Banking buckles up to meet Mythos threat

Industry races to upgrade infrastructure as advanced AI model poses risks to cybersecurity, report **Avik Das** & **Subrata Panda**

Risk account

- While humans take weeks to patch a security flaw, Mythos can find and use it in minutes
- It is capable of spotting holes in ageing 'legacy' software that many banks still rely on for their daily transactions
- As many banks use the same underlying technology, one AI-driven attack could potentially trigger a domino effect
- Mythos effectively gives a novice the power of a master hacker, dramatically lowering the 'barrier to entry' for carrying out sophisticated cybercrimes
- It looks beyond a bank's own app to find vulnerabilities in the global web of third-party providers that keep the financial system running

The International Monetary Fund (IMF) last week warned the finance industry about Anthropic's Claude Mythos, an advanced artificial intelligence (AI) tool that can speed up finding and exploiting weaknesses in software.

"This foreshadows how fast-moving, AI-driven cyber risks could destabilise the financial system if not managed carefully, and why authorities must focus on building resilience through supervision and coordination — rather than treating these developments as purely technical or operational issues," it said in a blog post.

The IMF warned that powerful AI tools could be weaponised to undermine the global financial system, as the offensive capabilities of intruders outpace traditional defences. Extreme cyber incidents could trigger severe funding strains, raising solvency concerns and disrupting wider markets. This vulnerability stems from a global digital infrastructure that is now deeply interconnected.

The international agency's statement is in line with what Finance Minister Nirmala Sitharaman said last month. She expressed concern that banks' cybersecurity systems may be insufficient to handle emerging threats from Mythos and other such advanced AI models.

While banks have diligently protected their customers over the years, their capabilities may not be sufficient in the age of advanced AI. "There is a need for new and more versatile measures to counter emerging threats," Sitharaman said, urging extensive interaction among companies under the aegis of the Indian Banks' Association (IBA) to assess investment needs, adopt new technologies and use AI to counter threats.

The concern radiating from the top of India's financial sector underscores a growing global anxiety among regulators over the disruptive power of AI systems like Mythos. The Australian Securities and Investments Commission recently sent a letter to the country's financial services industry saying it needs to fortify current cybersecurity systems.

Claude Mythos Preview, which was released last month to select enterprises in the United States, marks a shift in the landscape as a general AI model. Thanks to its sophisticated coding logic, it possesses an unprecedented ability to detect vulnerabilities in every major operating system and web browser — even when directed by non-experts. This capability has led cybersecurity companies and experts to warn that the barrier to executing sophisticated cyberattacks has been lowered.

"Advanced AI models can dramatically reduce the time and cost needed to identify and exploit vulnerabilities, raising the likelihood of simultaneously discovering and targeting weaknesses in widely used systems. As a result, cyber risk is increasingly about correlated failures that could disrupt financial intermediation, payments, and confidence at the systemic level," the IMF added.

That puts the spotlight on Indian banking which runs on legacy systems and could be extremely vulnerable to powerful attacks — just like in other countries. Upgrading such systems takes time and money. While banks have been protecting themselves from potential cyberattacks over the years, the new AI models pose risks far greater than generic security threats.

Ashok Vaswani, managing director (MD) and chief executive officer (CEO) of Kotak Mahindra Bank, said the nature of cyber risks is fundamentally changing. "We have always been geared up to deal with cyberattacks at the speed of a human. Now we have to deal with cyberattacks at the speed of a machine," he told analysts after announcing the company's fourth-quarter results early this month.

"If there is one thing that keeps me up at night, surely this is the one," Vaswani said, referring to AI tools like Mythos.

The problem, security experts say, lies in the complex web of technology forming the backbone of India's banks and fintech players. The attack surface is no longer a single application but an entire software supply chain reaching three and four tiers deep — often comprising libraries maintained by volunteer communities with minimal formal security reviews or standardised disclosures. Compounding this is the fact that discovering a vulnerability is only half the battle. Addressing it with traditional tools is no longer enough, particularly through legacy patch management built on quarterly cycles and rigid maintenance windows.

"It [current cybersecurity technology] was designed for a world where the attacker also needed time. That world no longer exists. When Mythos can identify and chain a working exploit in hours, a 90-day patch SLA is not a risk management posture — it is an open invitation," Pankit Desai, cofounder and CEO of cybersecurity firm Sequretek, wrote in a LinkedIn post, referring to a contractual agreement for identifying and fixing vulnerabilities in software within 90 days of discovery.

Srinivas L, joint MD and joint CEO of cybersecurity solutions company 63Sats Cybertech, said that many banks in India still run on the old COBOL programming language, which makes them vulnerable to threats from Mythos. India will be a primary target of AI-powered cyberattacks, considering the volume of business that takes place in the country.

"The fear is coming with respect to all the enterprises because we were always skill-gated. Now, the attacks have become commodity. Before Mythos, if you had to exploit a very serious vulnerability, you really needed a lot of deep real technical skills. But then with this, you just have a small simple prompt-like offering and you are able to launch right from reconnaissance to finding a vulnerability and exploiting it. When this kind of democratisation of capability happens, that is with nation-state proxies or criminal enterprises, it becomes concerning," said Srinivas.

How can Indian banks build resilience in this new era? As AI reshapes cybersecurity, the question for the authorities is whether the financial system can withstand such severe stress. The outlook is sobering: most Indian institutions lack access to Mythos even for defensive testing in a sandbox environment.

M Nagaraju, secretary, Department of Financial Services, highlighted the risk posed by the Mythos AI model and asked the banking sector to be prepared. He classified such risks as "extremely dynamic, extremely complicated and quite unknown to all of us."

"Banking risks are no longer confined to trade books or balance sheets, they now arise from geopolitical developments, technology, cyber threats, operational disruptions among others," Nagaraju said at an IBA event last week.