HORIZONSHIELD

Securing Your Digital Future, Today.

SMB & BUSINESS SECURITY · BOOK 01 OF 16

The SMB Cybersecurity Guide 2026

Practical Security for Every Business

A no-jargon field guide built on real-world Tier-1 financial institution experience — now accessible to every business. From threat landscape to 30-day action plans, identity security, email hardening, backup strategy, and incident response.

CHAPTERS	CONTROLS	STANDARD	LEVEL
10	150+	CIS v8	All

Contents

SMB CYBERSECURITY GUIDE 2026

CHAPTER 01

Why SMBs Are Prime Targets

The most dangerous belief in SMB security is "we are too small to be a target." This belief is precisely what makes you attractive.

THREAT INTEL | STATISTICS | SUPPLY CHAIN

The Uncomfortable Truth

Small and medium businesses represent **43% of all cyberattack targets globally** — yet fewer than 14% have a documented incident response plan. Automated attack tools do not read your revenue reports. They scan millions of IP addresses simultaneously, identifying paths of least resistance.

43%
SMB SHARE OF ALL ATTACKS
Verizon DBIR 2025

$4.88M
AVERAGE BREACH COST 2025
IBM Security

60%
SMBS CLOSE WITHIN 6 MONTHS
NCSA Research

194
DAYS AVG TO DETECT BREACH
Without monitoring

Why SMBs Are Targeted Systematically

Attack Factor	Why It Attracts Attackers	Enterprise Comparison
Zero dedicated security staff	78% of SMBs have no dedicated security personnel — IT generalists manage security as a secondary task	Enterprises have 50–500 dedicated security professionals
Minimal security budget	Average SMB security spend: $15K/year. Covers basic AV at best.	Enterprises spend $2.4M+ annually on security tools alone
Manual patch management	Updates applied weeks after release. No automated patch pipeline.	Automated patching with 24–48hr SLAs for critical CVEs

Attack Factor	Why It Attracts Attackers	Enterprise Comparison
No monitoring	No SIEM, no EDR telemetry, no alerting. Breaches discovered by customers.	24/7 SOC with SIEM, EDR, and automated alerting
No incident response plan	First response improvised under crisis pressure	Tested IR playbooks, retained IR firms, cyber insurance

SUPPLY CHAIN REALITY

Sophisticated threat actors compromise smaller businesses in supply chains — using them as trusted entry points into harder targets. If you provide services to larger organisations, a breach at your firm exposes your clients. Enterprise clients hold vendors contractually liable. Being secure is now a competitive differentiator.

Industry Risk Profiles 2026

Industry	Primary Attack	Avg Loss	Regulatory Exposure
Professional Services (Legal, Accounting)	BEC + Data theft via spear phishing	$185,000	GDPR, professional conduct rules
Healthcare SMB (Clinics, Dental)	Ransomware targeting patient records	$310,000	HIPAA ($10K-$50K per violation)
Retail & E-Commerce	Card skimming, credential stuffing	$95,000	PCI-DSS fines + card brand penalties
Manufacturing	OT/ICS ransomware, production stoppage	$420,000	NIS2, sector-specific regulations
Financial Services SMB	BEC wire fraud, insider threat	$275,000	FCA, DORA, state banking regulations
Technology / MSP	Supply chain, client data theft	$525,000	Client contract liability + GDPR

The Ransomware Kill Chain

Ransomware operators spend an average of 14 days inside SMB networks before detonating ransomware. Understanding this timeline reveals intervention opportunities at every phase.

1

Reconnaissance

DAYS TO WEEKS BEFORE ATTACK

Entirely passive — attackers research your business using LinkedIn, Hunter.io, Shodan, and job postings. They identify employee names, email formats, technology stack, and exposed services. You have zero visibility into this phase.

2

Initial Access

DAY ZERO

68% of SMB breaches start with phishing. Other vectors: unpatched VPN/RDP exposed to internet, and credential reuse from previous breaches ($5-10 for 1000 username/password pairs on dark web markets).

3

Establish & Persist

DAYS 0–7

Attacker deploys multiple backdoors, disables security tools, creates new admin accounts, and begins lateral movement using Pass-the-Hash, Kerberoasting, and credential dumping techniques. All silently.

4

Discovery & Staging

DAYS 7–14

Silent mapping of your entire network. Critical systems identified. Backup servers located (targeted first for destruction). Domain admin credentials stolen. Data exfiltration begins for double-extortion.

5

Impact

D-DAY

Ransomware deployed simultaneously across all systems. Backup servers destroyed first. Average ransom demand for SMBs: $247,000. Double extortion: pay for decryption AND pay to prevent publication of stolen data.

BACKUPS ARE NO LONGER SUFFICIENT ALONE

73% of ransomware attacks in 2025 affected backup systems. Modern ransomware specifically identifies and destroys online backups before encrypting production data. Your

backup MUST be: (1) OFFLINE — air-gapped or object-locked immutable, (2) ENCRYPTED — ransomware cannot read stolen backup data, (3) REGULARLY TESTED — a backup never successfully restored from is not a backup.

The Business Email Compromise Threat

BEC Type	Method	Average Loss	Primary Defence
CEO Fraud / Wire Transfer	Impersonate CEO — request urgent wire to new account	$137,000	Verbal confirmation policy for ALL wire transfers
Vendor Invoice Fraud	Compromise vendor email, change bank account in invoice	$89,000	Call known number to verify ANY account change
Attorney Impersonation	Impersonate legal counsel during M&A or litigation	$185,000	Never send funds based solely on attorney email
Payroll Diversion	Impersonate employee to HR — change direct deposit	$45,000	Verify all payroll changes via separate channel
Gift Card Fraud	Impersonate executive — request gift card purchase	$3,000	Gift cards are NEVER a legitimate business payment

CHAPTER 03

The 30-Day Security Sprint

High-impact, low-cost actions prioritised by real-world risk reduction. 80% of your breach risk comes from 20% of vulnerability categories.

ACTION | QUICK WINS | FREE TOOLS

Week-by-Week Action Plan

Week	Day	Action	Risk Eliminated	Time	Cost
1	1-2	Enable MFA on ALL email — authenticator app, not SMS	Eliminates 99.9% of account takeover	2hrs	Free
1	3	Audit ALL user accounts — disable inactive, remove ex-employees	Eliminates dormant account exploitation	2hrs	Free
1	4-5	Deploy password manager (Bitwarden Teams) — enforce use	Eliminates password reuse — root cause of 80%+ account takeovers	3hrs	$3/user/mo
1	6-7	Enable automatic updates on all devices — OS, browser, Office	Eliminates 85% of known vulnerability exploitation	1hr	Free
2	8-9	Deploy offline/immutable backup — test restore on day 9	Makes ransomware a recovery exercise, not catastrophe	3hrs	$100-200/yr
2	10-11	Enable DNS filtering — Cloudflare Zero Trust (free)	Blocks 85% of malware/phishing at DNS layer	1hr	Free
2	12-13	Change ALL default passwords — routers, switches, cameras	Eliminates trivial automated exploitation	2hrs	Free

Week	Day	Action	Risk Eliminated	Time	Cost
2	14	Audit email forwarding rules — remove unauthorized auto-forwards	Detects existing BEC compromise immediately	1hr	Free
3	15-17	Firewall audit — close unused ports, enable outbound logging	Limits lateral movement blast radius	3hrs	Free
3	18-20	Deploy EDR on ALL endpoints (Microsoft Defender for Business)	Detects and blocks malware execution	4hrs	$5-8/device/mo
4	21-23	Run phishing simulation — measure click rate, train failures	Identifies highest-risk individuals	2hrs	$200
4	24-25	Test backup restoration end-to-end with real file recovery	Confirms backups work before you need them	2hrs	Free
4	26-27	Configure DMARC p=reject — prevent domain spoofing	Prevents impersonation of your domain in phishing	1hr	Free
4	28-30	Document IR contacts, print and post. Create security baseline.	Ensures correct actions under crisis pressure	2hrs	Free

Free & Low-Cost SMB Security Stack

FREE

Cloudflare Zero Trust DNS

DNS-layer protection blocking malware, phishing, and C2 traffic. Set DNS to 1.1.1.2 (malware blocking) or configure full Zero Trust DNS gateway. 15-minute setup. Processes 1.7T queries/day.

$3/USER/MO

Bitwarden Teams

Open-source, independently audited password manager. Browser extension, mobile app, secure vault sharing, admin console. Eliminates password reuse — root cause of 80%+ account takeovers.

$5/DEVICE/MO

Microsoft Defender for Business

EDR, next-gen AV, firewall management, attack surface reduction. Integrates with M365. Best value endpoint security for SMBs with automated investigation and response.

CHAPTER 04

Identity & Access Management

Identity is the new perimeter. Over 80% of data breaches involve compromised credentials. This is your highest-ROI security investment.

MFA PASSWORDS PAM ZERO TRUST

MFA — Implementation Guide

MFA Method	Security	Phishing Resistant	User Friction	Recommended Use
FIDO2 / Passkeys (YubiKey, Face ID)	VERY HIGH	YES — cryptographically bound	LOW — tap or biometric	Default for all staff — best security and UX
Authenticator App TOTP (Google/Authy)	HIGH	PARTIAL	LOW-MEDIUM	Standard for staff if passkeys unavailable
Push Notification with number matching	HIGH	PARTIAL — fatigue risk without matching	LOW	M365, Google Workspace, SaaS apps
SMS OTP	MEDIUM	NO — SIM-swappable	LOW	Last resort legacy fallback only — avoid
Email OTP	LOW	NO	MEDIUM	Avoid — email often less secure than what you protect

MFA FATIGUE ATTACKS — GROWING FAST

Attackers flood users with push notifications hoping they approve accidentally. 35% of MFA bypasses in 2025 used this technique. Defence: Enable number matching (user types code

shown on login into push), enable location context, and lock account after 3 failed MFA attempts.

Password Policy 2026

Parameter	Minimum	Recommended	Rationale
Minimum length	12 characters	16+ characters	Length is the primary driver of password security
Complexity	Not required if 16+ chars	Passphrase preferred	Long passphrases beat complex short passwords
Expiry policy	Only on suspected compromise	No regular forced expiry	Regular expiry drives weak predictable patterns
Breach checking	Recommended	Required — block known-breached passwords	Prevent use of passwords found in breach databases
Password manager	Encouraged	Required for all staff	Eliminates reuse without memorisation burden
Admin account separation	Required	Required	Admin accounts never used for email or browsing

Privileged Access Management

- **Separate admin accounts:** IT admins must have two accounts — daily-use account (email, browsing) and a separate admin account used only for admin tasks. Admin accounts never used for email.
- **Just-In-Time (JIT) access:** Grant elevated privileges only when needed, with automatic expiry. Eliminates standing privileged access.
- **No shared admin credentials:** Every administrator has their own named account. Shared passwords make post-breach investigation impossible.
- **Break-glass accounts:** Emergency access stored in sealed envelope in physical safe. Every use triggers alert and post-use review.
- **Quarterly access reviews:** Review all privileged account assignments. Remove access for role-changers and departures immediately.

```
# Azure Entra ID — Block Legacy Authentication (Conditional Access)
# Legacy auth (SMTP AUTH, POP3, IMAP, MAPI) bypasses MFA entirely
# Block via Conditional Access:
# Policy: Block Legacy Authentication
# Assignments → Users: All Users
# Conditions → Client apps: Check 'Exchange ActiveSync clients' AND 'Other clients'
# Grant: Block Access
```

```
# Verify legacy auth usage before blocking:
Get-AzureADAuditSignInLogs | Where-Object {$_.clientAppUsed -match 'SMTP|POP3|IMAP|MAPI'} |
Select-Object userDisplayName, clientAppUsed, ipAddress | Sort-Object -Unique
```

CHAPTER 06

Email Security — DMARC, SPF & DKIM

91% of all cyberattacks start with a phishing email. A properly configured email authentication stack prevents domain spoofing entirely.

SPF DKIM DMARC FILTERING

Email Authentication — SPF, DKIM, DMARC

Without email authentication, anyone can send email claiming to be from your domain. DMARC p=reject combined with SPF and DKIM makes domain spoofing virtually impossible.

```
# STEP 1: SPF — List authorised mail servers
# Add TXT record to DNS:
# Name: @ (yourdomain.com)
# Value: "v=spf1 include:_spf.google.com include:sendgrid.net -all"
# -all = FAIL all other senders (strict)

# STEP 2: DKIM — Cryptographic signature on outbound email
# Google Workspace: Admin → Apps → Gmail → Authenticate Email → Generate key
# Microsoft 365: Admin Center → Exchange → Email Auth → DKIM → Enable

# STEP 3: DMARC — Enforcement policy
# Add TXT record to DNS:
# Name: _dmarc.yourdomain.com
# Value: "v=DMARC1; p=reject; rua=mailto:dmarc@yourdomain.com; fo=1"
# Start with p=none (monitoring), then p=quarantine, then p=reject

# Verify: mxtoolbox.com/dmarc.aspx
# Target: SPF=pass, DKIM=pass, DMARC=pass with p=reject
```

Filter Setting	M365 Setting	Google Workspace	Risk Blocked
Block executable attachments	.exe .vbs .js .bat .ps1 .hta — quarantine	Advanced Security → Block file types	Malware via attachment — 40% of delivery

Filter Setting	M365 Setting	Google Workspace	Risk Blocked
			method
Safe Links	Defender for O365 → Safe Links	Gmail link protection	Drive-by download links in email body
Attachment sandboxing	Safe Attachments → Dynamic Delivery	Enable sandbox for unknown attachments	Zero-day malware not caught by signature AV
External sender warning	Add [EXTERNAL] banner via mail flow rules	External warning banner	Impersonation and spoofing awareness
Anti-spoofing	Anti-phishing → Enable antispoofing	Email impersonation protection	Display name impersonation
BEC / impersonation detection	Anti-phishing → Impersonated users/domains list	CEO/VIP impersonation detection	Targeted BEC against your organisation

SINGLE MOST IMPACTFUL EMAIL ACTION

Configure DMARC p=reject for your domain. This prevents any attacker from sending email appearing to come from your domain — eliminating domain-spoofing phishing against your clients and partners. 30 minutes to configure. Protects both you and everyone who receives email from your domain.

CHAPTER 08

Backup & Disaster Recovery

When all controls fail, your backup determines whether you recover. The 3-2-1-1-0 rule in 2026.

3-2-1-1-0 | OFFLINE | IMMUTABLE | TESTED

The 3-2-1-1-0 Backup Rule

Rule	Requirement	Why Critical	Implementation
3 copies	At least 3 copies of your data	Single copy has no redundancy	Production + backup server + offsite
2 different media	2 different storage types	Same media has batch failure risk	Disk + cloud, or disk + tape
1 offsite	1 copy physically separate from primary	Fire/flood/theft destroys same-location copies	Cloud backup or drive at different location
1 offline/immutable	1 copy completely disconnected or immutable	Online backups deletable by ransomware	Air-gapped drive, or Object Lock immutable cloud storage
0 errors	Last restore test shows zero errors	Untested backups fail in crisis	Monthly restore tests — spot-check specific files quarterly

IF YOU HAVE NEVER TESTED YOUR RESTORE, YOU DO NOT HAVE A BACKUP

42% of organisations that paid ransomware in 2025 discovered backups were corrupted or inaccessible during recovery. The attacker checked your backup integrity before encrypting. Answer "do our backups work?" BEFORE a crisis.

RTO/RPO Planning by System Tier

System Tier	Priority	Target RTO	Target RPO	Backup Frequency
Critical — Revenue systems (payments, orders)	Tier 1	< 4 hours	< 1 hour	Every 15-60 minutes — continuous replication
Critical — Core ops (email, ERP, file servers)	Tier 1	< 8 hours	< 4 hours	Every 4 hours — incremental
Important — Internal tools (HR, CRM, project)	Tier 2	< 24 hours	< 8 hours	Daily full with weekly verification
Standard — Dev/test, non-production	Tier 3	< 72 hours	< 24 hours	Daily or weekly
Archive — Historical data, compliance records	Tier 4	< 7 days	< 24 hours	Daily incremental

Backup Testing Protocol

1. **Weekly:** Verify backup jobs completed — check dashboard for errors, spot-restore 1-2 specific files
2. **Monthly:** Full file-level restore of a complete folder to test environment, verify data integrity
3. **Quarterly:** Full system recovery of one critical server to test environment, measure actual vs target RTO
4. **Annually:** Full disaster recovery drill — simulate primary site failure, recover all critical systems, update runbooks

CHAPTER 09

Incident Response

When — not if — a security incident occurs. A documented, tested IR plan is the difference between a recoverable event and a business-ending one.

CONTAIN | ERADICATE | RECOVER | NOTIFY

6-Phase Incident Response

1

Identify — Confirm the Incident

T+0 TO T+15 MINUTES

Confirm the incident is real. Classify severity. Assign ONE incident commander — decision authority must be singular. Open secure communication channel OUTSIDE potentially compromised systems (Signal, WhatsApp, phone). Never use email/Slack if they may be compromised.

2

Contain — Stop the Spread

T+15 TO T+60 MINUTES

Isolate affected systems IMMEDIATELY — unplug ethernet (faster than software). Disable WiFi. Segment network at switch level if lateral movement suspected. Disable compromised user accounts. Block attacker infrastructure at firewall. Preserve memory before powering off.

3

Eradicate — Remove the Threat

T+1 TO T+48 HOURS

Remove ALL malware, backdoors, and persistence — not just the visible ransomware payload. Attackers install multiple backdoors. Reset ALL potentially compromised credentials. Patch the exploited vulnerability before reconnecting systems.

4 Recover — Restore Operations

T+24 TO T+72 HOURS

Restore from VERIFIED CLEAN backups. Test restored systems in isolation before reconnecting. Monitor closely for recurrence — attackers return within 30 days in 40% of cases. Restore critical systems first per your RTO tiers.

---

5 Notify — Legal Obligations

T+1 TO T+72 HOURS (PARALLEL)

Notify cyber insurance immediately. Engage legal counsel for notification obligations. GDPR: 72-hour notification to supervisory authority. HIPAA: 60 days. PCI-DSS: immediately. File FBI IC3 report for ransomware or BEC.

---

6 Improve — Root Cause Fix

POST-INCIDENT

Fix the initial access vector permanently. Conduct lessons-learned session. Update IR playbooks. Schedule follow-up penetration test within 90 days. Brief board/leadership on findings and cost.

EMERGENCY CONTACT CARD — PRINT THIS AND POST IT

Insurance provider 24/7 claims line (number on your policy). FBI IC3: ic3.gov. Bank fraud hotline (wire recalls succeed 70% if called within 24 hours, drop to <10% after). Legal counsel mobile. HorizonShield Emergency IR: support@horizonshield.net. Have these before you need them.

H O R I Z O N S H I E L D

Securing Your Digital Future, Today.

The SMB Cybersecurity Guide 2026

Part of the HorizonShield Security Series — 16 comprehensive professional cybersecurity manuals covering every domain of modern enterprise security.