Nasscom Advisory: Strengthening Operational and Cyber Resilience Amid Evolving Middle East Situation

In light of the evolving geopolitical situation in the Middle East, Nasscom has issued another advisory to member companies urging heightened vigilance and preparedness across business continuity and cybersecurity frameworks.

While business operations currently remain stable, organizations are proactively reviewing contingency plans and strengthening resilience measures to mitigate potential disruptions should the situation evolve over time.

Steps taken by member companies include:

1. **Business continuity plans activated / readiness for impacted countries** – Companies are reviewing and activating contingency frameworks to ensure operational continuity and uninterrupted service delivery in the event of regional disruptions.
2. **Employee safety and work from home for employees in impacted areas** – Organizations are prioritizing employee well-being by enabling remote work arrangements and closely monitoring the situation for employees located in affected geographies.
3. **Alternate options for cloud and data centre resilience in impacted areas** – Firms are evaluating alternate infrastructure routing to ensure cloud and data centre resilience and safeguard critical systems.
4. **Limit travel as the region is a popular transit option** – Companies are advising employees to limit non-essential travel through the region and explore alternative transit routes where required.
5. **Customer connect and providing all necessary support** – Organizations are proactively engaging with clients to communicate preparedness measures and ensure continuity of services.

At the same time, periods of geopolitical uncertainty often see a rise in coordinated cyber threats, disinformation campaigns, and infrastructure targeting. Organizations are therefore advised to strengthen their cybersecurity posture and treat the following as immediate priorities.

1. **Credential Reset & Accelerated Patching**: Recommended rotation of credentials organisation-wide and apply patches for critical CVEs.
2. **Zero Trust & MFA Enforcement:** Enforce multi-factor authentication on all external access paths (VPN, RDP, SSH, cloud admin) and implement conditional access controls to counter token-theft and adversary-in-the-middle attacks.
3. **Supply Chain Audit:** Assess all third-party vendors with Middle Eastern exposure. One compromised vendor can cascade into sector-wide disruption.

4. **DDoS Surge Readiness:** Engage ISPs and cloud providers for DDoS scrubbing capacity.
5. **Offline, Immutable Backups:** Maintain air-gapped backups for ICS/OT, core banking, and healthcare systems.
6. **Awareness around Disinformation**: Conduct employee awareness on social engineering attacks themed around possible war like situation, govt. alerts with intent to cause harm.

Nasscom continues to monitor the evolving situation in parts of the Middle East and remains in regular contact with the Middle East Council to assess developments on the ground and extend support where required. The industry body is also coordinating with relevant authorities wherever possible to assist member company employees who may be currently in the region.