Top 10 Steps for Executives

PROJECT CYBERSAFE™

Strengthening Crisis Management & Incident Response (CMIR) Capabilities

1 Establish Executive Ownership
- Define crisis leadership roles at the C-level.
- Make CMIR a board-level priority – not just IT's responsibility.

2 Align with Business Strategy
- Link response goals to business continuity, brand protection, and customer trust.
- Prioritize critical business processes and assets.

3 Form a Cross-Functional Team
- Bring together key leaders from IT, Security, Legal, Comms, HR, and Operations.
- Assign decision-making authority and escalation pathways.

4 Define Roles & Responsibilities
- Ensure technical teams and business leaders know their specific duties during a crisis.
- Use RACI charts to eliminate confusion.

5 Develop & Maintain an IR Plan
- Include playbooks for ransomware, data breaches, insider threats, and third-party incidents.
- Keep it updated with evolving threats and organizational changes.

6 Build a Communication Strategy
- Pre-draft communications for stakeholders, regulators, media, and customers.
- Coordinate messaging between technical and business teams to avoid conflicting narratives.

7 Develop an Executive Playbook
- Create a concise, action-oriented guide for leadership during cyber crises.
- Include decision triggers, key contacts, escalation protocols, and press response considerations.

8 Test the Plan with Tabletops
- Run simulations for executives and technical teams – separately and together.
- Use realistic scenarios to uncover gaps and build muscle memory.

9 Access to Tools & Data During a Crisis
- Validate that response teams can access logs, backups, contact lists, and documentation – even when systems are compromised.
- Plan for degraded operations and offline contingencies.

10 Establish Recovery Criteria & Conduct Post-Incident Reviews
- Define what triggers recovery actions and align decision thresholds across teams.
- Debrief after real incidents or simulations, and track improvement areas across departments.