SMB RANSOMWARE-RESILIENCE CHECKLIST
A MILESTONE ROADMAP WITH /AND WITHOUT YOUR MSP

WITH YOUR MSP

SMB RANSOMWARE-RESILIENCE CHECKLIST

Know What You're Protecting (≈ 1 week)

Action	Outcome
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. Document SaaS apps and APIs with access to critical data. Identify shadow IT using network scans or CASB tools.[t1] i Map dependencies between systems and applications to understand cascading effects during an attack [t1]Important	shared visibility and clear ground rules.

SMB RANSOMWARE-RESILIENCE CHECKLIST

Lock Down Identity (≈ 1 week)

Action	Outcome
3.Turn on multifactor authentication (MFA) everywhere. 4.Create separate, least-privilege admin accounts for IT tasks.	Even stolen passwords won’t open the front door.
5.Enable Google’s 2SV or O365’s Conditional policies to protect from suspicious access. Enforce phishing-resistant MFA (FIDO2/WebAuthn) for admins. Implement privileged access workstations (PAWs) for IT admins. Disable inactive accounts (30-day threshold). Implement role-based access control (RBAC)-Least privilege access	

SMB RANSOMWARE-RESILIENCE CHECKLIST

Basic Hygiene at Scale (≈ 1–2 weeks)

Action	Outcome
6.Enable automatic patching for operating systems, browsers, and major business apps. Patch network devices (firewalls, switches) and IoT firmware. Use vulnerability scanning (e.g., Nessus, OpenVAS) monthly Use configuration management tools (e.g., Ansible, Puppet) to enforce secure baselines across endpoints and servers	closes most known holes before attackers can exploit them.

SMB RANSOMWARE-RESILIENCE CHECKLIST

Protect & Prune Your Data (≈ 2 weeks)

Action	Outcome
7. Back up cloud and on-prem data to a second, immutable location. 8. Run a small restore test (files + mailbox) to prove it works. 9. Reduce or auto-expire external sharing links in M365/Google Workspace. Enable versioning and recycle bins in cloud storage. Encrypt backups and test decryption (avoid backup ransomware). Classify data (PII, financial) and restrict access via DLP policies. 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.

SMB RANSOMWARE-RESILIENCE CHECKLIST

Stop Malware at the Endpoint (≈ 2 weeks)

Action	Outcome
10. Deploy modern endpoint protection / EDR on every laptop and server. Enable application allowlisting (e.g., AppLocker). • Disable macros in Office files (or restrict to signed macros). • Deploy LAPS (Local Admin Password Solution) for on-prem devices 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.

SMB RANSOMWARE-RESILIENCE CHECKLIST

Be Ready When Trouble Strikes (≈ 1 week)

Action	Outcome
11. Build a one-page incident-response cheat-sheet and drill it quarterly. Pre-negotiate ransomware negotiation/response retainer with a third party. Store offline copies of IR contacts, backups, and network diagrams.	Everyone knows who to call and what to do under stress.

SMB RANSOMWARE-RESILIENCE CHECKLIST

Transfer the Residual Risk (as part of annual renewal)

Action	Outcome
12. Review and purchase cyber-insurance that explicitly covers ransomware (verify backup & MFA requirements). Verify insurance covers ransom payments (if legal) and regulatory fines. Require MSP cyber insurance if they handle your data.	Financial backstop for costs you can't eliminate technically.

SMB RANSOMWARE-RESILIENCE CHECKLIST

Extra (≈ 1 week)

Action	Outcome
13.Add email & DNS filtering to block malicious links and macro payloads Deploy canary tokens in critical folders to detect ransomware early. Monitor for data exfiltration (unusual outbound traffic).	Ransomware is detected or blocked before it can detonate.

SMB RANSOMWARE-RESILIENCE CHECKLIST
A MILESTONE ROADMAP WITH /AND WITHOUT YOUR MSP

WITHOUT YOUR MSP

NO SMB RANSOMWARE-RESILIENCE CHECKLIST

Know What You're Protecting (≈ 1 week)

Action	Outcome
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. Require MSP to document shared responsibility matrix (RACI).	Shared visibility and clear behavioural rules.

NO SMB RANSOMWARE-RESILIENCE CHECKLIST

Be Ready When Trouble Strikes (≈ 1 week)

Action	Outcome
4.Draft a Backup & Restoration Policy that sets RPO/RTO and legal-hold needs.	Documented expectations for the MSP and a rehearsed plan if ransomware strikes.
5.Write a one-page Incident-Response Plan with phone tree; calendar quarterly joint drills. Define ransomware communication protocols (e.g., who talks to law enforcement?). Require MSP to provide forensic investigation SLA (e.g., 4-hour response).	

NO SMB RANSOMWARE-RESILIENCE CHECKLIST

Sharpen Staff Senses (≈ 1 week)

Action	Outcome
6.Launch rolling security-awareness: monthly phish tests + annual refresher.	Fewer risky clicks and faster reporting of weird activity
7.Automatically insert a banner on emails that come from outside the company, so staff can instantly spot external senders. Train staff to report MSP remote access abuse (common ransomware vector).	

NO SMB RANSOMWARE-RESILIENCE CHECKLIST

Transfer & Contract (≈ 1 week, at renewal)

Action	Outcome
8.Purchase/renew cyber-insurance with explicit ransomware cover.	Financial back-stop and contractual leverage to keep controls in force
9.Embed your policies (1 to 3) and evidence requirements into the MSP SLA. Require MSP to comply with CIS Controls or NIST CSF. Mandate third-party audits (SOC 2, ISO 27001) for MSP. Mandate Regular Pentest	

SERVICE PROVIDER MILESTONES

Secure Identity (≈ 1 month)

Action

- Enforce MFA for every account.
- Create separate least-privilege admin IDs.
- Disable legacy protocols (IMAP/POP, SMB v1, etc.).
- Implement just-in-time (JIT) admin access (e.g., PIM in Azure AD).

Outcome

Identity hardened; even stolen passwords won't open the front door.

SERVICE PROVIDER MILESTONES

Patch & Protect (≈ 1-2 months)

Action

- Turn on automatic OS, application, and firmware patching.
- Deploy endpoint protection / EDR to 100 % of devices.
- Enforce EDR/XDR with 24/7 managed detection (e.g., SentinelOne,Huntress, Vigilance)

Outcome

Known holes closed and malware watched.

SERVICE PROVIDER MILESTONES

Back Up & Validate (≈ 2 months)

Action

- **Configure immutable, off-tenant backups for cloud and servers.**
- **Perform a test restore (files + mailbox) and document results.**
- **Test full-environment restore (not just files) annually.**

Outcome

Clean, recoverable data if ransomware strikes.

SERVICE PROVIDER MILESTONES

Harden Data Access (≈ 2-3 months)

Action

- Restrict external-sharing defaults and auto-expire new links.
- Review and prune third-party SaaS / OAuth applications.

Outcome

Lower data-leak surface.

SERVICE PROVIDER MILESTONES

Network & Edge Security (≈ 3 months)

Action

- Patch firewalls and routers; enable geo-IP & DNS filtering.
- Segment the network (staff, guest, printers).
- Deploy microsegmentation for critical systems (e.g., OT/IoT).
- Block RDP/SMB over the internet (use VPN/ZTNA instead)

Outcome

Perimeter attacks blocked and lateral movement curtailed.

SERVICE PROVIDER MILESTONES

Detect & Report (≈ 3 months, onward monthly)

Action

- Forward logs to a SIEM/SOC and monitor 24 × 7.
- Send a monthly security-metrics email to the customers.
- Monitor for C2 beaconing (e.g., DNS tunneling, HTTPS anomalies,Proxy usage)

Outcome

Continuous visibility and measurable assurance.

SERVICE PROVIDER MILESTONES

Drill & Attest (≈ Quarterly / Annually)

Action

- Participate in the quarterly incident-response drill.
- Sign an annual control-attestation letter for cyber-insurance.

Outcome

Readiness proven and policy compliance maintained.