The 'Mythos' Risk

How Prepared Are Banks in India?

The release of Anthropic's Mythos has triggered a Y2K equivalent era for cybersecurity.

Pankit Desai, CEO and Co-Founder, Sequretek, Mumbai

> **"Knowing about a vulnerability is only one part of the problem. Communicating it across the value chain, understanding its specific enterprise impact, and executing a mitigation strategy is where the real challenge lies.**

While initial industry reactions leaned heavily into fear, recent counter narratives from outlets like Reuters correctly point out that this is not an apocalyptic scenario. It is simply a new baseline. Mythos operates at unprecedented scale and speed, exposing flaws in foundational systems like operating systems and databases that have remained hidden for decades. The application side of the house is almost secondary to this concern. This paradigm shift moves the industry away from reactive patching and forces a move toward proactive architectural resilience. Panic is the wrong response. Preparedness, relentless hygiene, and proactive chain-aware defenses will reduce any massive blast radius and keep financial institutions secure.

Protecting the banking ecosystem

The core challenge financial institutions face today is a lack of comprehensive IT asset visibility. Without a complete Software Bill of Materials (SBOM), banking, financial services, and insurance (BFSI) organizations remain blind to vulnerabilities hiding within underlying web servers, middleware, APIs, or software libraries; IBM defines a SBOM as a formal, machine-readable inventory of all the components, libraries, and dependencies that make up a software application. It functions like a de-

tailed "ingredients list," providing total transparency into the software supply chain to help track security vulnerabilities and manage licensing risks. As Microsoft's MDASH threat feeds begin to populate with Mythos-discovered zero-days, a time-delay activity starts to set in. Will the discoverers inform the government, the software providers, or will the vulnerability be immediately exploited by threat actors?

Knowing about a vulnerability is only one part of the problem. Communicating it across the value chain, understanding its specific enterprise impact, and executing a mitigation strategy is where the real challenge lies. The vulnerability exists at the original equipment manufacturers' (OEM) software level, meaning end-user organizations cannot fix it by themselves. They have to wait for the patch, which takes time.

Regulators cannot remediate third-party software, but their enforcement mechanisms are actively shaping the response. We see this clearly with SEBI's recent Annexure-A, which mandates stricter third-party risk assessments and incident reporting for financial entities. Policymakers are beginning to hold OEMs responsible for being at the front end of the problem. Mandating that OEMs run Mythos equivalent testing on their own products and submit validated reports directly to the regulator is the logical next step. While OEMs bear the responsibility for patching, financial institutions must proactively prepare to meet these compliance standards without disrupting daily operations.

Triage and chain-aware defenses against multi-step AI exploits

When remediation begins, structured triage (refers to knowing how to answer the following three questions: *What needs immediate attention? What can wait? And what can be resolved later or not at all?*) is the only viable discipline. BFSI organizations must first build and maintain a granular, near real-time repository of every software component in use.

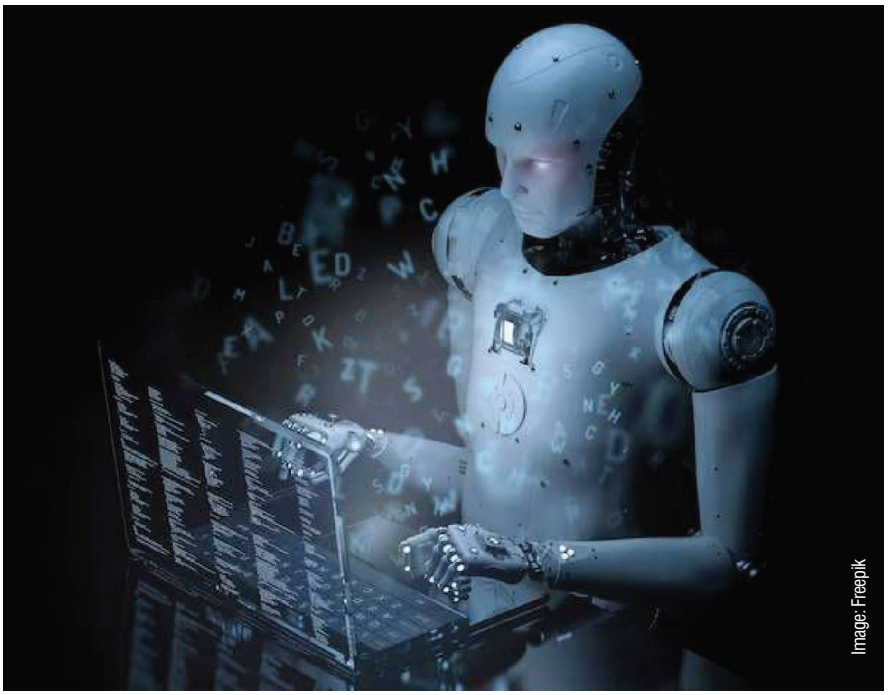

Image: Freepik

They must then establish contractual agreements mandating that OEMs provide notification within 24 hours of discovering a potential issue. You cannot just go and fix a vulnerability overnight. Rushing a patch risks introducing new failures that compound the original disruption. Organizations must evaluate the exploitability of each vulnerability, assess whether it has been observed in the field, determine the criticality of the affected asset, and identify whether a compensating control can provide interim protection. Compensating controls might include segmenting vulnerable networks, tightening identity access management, or deploying specialized web application firewalls to shield exposed assets. A protective wrap-around on existing software buys time until a permanent patch is ready.

> **The core challenge financial institutions face today is a lack of comprehensive IT asset visibility. Without a complete Software Bill of Materials (SBOM)—a Software Bill of Materials (SBOM) is a formal, machine-readable inventory of all the components, libraries, and dependencies that make up a software application—BFSI organizations remain blind to vulnerabilities hiding within underlying web servers, middleware, APIs, or software libraries**

Closing the security debt crisis

This is the classic *chor*-police equivalent of cybersecurity. The offensive side has made a massive leap, but defensive technologies will inevitably catch up. AI-driven capabilities will emerge to provide automated, real-time mitigation. The current anxiety will eventually settle into structured operating processes and clearer institutional discipline. What we must recognize is that this shift is permanent. The Pandora's box of automated threat discovery is open, and there is no way they can put the genie back in the bottle. By focusing on relentless hygiene and proactive defenses, banks can navigate this new era with confidence and stability. ■

Reference # 20M-2026-06-11-01