The 90-Day Cyber Resilience Playbook

Detailed Instructions to Help Mid-Sized Businesses Build Real Operational Resilience

Contents

Overview

This guide to building your own 90-Day Cyber Resilience Playbook, offers step-by-step instructions to help organizations turn visibility into ownership, and ownership into sustainable operational readiness. Each phase outlines not only what to do, but how to do it, so you can make meaningful progress every week.

Phase 1: Gain Visibility (Weeks 1–4)

1. Identify 5–10 Business-Critical Systems:

- Review core business processes (e.g. invoicing, order fulfillment, client services).
- List systems that support those processes—whether cloud, on-prem, or vendor-provided.
- Prioritize based on revenue impact, compliance, or reputational risk.

2. Map Internal and External Dependencies:

- Identify who uses each system, both inside and outside your company.
- Include service providers and upstream/downstream data flows.

3. Evaluate Monitoring, Backup, and Shared Access:

- Check if each system has real-time alerts, and verify the last successful backup.
- Flag systems using shared credentials—note who has access.

4. Interview Frontline Staff:

- Ask: “If this system failed, what would you do?”
- Capture unofficial workarounds and communication paths.

5. Build a Resilience Priority Grid:

- Create a 2x2 grid: Impact (High/Low) vs. Visibility (High/Low).
- Focus on High Impact / Low Visibility systems first.

6. Create a Role Map:

- Assign ownership of each system’s operation and fallback process.
- Use a simple table with system, owner, backup owner, contact details.

Phase 2: Take Ownership (Weeks 5–8)

1. Assign Fallback Plan Owners:

- For each red-zone system, assign a fallback plan owner.
- Ensure they understand their role in an outage scenario.

2. Draft One-Page Fallback Plans:

- Include: Trigger (when to activate), Action Steps (3–5 bullets), Communications (who to notify).
- Keep it simple and printable.

3. Run a Dry Run Tabletop:

- Choose one high-risk scenario.
- Gather the fallback owner, IT, ops, and comms.
- Simulate an incident for 20–30 minutes. Document gaps.

4. Capture and Fix Gaps:

- Identify missing contacts, unclear triggers, system delays, or confusion.
- Update the fallback plan and role map accordingly.

5. Schedule a Leadership Review:

- Present findings and updates to exec team.
- Use this as a checkpoint before full-scale testing.

Phase 3: Build the Rhythm (Weeks 9–12)

1. Schedule a Tabletop Drill:

- Pick a date and invite all stakeholders: IT, HR, leadership, ops.
- Prepare a realistic incident scenario (e.g. ransomware or supply chain outage).

2. Assign Drill Roles:

- Facilitator to run the scenario.
- Recorder to capture actions, decisions, and gaps.

3. Refresh Ownerships:

- Review your Role Map.
- Confirm names, roles, and backups are up-to-date.

4. Draft a 'Drill Trigger' Checklist:

- Define what types of incidents require immediate action.
- Example: Data breach, primary system offline > 4 hours, public outage.

5. Create a Resilience Scorecard:

- Use a simple red/yellow/green scale for each system and process.
- Track improvements and re-test quarterly.

Final Thought

Resilience isn't about documentation, it's about clarity, ownership, and practiced response. If you execute this playbook over 90 days, you'll have more than a binder, you'll have a team that knows how to respond when it matters most.