# 2026 SMB Cybersecurity Checklist

# 2026 SMB Cybersecurity Checklist

**The Complete 25-Point Security Assessment for Small & Medium Businesses**

*Published by lilMONSTER (lil.business) — March 2026 Version 1.0 | Covers threats and compliance requirements as of Q1 2026*

---

## How to Use This Checklist

Work through each section with your IT team (or your managed service provider). For each item:

- **Check the box** when the control is fully implemented
- **Note your status**: ✅ Done | 🟡 Partial | ❌ Not Started
- **Priority levels**: 🔴 Critical (do this week) | 🟠 High (do this month) | 🟡 Medium (do this quarter)
- **Score yourself**: 20+ items checked = Strong | 15-19 = Needs Work | Below 15 = At Risk

---

## Section 1: Access Control & Identity

### 1. Multi-Factor Authentication (MFA) on All Business Accounts

**Priority: 🔴 Critical**

☐ MFA is enabled on email (Microsoft 365, Google Workspace, etc.)

☐ MFA is enabled on cloud storage (OneDrive, Google Drive, Dropbox)

☐ MFA is enabled on financial/banking platforms

☐

- [ ] MFA is enabled on VPN and remote access
- [ ] MFA is enabled on social media and marketing accounts

**Why it matters:** In 2026, credential stuffing attacks using AI-generated password lists have made single-factor authentication effectively worthless. Microsoft reports that MFA blocks 99.9% of automated attacks. If you implement only one item from this checklist, make it this one.

**Action:** Enable MFA everywhere. Use authenticator apps (Microsoft Authenticator, Google Authenticator) or hardware keys (YubiKey). Avoid SMS-based MFA where possible — SIM-swap attacks are up 340% in 2025-2026.

---

## 2. Privileged Access Management (PAM)

**Priority: 🟠 High**

- [ ] Admin accounts are separate from daily-use accounts
- [ ] Admin access requires additional authentication steps
- [ ] A complete list of who has admin access exists and is reviewed quarterly
- [ ] Former employees/contractors have been fully deprovisioned within 24 hours of departure

**Why it matters:** 74% of breaches involve privileged credential misuse (Verizon DBIR 2025). If an attacker compromises a regular user account, the blast radius is limited. If they get an admin account, they own everything.

**Action:** Create dedicated admin accounts (e.g., admin-john@company.com) that are never used for email or web browsing. Review admin access quarterly. Automate deprovisioning in your HR offboarding workflow.

---

## 3. Password Policy & Credential Hygiene

**Priority: 🟠 High**

- [ ] A business password manager is deployed (1Password, Bitwarden, etc.)
- [ ]

- [ ] All employees use unique passwords for every business account
- [ ] Passwords are minimum 16 characters or passphrase-based
- [ ] Known-breached credentials are checked against Have I Been Pwned or equivalent

**Why it matters:** AI-powered password cracking in 2026 can brute-force 8-character complex passwords in under 4 hours. Reused credentials from personal breaches are the #1 initial access vector for SMB attacks. A password manager eliminates both risks.

**Action:** Deploy a team password manager this week. Migrate shared credentials (Wi-Fi, vendor portals, shared inboxes) into shared vaults. Enforce minimum 16 characters.

---

### 4. Single Sign-On (SSO) for Core Applications

**Priority: 🟡 Medium**

- [ ] SSO is configured for major SaaS platforms (CRM, project management, etc.)
- [ ] SSO reduces the total number of credentials employees manage
- [ ] SSO is paired with conditional access policies (location, device, risk score)

**Why it matters:** SSO combined with conditional access lets you enforce security policies across all applications from one place. When an employee leaves, one deactivation cuts access everywhere. Without SSO, you're relying on remembering to disable accounts across dozens of services.

**Action:** If you use Microsoft 365 or Google Workspace, you already have SSO capability. Enable it for Slack, Salesforce, HubSpot, and other core tools. Prioritise any app that contains customer data.

---

## Section 2: Email Security

### 5. Advanced Email Filtering & Anti-Phishing

**Priority: 🔴 Critical**

- [ ]

- [ ] Email filtering is enabled beyond basic spam (Microsoft Defender for Office 365, Google Advanced Protection, or equivalent)
- [ ] AI-generated phishing simulation training runs quarterly
- [ ] DMARC, DKIM, and SPF records are configured and enforced (not just monitoring)
- [ ] External email warnings are displayed on inbound messages from outside the organisation

**Why it matters:** AI-generated phishing emails in 2026 are nearly indistinguishable from legitimate communications. They're grammatically perfect, contextually relevant (often referencing real projects or colleagues scraped from LinkedIn), and sent from spoofed domains. Your employees will click. Your email security must catch what humans can't.

**Action:** Verify your DMARC policy is set to `p=reject` (not `p=none`). Run a phishing simulation this month. If more than 15% of staff click, increase training frequency.

---

## 6. Business Email Compromise (BEC) Protection

**Priority: 🔴 Critical**

- [ ] Wire transfer / payment change requests require verbal (phone call) confirmation
- [ ] Finance team has a documented verification process for new vendor bank details
- [ ] CEO/executive impersonation protection is enabled in email security
- [ ] Invoice fraud detection is active

**Why it matters:** BEC attacks caused $2.9 billion in losses in 2025 (FBI IC3). AI now clones voice patterns from as little as 3 seconds of audio. An email from your "CEO" asking to wire funds, followed by a phone call that sounds exactly like them, is no longer science fiction — it's happening now.

**Action:** Establish a mandatory verbal verification policy for any financial transaction over $1,000 or any change to payment details. Use a pre-agreed code word for high-value approvals. Never verify by calling the number in the email — use a known contact number.

---

## Section 3: Endpoint Protection

### 7. Endpoint Detection & Response (EDR)

**Priority: 🔴 Critical**

- [ ] EDR software is installed on all company devices (laptops, desktops, servers)
- [ ] EDR covers Windows, macOS, and Linux endpoints
- [ ] EDR alerts are monitored (by internal team or managed service)
- [ ] EDR can isolate a compromised device remotely

**Why it matters:** Traditional antivirus uses signature matching — it can only detect known threats. EDR uses behavioural analysis to detect novel attacks, including fileless malware and living-off-the-land techniques that represent 71% of attacks in 2026. If you're running just Windows Defender without EDR, you're running with your eyes closed.

**Action:** Deploy a modern EDR solution (CrowdStrike Falcon Go, SentinelOne Singularity, Microsoft Defender for Business). Ensure someone is actually reviewing alerts — an unmonitored EDR is only marginally better than nothing.

---

### 8. Device Encryption & Mobile Device Management

**Priority: 🟠 High**

- [ ] Full disk encryption is enabled on all laptops (BitLocker / FileVault)
- [ ] Mobile devices accessing business data are managed (Intune, Jamf, etc.)
- [ ] Remote wipe capability exists for lost/stolen devices
- [ ] BYOD policy is documented and enforced

**Why it matters:** A stolen unencrypted laptop is a data breach notification event under Australian Privacy Act, GDPR, and most US state laws. With encryption, it's a lost asset. The compliance and reputation difference is enormous.

**Action:** Enable BitLocker (Windows) or FileVault (Mac) on every company laptop today. For BYOD, require a work profile or container that can be wiped independently.

---

### 9. Patch Management & Vulnerability Scanning

**Priority: 🔴 Critical**

- [ ] Operating system patches are applied within 48 hours for critical vulnerabilities
- [ ] Application patches (browsers, PDF readers, office suites) are automated
- [ ] A vulnerability scan runs monthly against internet-facing systems
- [ ] End-of-life software (Windows 10, unsupported applications) has been replaced or isolated

**Why it matters:** The average time from vulnerability disclosure to active exploitation dropped to 5 days in 2026 (down from 32 days in 2022). AI-powered exploit development means attackers weaponise CVEs faster than ever. If you're patching on a monthly cycle, you're perpetually exposed.

**Action:** Enable automatic updates for operating systems and browsers. For critical infrastructure, establish a 48-hour patch SLA. Audit for any Windows 10 devices (end of support: October 2025) and any software no longer receiving security updates.

---

## Section 4: Cloud Security

### 10. Cloud Configuration Audit

**Priority: 🔴 Critical**

- [ ] Cloud storage (S3, Azure Blob, Google Cloud Storage) has been audited for public access
- [ ] No databases are directly exposed to the internet
- [ ] Cloud admin consoles are protected with MFA and IP restrictions
- [ ]

- [ ] Default credentials on cloud services have been changed

**Why it matters:** Cloud misconfiguration is the #1 root cause of data breaches in 2026, surpassing phishing for the first time. A single misconfigured S3 bucket or publicly accessible database can expose your entire customer list. These misconfigurations are trivially discoverable using automated scanning tools.

**Action:** Run your cloud provider's free security assessment (AWS Security Hub, Azure Secure Score, Google Security Command Center). Fix any "critical" or "high" findings this week. Schedule quarterly reviews.

---

## 11. SaaS Application Inventory & Shadow IT

**Priority: 🟠 High**

- [ ] A complete inventory of all SaaS applications used by the business exists
- [ ] Each application has a designated owner and data classification
- [ ] Unauthorized SaaS usage (shadow IT) is monitored
- [ ] Offboarding checklist includes deprovisioning from all SaaS apps

**Why it matters:** The average SMB uses 87 SaaS applications (BetterCloud 2025). Most IT teams are only aware of 40-50. Each unknown app is an unmanaged attack surface with credentials, customer data, and integrations you don't know about. When an employee leaves, their access to these apps persists.

**Action:** Audit your DNS logs, credit card statements, and SSO/OAuth grants to discover all SaaS apps in use. Create a simple spreadsheet: app name, owner, data stored, authentication method. Revoke access to anything unused.

---

## 12. Backup & Disaster Recovery (3-2-1-1-0 Rule)

**Priority: 🔴 Critical**

- [ ] Backups follow the 3-2-1-1-0 rule: 3 copies, 2 different media, 1 offsite, 1 immutable/air-gapped, 0 errors on recovery test
- [ ] Backups are tested with a full restore drill at least quarterly

- [ ] Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are defined
- [ ] Ransomware cannot encrypt or delete backup copies (immutability or air-gap)

**Why it matters:** 96% of ransomware attacks in 2026 specifically target backup systems before encrypting production data. If your backups are on the same network, accessible with the same credentials, or stored in a writable cloud location, they will be destroyed alongside your primary data. Immutable backups are the difference between a bad day and a business-ending event.

**Action:** Verify your backups are truly immutable (not just “offsite”). Test a full restore this month — most businesses discover their backups are incomplete or corrupt only when they need them. Define your RTO (how fast you need to recover) and RPO (how much data you can afford to lose).

---

## Section 5: Network Security

### 13. Firewall & Network Segmentation

**Priority: 🟠 High**

- [ ] A next-generation firewall (NGFW) protects the network perimeter
- [ ] Firewall firmware is current (check vendor advisories weekly)
- [ ] Internal network is segmented (guest Wi-Fi, IoT, and production systems on separate VLANs)
- [ ] Firewall management interface is not accessible from the internet

**Why it matters:** Flat networks — where every device can talk to every other device — allow lateral movement. One compromised IoT device (printer, security camera, smart TV) becomes a pivot point to reach your file server, accounting software, and customer database. Network segmentation limits blast radius.

**Action:** At minimum, create three network segments: Corporate (laptops, desktops), IoT/Guest (printers, cameras, visitor Wi-Fi), and Servers (critical systems). Ensure your firewall management interface is only accessible from your internal network.

---

### 14. DNS Filtering & Web Security

**Priority: 🟡 Medium**

- [ ] DNS-level filtering blocks known malicious domains
- [ ] Web filtering prevents access to high-risk categories (newly registered domains, uncategorised sites)
- [ ] HTTPS inspection is enabled for outbound traffic (or DNS-based alternative)

**Why it matters:** DNS filtering is the cheapest, easiest security control you can deploy. It blocks 90%+ of known malware callbacks, phishing sites, and command-and-control communications before they reach endpoints. It takes 15 minutes to set up and costs $0-$2/user/month.

**Action:** Deploy Cloudflare Gateway (free for <50 users), Cisco Umbrella, or DNSFilter. Point your network's DNS to the filtering service. Block newly registered domains (<30 days old) — they're used in 70%+ of phishing campaigns.

---

## Section 6: Incident Response

### 15. Documented Incident Response Plan

**Priority: 🟠 High**

- [ ] A written incident response plan exists and is accessible offline (printed copy or separate system)
- [ ] Roles are assigned: who declares an incident, who communicates externally, who contacts legal
- [ ] Contact list includes: IT lead, legal counsel, insurance provider, forensics vendor, regulator
- [ ] Plan has been tested with a tabletop exercise in the last 12 months

**Why it matters:** The average cost of a data breach is $4.88M (IBM 2025). Organisations with a tested incident response plan reduce that cost by an average of $2.66M and resolve

incidents 108 days faster. In a real incident, you won't have time to figure out who does what.

**Action:** Write a one-page incident response plan covering: detection, containment, communication, eradication, and recovery. Assign roles. Print it out. Run a 90-minute tabletop exercise with your team this quarter.

---

## 16. Cyber Insurance

**Priority: 🟠 High**

- [ ] Cyber insurance policy is active and covers ransomware, BEC, data breach, and business interruption
- [ ] Policy limits are adequate for your revenue and data volume
- [ ] You meet all policy prerequisites (MFA, backups, EDR — many policies void without these)
- [ ] Claims process is documented and insurer contact is in the incident response plan

**Why it matters:** Cyber insurance premiums have stabilised in 2026 after years of increases, but carriers are enforcing prerequisites aggressively. If your policy requires MFA and you suffer a breach without MFA enabled, your claim will be denied. Know your obligations.

**Action:** Review your policy this month. Verify you meet every prerequisite. If you don't have cyber insurance, get quotes — for most SMBs, it's $1,500-$5,000/year for $1M+ coverage.

---

## 17. Log Collection & Monitoring

**Priority: 🟡 Medium**

- [ ] Security-relevant logs are collected centrally (SIEM, or at minimum, cloud-native logging)
- [ ] Logs are retained for at least 90 days (365 days recommended for compliance)
- [ ]

- [ ] Failed login attempts, privilege escalation, and data exports generate alerts
- [ ] Logs are stored in a location attackers cannot modify or delete

**Why it matters:** The median dwell time (time between breach and detection) is 10 days for SMBs in 2026. Without logging, you can't detect intrusions, investigate incidents, or prove compliance. When the breach happens, logs are the only way to understand what was accessed and satisfy notification requirements.

**Action:** Enable audit logging in Microsoft 365 / Google Workspace (it may not be on by default). Forward logs to a central location. Set up basic alerts for impossible travel, failed MFA, and new admin account creation.

---

## Section 7: Employee Security

### 18. Security Awareness Training

**Priority: 🟠 High**

- [ ] All employees complete security awareness training at onboarding and annually
- [ ] Training covers: phishing (including AI-generated), social engineering, physical security, reporting procedures
- [ ] Phishing simulation tests run quarterly with tracked results
- [ ] A clear, blame-free reporting process exists ("see something, say something")

**Why it matters:** Humans remain the #1 attack vector. But punitive approaches backfire — employees hide mistakes instead of reporting them. A culture where reporting a clicked phishing link is rewarded (not punished) reduces dwell time from days to minutes.

**Action:** Deploy quarterly phishing simulations. Track click rates over time (goal: under 5%). Celebrate employees who report suspicious emails. Include AI-generated deepfake awareness in training for 2026.

---

### 19. Acceptable Use & Remote Work Policy

**Priority: 🟡 Medium**

- [ ] An acceptable use policy covers company devices, personal devices (BYOD), and remote work
- [ ] Public Wi-Fi usage guidelines are documented (VPN required or equivalent)
- [ ] Data handling rules exist: what can be stored locally, what must stay in the cloud, what cannot be shared externally
- [ ] Policy is signed by all employees and reviewed annually

**Why it matters:** Remote and hybrid work is the norm in 2026. Without clear policies, employees make well-intentioned but insecure decisions: storing client data on personal Dropbox, using coffee shop Wi-Fi without VPN, sharing passwords via Slack DM.

**Action:** Write a one-page acceptable use policy. Key rules: use VPN on public networks, don't store business data on personal devices unless managed, report lost devices immediately. Keep it short and readable — nobody reads a 30-page policy.

---

## Section 8: Compliance & Governance

### 20. Data Inventory & Classification

**Priority: 🟠 High**

- [ ] You know what personal/sensitive data you collect, where it's stored, and who has access
- [ ] Data is classified (Public, Internal, Confidential, Restricted)
- [ ] Retention schedules exist — data you don't need is deleted
- [ ] Data processing agreements are in place with all vendors who handle your data

**Why it matters:** You can't protect what you don't know about. Regulatory frameworks (Australian Privacy Act, GDPR, state-level US laws) require you to account for personal data. When a breach occurs, the first question regulators ask is "what data was involved?" If you can't answer, the penalties escalate.

**Action:** Create a simple data map: what data, where stored, who accesses it, how long kept. Start with customer PII, employee records, and financial data. Delete anything you no longer need.

---

## 21. Australian Privacy Act & Essential Eight Alignment

**Priority: 🟠 High (for Australian businesses)**

- [ ] Privacy Policy is current and reflects actual data handling practices
- [ ] Notifiable Data Breach scheme obligations are understood and prepared for
- [ ] Essential Eight maturity level has been self-assessed (target: Maturity Level 2 minimum)
- [ ] If processing EU data: GDPR Data Processing Agreements are in place

**Why it matters:** The Australian Privacy Act reforms of 2025-2026 expanded obligations significantly, including a statutory tort for serious privacy breaches and increased penalties. The Essential Eight framework, while not mandatory for all businesses, is increasingly used by cyber insurers and enterprise customers as a baseline requirement.

**Action:** Self-assess against the Essential Eight using the ACSC's free tool. Focus on: application control, patching, MFA, restricting admin privileges, and backups — these five cover 85% of common attacks.

---

## 22. Vendor & Third-Party Risk Management

**Priority: 🟠 High**

- [ ] Critical vendors (IT, cloud, payroll, accounting) have been security-assessed
- [ ] Vendor contracts include security requirements and breach notification obligations
- [ ] Vendor access to your systems is reviewed quarterly and uses least-privilege principles
- [ ] You monitor vendor breach disclosures (e.g., via alerts or threat intelligence feeds)

**Why it matters:** 62% of data breaches in 2025 involved a third-party vendor (SecurityScorecard). Your security is only as strong as your weakest vendor. When your payroll provider, MSP, or CRM platform gets breached, your data is exposed regardless of your own security posture.

**Action:** List your top 10 vendors by data access. Send them a simple security questionnaire (do they have MFA? EDR? Backups? Incident response plan?). Include breach notification requirements (24-48 hours) in all new contracts.

---

## Section 9: AI & Machine Learning Security

### 23. AI Tool Governance & Data Leakage Prevention

**Priority: 🔴 Critical**

- [ ] An inventory of AI tools used by staff exists (ChatGPT, Copilot, Claude, Gemini, etc.)
- [ ] Policies define what data can and cannot be entered into AI tools
- [ ] Enterprise/business versions of AI tools are used (not free/consumer tiers) where available
- [ ] AI-generated code and content are reviewed before deployment or publication

**Why it matters:** Employees are using AI tools whether you've authorised them or not. In 2026, the risk isn't AI itself — it's employees pasting customer data, financial projections, source code, and legal documents into consumer AI tools with no data protection guarantees. Samsung, Apple, and dozens of companies have already suffered data leaks this way.

**Action:** Audit AI tool usage (check browser extensions, app installs, and network traffic). Deploy enterprise AI tools with data retention controls. Create a one-page AI acceptable use policy: never paste customer PII, passwords, API keys, or confidential business data into consumer AI tools.

---

### 24. AI-Powered Attack Awareness

**Priority: 🟠 High**

- [ ]

- [ ] Staff are trained to recognise AI-generated phishing, deepfake voice calls, and synthetic video
- [ ] Verification procedures exist for any request that involves money, access, or data — regardless of how legitimate it appears
- [ ] Security tools can detect AI-generated malicious content (email security, EDR with AI detection)

**Why it matters:** AI has collapsed the skill barrier for attackers. In 2026, a $20/month AI subscription lets anyone generate convincing phishing emails in any language, clone a CEO's voice from a podcast appearance, and create deepfake video for social engineering. The volume of AI-generated attacks has increased 1,400% since 2024.

**Action:** Add deepfake/AI awareness to your security training. Establish out-of-band verification for all high-value requests (separate channel, code word, in-person confirmation). Ensure your email security solution flags AI-generated content.

---

## 25. AI Agent & Automation Security

**Priority: 🟡 Medium (🔴 Critical if you deploy AI agents)**

- [ ] AI agents/automations operate under least-privilege access (no admin rights)
- [ ] AI agent actions are logged, auditable, and reviewable
- [ ] Human-in-the-loop approval exists for any AI action with real-world consequences (sending emails, modifying data, making purchases)
- [ ] AI agent credential storage is secured (not hardcoded, rotated regularly)

**Why it matters:** AI agents — autonomous software that takes actions on your behalf — are the fastest-growing attack surface in 2026. A compromised AI agent with broad permissions can exfiltrate data, send phishing emails from legitimate accounts, and modify financial records at machine speed. Rogue AI agents operating without oversight have already caused significant incidents.

**Action:** Audit all AI agents and automations in your environment (Zapier, Make, Power Automate, custom scripts). Apply least-privilege: each agent should only have access to the specific resources it needs. Implement approval workflows for any action that modifies data or sends external communications.

## Scoring Your Security Posture

Count your checked items:

| Score | Rating | Recommendation |
|---|---|---|
| 22-25 | 🟢 **Strong** | You're ahead of 90% of SMBs. Focus on continuous improvement and testing. |
| 17-21 | 🟡 **Good Foundation** | Core controls are in place. Close the gaps this quarter. |
| 12-16 | 🟠 **Needs Attention** | Significant gaps exist. Prioritise 🔴 Critical items immediately. |
| 0-11 | 🔴 **At Risk** | Your business is highly vulnerable. Consider professional assessment. |

## Next Steps

1. **Complete the checklist** — be honest about your current state
2. **Prioritise 🔴 Critical items** — these should be addressed this week
3. **Schedule 🟠 High items** — target completion within 30 days
4. **Plan 🟡 Medium items** — complete within the quarter
5. **Reassess quarterly** — threats evolve, so should your defences

### Need Help?

**Book a free 30-minute security assessment** with lilMONSTER. We'll walk through this checklist with your actual systems and build a prioritised remediation plan.

→ https://lil.business/consult/



*Last updated: March 2026 | Next review: June 2026*