ERGO

KHAITAN &CO ADVOCATES SINCE 1911

Frontier AI Risk Defence: The New Standard for Incident Response

11 May 2026

Frontier AI Risk Defence: The New Standard for Incident Response

On 26 April 2026, the Indian Computer Emergency Response Team (CERT-In) issued an advisory titled, *"Defending Against Frontier AI Driven Cyber Risks"* (Advisory), categorised as high severity. While framed as an advisory, it reflects a clear regulatory shift. Artificial Intelligence (AI) incident preparedness is no longer a matter of best practice, it is increasingly a baseline compliance expectation against which organisational readiness may be assessed.

Importantly, the Advisory applies across the ecosystem, including organisations, Micro, Small and Medium Enterprises (MSMEs), and individual users, recognising that AI-driven cyber risks are systemic and capable of cascading across interconnected digital environments.

What the Advisory Requires

At a high level, the Advisory prescribes a set of minimum preparedness measures calibrated for AI-driven threats.

For organisations, this includes maintaining incident response and cyber crisis management frameworks capable of handling simultaneous, multi-vector attacks, ensuring real-time monitoring and logging, promptly addressing vulnerabilities and being able to report incidents in a timely and substantively complete manner. A key expectation is the establishment of pre-defined response frameworks, including clearly identified points of contact across technical, regulatory, and legal functions, supported by pre-arranged engagement mechanisms.

For MSMEs, the focus is on foundational cyber hygiene, secure configurations, timely patching, use of trusted systems and prompt escalation of suspicious activity.

For individuals, the Advisory emphasises basic digital hygiene, including use of updated systems, strong authentication practices, and caution against AI-enabled phishing and social engineering.

Crucially, the Advisory also underscores manpower preparedness. Organisations are expected to ensure that internal teams across IT, legal, compliance and management are trained to respond in real time, including through scenario-based exercises and clearly defined escalation protocols.

From Advisory to Firmer Compliance Expectations

Although the Advisory does not carry the same statutory force as the CERT-In Directions of April 2022, regulatory practice increasingly treats high-severity advisories as *de facto* compliance benchmarks. CERT-In has, in enforcement-facing contexts in the past, required entities to demonstrate alignment with relevant advisories.

This position is reinforced by broader regulatory developments, including draft amendments to intermediary rules that contemplate compliance with advisories and clarifications. The distinction between guidance and obligation is therefore narrowing, particularly in areas involving systemic risk.

A Converging Regulatory Scenario

The Advisory must be viewed alongside a broader and increasingly coordinated regulatory and market response to AI-driven cyber risks. In April 2026, Union Finance Minister Nirmala Sitharaman convened a high-level meeting with banking sector leadership, alongside representatives from MeitY, the Reserve Bank of India and CERT-In, to assess emerging risks and emphasise proactive preparedness. In parallel, the Securities and Exchange Board of India has initiated steps to strengthen cybersecurity governance, including the formation of a dedicated task force on AI-related threats.

Market behaviour reflects this shift, with organisations increasing cybersecurity investment and strengthening incident response capabilities. Taken together, these signals point to a convergence of regulatory intent and market response, centred on proactive resilience.

Possible Compliance Gap

Against this backdrop, many existing incident response plans are likely to fall short of the emerging standard. They are typically designed around single-incident scenarios, assume response timelines measured in days and treat legal and regulatory engagement as a subsequent phase.

In practice, however, cyber incidents trigger simultaneous and overlapping obligations within compressed timelines. These include reporting to CERT-In within prescribed timelines, sectoral reporting requirements (for regulated entities), personal data breach obligations under the Digital Personal Data Protection Act, 2023 (*once core obligations are enforced*), potential law enforcement engagement and contractual disclosures. Where systems and data are distributed globally, cross-border considerations further complicate response timelines and coordination.

In this environment, timelines effectively collapse into a single response window. Incident response plans that do not account for this convergence, through pre-designated teams, coordinated escalation and immediate legal involvement, risk being viewed as inadequate against a clearly articulated regulatory benchmark.

The Way Forward

The immediate priority is a targeted recalibration of incident response frameworks. Organisations should also pre-designate and retain legal, forensic and incident response partners on terms that permit immediate activation and establish tested communication channels with CERT-In and relevant regulators.

Equally important is manpower readiness, training cross-functional teams through scenario-based exercises that reflect AI-driven, multi-vector incidents and compressed timelines.

In parallel, organisations should align logging, evidence preservation and reporting workflows with regulatory expectations, and ensure that legal and regulatory decision-making is embedded from the outset of incident response.

Conclusion

The Advisory effectively establishes a new standard of care for incident response. As AI-driven threats compress response timelines and increase the complexity of incidents, organisations will increasingly be assessed not only on how they respond to incidents, but on whether they had demonstrable preparedness in place before the incident occurred.

- *Supratim Chakraborty (Partner) and Himeli Chatterjee (Senior 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**