Cyber Preparedness Checklist

Responding to Elevated Cyber Retaliation Risks Linked to the 2026 US-Israel-Iran Conflict

This checklist summarises the critical steps organisations should take now in response to heightened cyber retaliation risks from Iranian state linked and Iran aligned threat actors. It is designed for boards, senior management, compliance leaders, CISOs, and operational risk teams.

Click here to download our accompanying publication on cyber retaliation.

1. Strengthen Core Cyber Hygiene

Patch & Update Systems

Ensure all operating systems, browsers, apps, mobile devices, and third-party software are fully patched.

Enable auto matic updates where possible.

Confirm antivirus/EDR tools are active and current.

Verify Access Controls

Enforce strong, unique passwords; prohibit reuse across personal and business accounts.

Implement Multifactor Authentication (MFA) across all critical systems and administrative accounts.

Conduct an audit to remove dormant or unnecessary user accounts, including vendors/partners.

Ensure staff can promptly report phishing attempts and that the organisation can triage them quickly.

Review Internet Facing Assets

Identify all public facing systems and ensure they follow secure configuration and hardening standards.

Validate that remote administration tools are securely configured and restricted.

2. Reinforce Incident Response & Business Continuity

Incident Response Plan

Ensure the IR plan is up to date, with clear roles, out-of-hours decision authorities, and rapid escalation pathways.

Maintain offline copies of critical information (e.g., tokens, private keys, emergency contacts).

Backup & Recovery

Confirm that data backups are working, recent, securely stored, and tested.

Validate that alternative compute environments (e.g., cloud regions) can be activated if needed.

Business Continuity

Stress test continuity plans for disruptions to power, communications, cloud hosting, or water systems, which have been at risk in recent escalations.

3. Defend Against DDoS & Service Disruption

Map critical services to identify potential single points of failure.

Use diverse service providers (DNS, hosting, ISPs) to ensure continuity if one is compromised.

Implement graceful degradation so services can run in reduced capacity mode under attack.

Update your DDoS response runbook to account for rapidly changing attack tactics.

Conduct controlled DDoS simulations and monitor for early indicators (traffic anomalies, unusual login patterns).

4. Mitigate Phishing & Social Engineering Risk

Train staff, especially high-risk individuals in senior roles, legal/finance, and external facing functions, to recognise spear phishing and social engineering tactics.

Encourage caution around unexpected contact, credential prompts, document downloads, or requests to use alternative communication channels.

Require MFA, strong device passwords, and prohibit the use of public USB charging points.

Monitor devices for signs of compromise (battery drain, unusual restarts, unexplained network activity).

5. Protect High Value & High Exposure Assets

Prioritise protection for financial systems, payment channels, telecoms, logistics platforms, privileged identities, and cloud environments.

Review vendor and third-party exposure, ensuring suppliers follow equivalent security controls.

Monitor for disinformation, fabricated breach claims, or recycled leaks designed to create panic or distort risk perception.

6. Governance & Leadership Actions

Share this checklist and your threat briefing with Compliance, EXCO, and Board level stakeholders.

Establish a senior level working group to track evolving threats and ensure accountability for control improvements.

Confirm organisational contact details are registered with relevant national cyber alerting services (e.g., NCSC Early Warning for UK entities).

7. Engage Support

If you are concerned about these threats or want to significantly enhance organisational readiness, Themis can support you through:

- Board & Senior Management Threat Intelligence Briefings
- Sector specific cyber resilience guidance
- Gap assessments and scenario based exercises

We are ready to assist your leadership teams with the latest intelligence and practical steps to strengthen your protective frameworks
- Click here to be taken to our contact page.