutions.com, or dial 470-529-1421. We cover Adairsville, Cartersville, Calhoun, Dalton, Rome, and Marietta on-site, and the rest of North Georgia remotely.

Sources

1. FBI Internet Crime Complaint Center (IC3), 2024 Annual Report. ic3.gov.
2. Verizon, 2025 Data Breach Investigations Report, SMB snapshot. verizon.com/business/resources/reports/dbir.
3. U.S. deepfake fraud loss figure: industry reporting on AI-enabled fraud, 2025 (Deloitte projection, consumer-protection and insurer data).
4. IBM Security, Cost of a Data Breach Report 2025.
5. CISA, Implementing Phishing-Resistant MFA, fact sheet.