SMB Ransomware Resilience Checklist: A Milestone Roadmap With (and Without) Your MSP

Ransomware continues to rank among the most disruptive—and costly—threats facing small and mid-size enterprises. A single compromised endpoint or cloud tenant can halt operations, erode customer confidence, and trigger regulatory obligations in a matter of hours. Yet effective safeguards need not be complex or prohibitively expensive.

The **SMB Ransomware Resilience Checklist** distils proven security practices into sequential milestones. The first section outlines governance measures every organisation can implement internally; the second specifies the technical controls that a managedservice provider (MSP) should deliver and document. By completing each milestone in turn, leadership gains clear visibility into progress, ensures accountability for external partners, and establishes a layered defence capable of withstanding modern ransomware attacks.

If you manage your IT environment, processes and tools.

Milestone (duration)		Actions	Outcome	
1	**Know What You're Protecting (≈ 1 week)**	1. Map your "crownjewel" data – list every place critical documents live, including SaaS applications and APIs with access to critical data. 2. Publish a one-page security & acceptable use and backup policy in plain language.	*Shared visibility and clear ground rules.*	☐ ☐
2	**Lock Down Identity (≈ 1 week)**	1. Turn on multifactor authentication (MFA) everywhere. 2. Create separate, least-privilege administrative accounts secured with MFA (FIDO2/WebAuthn). 3. Enable Google's 2SV or O365's Conditional policies to protect from suspicious access.	*Even stolen passwords won't open the front door.*	☐ ☐ ☐

		4. Disable inactive accounts (30-day threshold). 5. Implement privileged access workstations (PAWs) for IT admins.		☐ ☐
3	**Basic Hygiene at Scale (≈ 1–2 weeks)**	1. Enable automatic patching for operating systems, browsers, and major business apps. 2. Patch network devices (firewalls, switches) and IoT firmware. 3. Use configuration management tools (e.g., Ansible, Puppet) to enforce secure baselines across endpoints and servers	*Closes the most known holes before attackers can exploit them.*	☐ ☐ ☐
4	**Protect & Prune Your Data (≈ 2 weeks)**	1. Back up cloud and onprem data to a second, immutable location and encrypt backup. 2. Run a small restore test (files + mailbox) to prove it works. 3. Reduce or autoexpire external sharing links in M365/Google Workspace. 4. Enable activity logging for backups to detect unauthorized access or modifications	*Even if data is encrypted or leaked, you still have a clean copy—and less of it is exposed.*	☐ ☐ ☐ ☐
5	**Stop Malware at the Endpoint (≈ 2 weeks)**	1. Deploy modern endpoint protection / EDR on every laptop and server. 2. Enable application allowlisting (e.g., AppLocker). 3. Enable behaviour-based detection in endpoint protection tools to catch zero-day threats (Carbon Black, Microsoft Defender)	*ransomware is detected or blocked before it can detonate.*	☐ ☐ ☐
6	**Be Ready When Trouble Strikes (≈ 1 week)**	1. Build a onepage incidentresponse cheatsheet and drill it quarterly.	*Everyone knows who to call and what to do under stress.*	☐

		2. Store offline copies of IR contacts, backups, and network diagrams. 3. Pre-arrange a ransomware response contract with a specialist firm.		☐ ☐
7	**Transfer the Residual Risk (as part of annual renewal)**	1. Review and purchase cyberinsurance that explicitly covers ransomware (verify backup & MFA requirements). 2. Verify insurance covers ransom payments (if legal) and regulatory fines, not only response and remediation cost.	*Financial backstop for costs you can't eliminate technically.*	☐ ☐
8	**Extra (≈ 1 week)**	1. Add email & DNS filtering to block malicious links and macro payloads. 2. Deploy canary tokens in critical folders to detect ransomware early. 3. Monitor for data exfiltration.	*Ransomware is detected or blocked before it can detonate.*	☐ ☐ ☐

If you outsourced your IT environment, processes and tools to service provider.

Milestone (duration)		Actions	Outcome	
Your milestones				
1	**Know What You're Protecting** *(≈ 1 week)*	1. Map your "crown jewel" data – list every place critical documents live. 2. Publish a one page security & acceptable use and backup policy in plain language. 3. Require MSP to document shared responsibility matrix (RACI).	*Shared visibility and clear behavioral rules.*	☐ ☐ ☐
2	**Be Ready When Trouble Strikes** *(≈ 1 week)*	1. Draft a Backup & Restoration Policy that sets RPO/RTO and legal hold needs. 2. Write a one page Incident Response Plan with phone tree; calendar quarterly joint drills.	*Documented expectations for the MSP and a rehearsed plan if ransomware strikes.*	☐ ☐

		3. Define ransomware communication protocols (e.g., who talks to law enforcement?). 4. Require MSP to provide forensic investigation SLA (e.g., 4-hour response).		☐ ☐
3	**Sharpen Staff Senses** *(≈ 1 week)*	1. Launch rolling security awareness: monthly phish tests + annual refresher. 2. Automatically insert a banner on emails that come from outside the company, so staff can instantly spot external senders. 3. Train staff to report MSP remote access abuse (common ransomware vector).	*Fewer risky clicks and faster reporting of weird activity*	☐ ☐ ☐
4	**Transfer & Contract** *(≈ 1 week, at renewal)*	1. Purchase / renew cyber insurance with explicit ransomware cover. 2. Embed your policies (1 to 3) and evidence requirements into the MSP SLA. 3. Require MSP to comply with CIS Controls or NIST CSF and have independent audits (SOC 2, ISO 27001).	*Financial back-stop and contractual leverage to keep controls in force*	☐ ☐ ☐
Service provider milestones				
1	**Secure Identity** *(≈ 1 month)*	1. Enforce MFA for every account. 2. Create separate least privilege admin IDs. 3. Disable legacy protocols (IMAP/POP, SMB v1, etc.). 4. Implement just-in-time (JIT) admin access (e.g., PIM in Azure AD).	*Identity hardened; even stolen passwords won't open the front door.*	☐ ☐ ☐ ☐
2	**Patch & Protect** *(≈ 1-2 months)*	1. Turn on automatic OS, application, and firmware patching. 2. Deploy endpoint protection / EDR to 100 % of devices.	*Known holes closed and malware watched.*	☐ ☐

		3. Enforce EDR/XDR with 24/7 managed detection (e.g., Sentinel One, Huntress, Vigilance)		☐
3	**Back Up & Validate** *(≈ 2 months)*	1. Configure immutable, off tenant backups for cloud and servers. 2. Perform a test restore (files + mailbox) and document results. 3. Test full-environment restore (not just files) bi-annually.	*Clean, recoverable data if ransomware strikes.*	☐ ☐ ☐
4	**Harden Data Access** *(≈ 2-3 months)*	1. Restrict external sharing defaults and auto expire new links. 2. Review and prune third-party SaaS / OAuth applications.	*Lower data leak surface.*	☐ ☐
5	**Network & Edge Security** *(≈ 3 months)*	1. Patch firewalls and routers; enable geo IP & DNS filtering. 2. Segment the network (staff, guest, printers). 3. Deploy micro segmentation for critical systems (e.g., OT/IoT). Block RDP/SMB over the internet (use VPN/ZTNA instead)	*Perimeter attacks blocked and lateral movement curtailed.*	☐ ☐ ☐
6	**Detect & Report** *(≈ 3 months, onward monthly)*	4. Forward logs to a SIEM/SOC and monitor 24 × 7. 5. Monitor for C2 beaconing (e.g., DNS tunneling, HTTPS anomalies, Proxy usage) 6. Send a monthly security metrics email to the customers.	*Continuous visibility and measurable assurance.*	☐ ☐ ☐
7	**Drill & Attest** *(≈ Quarterly / Annually)*	7. Participate in the quarterly incident response drill. 8. Sign an annual control attestation letter for cyber insurance.	*Readiness proven and policy compliance maintained.*	☐ ☐