Introduction:

On 25 May 2026, the Indian Computer Emergency Response Team (CERT-In), under the Ministry of Electronics and Information Technology (MeitY), released its "*Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation in Digital Infrastructure*" (Blueprint).

The Blueprint indicates that the Government's concern appears to extend beyond organisations directly deploying AI systems. The document recognises that advanced AI platforms may fundamentally transform the cyber threat landscape across digital infrastructure. Organisations may face heightened cybersecurity exposure because threat actors can leverage sophisticated AI systems to automate reconnaissance, identify software vulnerabilities, generate exploits, conduct large-scale phishing campaigns, and accelerate cyberattacks against conventional applications, APIs, cloud environments, and interconnected digital systems.

For instance, recent AI models are reportedly capable of identifying undetected software vulnerabilities, thereby significantly accelerating exploit discovery. This development reportedly prompted recent high-level discussions involving the Ministry of Finance and banking institutions in the country to assess potential risks to financial systems.

Key takeaways from the Blueprint:

Although not backed by a statutory rule-making provision, the Blueprint provides several significant suggestions for organisations. Some of the key takeaways are as follows:

- **'*Continuous*' over '*Periodic*' Security**: The Blueprint emphasizes that organisations should prioritise '*continuous exposure management*', '*continuous monitoring*', '*rapid remediation*', '*continuous vulnerability scanning*' and '*continuous audit*'. In other words, reactive assessments may no longer serve the purpose.

- **Aggressive remediation timeline**: The Blueprint sets out specific risk-based remediation timelines. For example, '*known exploited vulnerabilities affecting internet-facing systems*' should be patched or mitigated within 12 (twelve) hours, '*critical externally exposed vulnerabilities*' should be addressed within 1 (one) day, '*high severity vulnerabilities*' should be patched or mitigated within 5 (five) days, etc. These timelines, ***if*** eventually codified into regulation, would require organisations to significantly improve their cybersecurity vulnerability management workflows. Where immediate remediation is not possible, organisations should consider interim mitigation such as '*isolation*', '*access restriction*', Web Application Firewall and Application Programming Interface protection, or '*enhanced monitoring*'.

- **AI Governance framework**: Organisations are advised to define AI usage policies, establish approval and review mechanisms for AI integrations, maintain inventories of AI systems and monitor and identify shadow or unauthorised AI usage. Notably, the Blueprint addresses risks from public AI platform usage by employees and suggests incorporation of approval-based mechanism usage to restrict upload of sensitive information. Additionally, the Blueprint advises governance of agentic AI systems, including

defining operational boundaries, maintaining continuous monitoring, audit logging and incorporating emergency shutdown mechanisms.

- **Strengthening Identity and Access Security**: The Blueprint recommends organisations to implement stronger identity and access security measures, including Multi-Factor Authentication (MFA), Privileged Access Management (PAM), least-privilege architecture, adaptive authentication mechanisms, service account governance, etc. The Blueprint specifically identifies '*Zero Trust Security*' and '*Identity and Access Security*' as core defensive principles and recommends continuous verification, session monitoring and conditional access controls to reduce exposure arising from credential compromise, privilege escalation, and unauthorised access.

- **Supply chain and Third-Party risk management**: The Blueprint advises that organisations to strengthen supply chain visibility through the adoption of Software Bill of Materials (SBOM), AI Bill of Materials (AIBOM) mechanisms etc. These mechanisms are intended to support component visibility, dependency tracking, provenance validation, vulnerability impact assessment and rapid exposure identification. Reference has been made to CERT-In's Technical Guidelines on SBOM, QBOM, CBOM, AIBOM and HBOM Version 2.0 and recommends third-party and supply chain governance framework, requiring vendor assessments, contractual controls, dependency visibility and supplier reassessment.

- **Mandatory Incident Reporting**: The Blueprint reiterates that entities should ensure timely reporting of cyber incidents to CERT-In in accordance with CERT-In's 2022 Directions, which mandates a reporting within 6 hours from noticing (or being brought to notice) of prescribed cybersecurity incidents / cyber incidents.

- **Workforce and Deepfakes preparedness**: Organisations are advised to conduct awareness programmes addressing AI-enabled phishing, Deepfake-based impersonation and social engineering. The Blueprint highlights the need for Deepfakes detection given the threat to executives and financial institutions.

Comment:

The Blueprint is released at an interesting juncture, where AI needs to be given the right amount of push, but sufficient guardrails also need to be introduced. Although the Blueprint is not a binding document, it should be treated as an indicator of evolving regulatory expectations rather than a purely advisory and technical document, particularly because CERT-In repeatedly emphasises "***continuous governance***", "***continuous monitoring***", "***operational readiness***", and "***continuous assessment***" as foundational cybersecurity expectations for organisations facing AI-assisted cyber threats. Additionally, the threat of an AI-enabled cybersecurity incident may compel regulatory intervention from the Government in the near term.

- *Harsh Walia (Partner); Shobhit Chandra (Counsel) and Aadarsh Prakash (Associate)*

About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with over 1300+ legal professionals, including 340+ leaders and presence in India and Singapore. With more than a century of experience in practicing law, we offer end-to-end legal solutions in diverse practice areas to our clients across the world. We have a team of highly motivated and dynamic professionals delivering outstanding client service and expert legal advice across a wide gamut of sectors and industries.

To know more, visit **www.khaitanco.com**