June 2026

Indian Computer Emergency Response Team issues blueprint for reducing exposure and defending against Artificial Intelligence-assisted vulnerabilities and exploitation in digital infrastructure

On May 25, 2026, the Indian Computer Emergency Response Team ("**CERT-In**") issued the 'Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation in Digital Infrastructure' ("**Blueprint**"). The Blueprint recognises the growing use of Artificial Intelligence ("**AI**"), including generative AI, Large Language Models ("**LLMs**"), autonomous agents and AI-enabled automation platforms, by threat actors to automate cyber exploitation, accelerate vulnerability discovery, conduct highly targeted phishing attacks, generate adaptive malware and orchestrate attacks at scale.

The Blueprint has been positioned as an implementation-oriented framework intended to strengthen organisational resilience against AI-enabled cyber threats through governance measures, technical defensive controls, AI-aware monitoring, vulnerability and patch management, supply chain security, incident response preparedness and continuous security validation.

Introduction

The rapid advancement and accessibility of AI, including generative AI, large language models, autonomous agents, and AI-enabled automation platforms, are significantly transforming the cybersecurity landscape. Threat actors are increasingly leveraging AI capabilities to accelerate reconnaissance, automate vulnerability discovery, generate highly targeted phishing campaigns, develop adaptive malware, and enhance the scale and speed of cyber-attacks. AI-assisted cyber exploitation reduces the time required for adversaries to identify, weaponise, and exploit vulnerabilities. As organisations become increasingly dependent on interconnected digital infrastructure, cloud ecosystems, and AI-enabled platforms, the potential impact of AI-enabled cyber threats continues to increase across sectors.

Authority of the CERT-In to issue the Blueprint

The CERT-In was established under Section 70B of the Information Technology Act, 2000 ("**IT Act**"), and operates with statutory authority for cybersecurity preparedness and response in India. As a governmental nodal agency under the Ministry of Electronics and Information Technology, the CERT-In is empowered to coordinate the detection, prevention, and mitigation of cybersecurity incidents. Further, the CERT-In has the authority to require reporting of certain categories of cyber incidents such as unauthorised access, malware outbreaks, and breaches involving critical infrastructure and to coordinate with domestic stakeholders and international counterparts in responding to cyber threats. Under Section 70B(4)(e) and Section 70B(6) of the IT Act, the CERT-In is empowered to issue directions and

guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.

In this context, the CERT-In has released the Blueprint to support organisations in strengthening resilience against AI-enabled cyber threats through structured governance, defensive controls, continuous monitoring, operational preparedness, resilience enhancement, and adaptive cybersecurity practices aligned with evolving threat conditions.

Analysis of the key recommendations and operational implications under the Blueprint

AI-assisted cyber threats recognised as an accelerated systemic risk

The CERT-In has expressly acknowledged that AI-assisted cyber exploitation significantly reduces the timelines within which threat actors may identify, weaponise and exploit vulnerabilities. The Blueprint highlights that AI-enabled threats are increasingly capable of automating multiple stages of the cyber kill chain, including reconnaissance, exploitation, lateral movement and data exfiltration.

The Blueprint specifically identifies the following threats:

1. AI-enabled reconnaissance and attack surface mapping;
2. automated vulnerability discovery and exploit development;
3. AI-driven phishing, impersonation and social engineering;
4. AI-generated malware and adaptive payloads;
5. deepfake enabled fraud and executive impersonation; and
6. adversarial attacks targeting AI systems themselves, including prompt injections, model poisoning and insecure AI integrations.

Governance and board level accountability for AI-related cyber risk

The Blueprint places significant emphasis on executive oversight, cybersecurity governance and organisational accountability mechanisms for AI-enabled cyber risks. The CERT-In recommends that organisations implement formal governance structures covering cybersecurity risk management, AI adoption, shadow AI monitoring, third-party risk governance, incident escalation and continuous operational assurance.

In summary, the Blueprint makes the following recommendations:

1. AI usage and approval policies;
2. governance frameworks for AI integrations;
3. structured risk assessment processes;
4. cross functional accountability mechanisms;
5. continuous cybersecurity audits and assessments; and
6. workforce awareness programs addressing AI-enabled phishing, impersonation and deepfakes.

Notably, the CERT-In encourages organisations to undertake continuous cybersecurity audits and assessments through the CERT-In empaneled auditing organisations in alignment with the CERT-In's Comprehensive Cyber Security Audit Policy Guidelines.

Shift toward zero trust, continuous monitoring and exposure management

The Blueprint adopts an explicitly 'assume breach' and 'zero trust' approach toward cybersecurity architecture. The CERT-In recommends implementation of layered defensive controls including:

1. multi factor authentication;
2. privileged access management;
3. segmentation and micro segmentation;
4. attack surface monitoring;
5. endpoint detection and response;
6. behavioural analytics and anomaly detection;
7. continuous telemetry monitoring; and
8. integrated security information and event management systems.

The Blueprint further emphasises continuous exposure management and recommends that organisations continuously monitor internet facing systems, Application Programming Interface ("**APIs**"), identities, cloud infrastructure and software dependencies. The CERT-In has also recommended adoption of software bill of materials, AI bill of materials, quantum bill of materials and cryptographic bill of materials mechanisms to enhance supply chain visibility and vulnerability tracking.

Specific focus on AI system security and governance of enterprise AI adoption

A distinct section of the Blueprint is dedicated to security and governance of AI systems adopted by organisations. The CERT-In recognises that enterprise deployment of public AI platforms, LLMs, AI APIs and autonomous agents may create significant cybersecurity, operational, privacy, data governance and supply chain risks, particularly where appropriate governance, monitoring, validation and security controls are not properly implemented.

To strengthen AI governance, the CERT-In further recommends that organisations:

1. maintain inventories of AI systems and AI integrations;
2. restrict upload of sensitive information to public AI services;
3. implement AI-specific access controls and logging;
4. conduct adversarial testing for prompt injection and input manipulation risks;
5. monitor AI APIs and inference activity;
6. review AI-generated code through static application security testing, dynamic application security testing and dependency analysis;
7. validate model provenance and integrity; and
8. establish human oversight mechanisms for critical AI-assisted decisions.

The Blueprint also specifically addresses governance challenges arising from autonomous and agentic AI systems and recommends implementation of operational boundaries, override mechanisms and emergency shutdown controls.

Vulnerability remediation timelines

The Blueprint strongly emphasises continuous vulnerability management and recommends a risk based remediation framework tied to exploitability and operational criticality. The CERT-In recommends that:

1. known exploited vulnerabilities affecting internet facing or crown jewel systems should be contained and patched within 12 (twelve) hours where feasible;
2. critical externally exposed vulnerabilities should be patched within 1 (one) day;
3. known exploited vulnerabilities affecting internal systems should be remediated within 1 (one) day; and
4. high severity vulnerabilities should generally be patched within 5 (five) days based on risk prioritisation.

The Blueprint also recommends use of known exploited vulnerabilities prioritisation and exploit prediction scoring methodologies for remediation prioritisation.

Expanded operational expectations for security operations centres and incident response

The Blueprint encourages organisations to modernise security operations through AI-assisted monitoring, behavioral analytics, threat hunting and automated response orchestration. The CERT-In recommends strengthening:

1. threat intelligence integration;
2. AI-assisted detection engineering;
3. behavioural anomaly detection;
4. threat hunting exercises;
5. AI activity logging and monitoring;
6. automated triage and response workflows; and
7. deepfake and impersonation detection readiness.

The CERT-In also reiterates that entities should ensure timely cyber incident reporting to the CERT-In, including reporting of cyber incidents within 6 (six) hours in accordance with 'Directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet' issued by the CERT-In on April 28, 2022 under Section 70B(6) of the IT Act.

The Blueprint further encourages participation in the CERT-In led cyber drills, tabletop exercises and adversarial simulations to strengthen operational resilience.

Conclusion

The Blueprint acknowledges that the rapid advancement and accessibility of AI technologies are significantly transforming the cybersecurity landscape and enabling increasingly sophisticated, scalable, and automated cyber threats. AI-assisted cyber exploitation is accelerating reconnaissance, phishing, impersonation, malware generation, exploit development, and large-scale attack operations across interconnected digital ecosystems. In this evolving threat environment, the Blueprint recommends that organisations adopt adaptive, intelligence driven, continuously validated, and resilience-oriented cybersecurity practices rather than relying solely on static controls or periodic compliance driven assessments. Continuous monitoring, rapid remediation, adaptive defence, and coordinated cybersecurity preparedness are essential for strengthening resilience against evolving AI-assisted cyber threats and enhancing trust in India's digital ecosystem.

While the Blueprint is presently framed as guidance rather than binding regulation, it establishes a detailed operational benchmark for cybersecurity governance, AI security readiness, vulnerability management, incident response preparedness, and continuous security validation focusing on cybersecurity and AI-assisted exploitation. The recommendations indicate The CERT-In's increasing regulatory focus on proactive exposure reduction, continuous monitoring, supply-chain visibility, and AI governance across enterprise environments. For organisations, the Blueprint serves not only as a cybersecurity preparedness framework, but also as an indicator of evolving regulatory expectations around AI-enabled risks and operational resilience within India's digital infrastructure ecosystem.

Infotech Practice

Our team understands the importance of data privacy in today's digitally interconnected world. We have dedicated our practice to ensuring that your and your customers' personal and business data remains secure, compliant, and respects the sovereignty of individuals and jurisdictions globally.

We prioritise creating bespoke solutions tailored to your business needs. We recognise that every business has unique data privacy challenges, and we use our deep understanding of international and domestic regulations to provide you with the most effective and robust legal strategies. JSA provides advice on highly sophisticated data management, data security and privacy issues. Our depth of experience gives our clients the crucial advantage of consistent and comprehensive, yet practical advice. Our Technology Law Practice group has successfully worked with several multinational organisations for the structuring and roll-out of privacy and information-security programs. We have carried out audit and risk assessments, customised global privacy and information management policies, helped create international data transfer strategies, structure and negotiate complex international data transfer agreements.

This Prism has been prepared by:

Tony Verghese
Partner

Radhika Gupta
Partner

Uddhav Gupta
Associate

19 Practices and
40 Ranked Lawyers

8 Ranked Practices,
22 Ranked Lawyers

15 Practices and
20 Ranked Lawyers

13 Practices and
49 Ranked Lawyers

20 Practices and
24 Ranked Lawyers

2026

8 Practices and
15 Ranked Lawyers
Highly Recommended in 5 Cities

Regional Legal Expertise Awards (APAC) of the Year
Energy Firm Competition/
Antitrust Firm

Among Best Overall
Law Firms in India and
14 Ranked Practices
---
9 winning Deals in
IBLJ Deals of the Year
---
15 A List Lawyers in
IBLJ A-List – 2026

Recognised in World's 100 best
competition practices of 2026

Ranked Among Top 5 Law Firms in
India for ESG Practice

Asia M&A Ranking
2025 – Tier 1

For more details, please contact km@jsalaw.com

Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi