

Experts call for continuous security awareness and AI-driven vigilance

The Hindu, dt: 14.2.2026, pg. no. 14



Experts speak at the session titled 'Beyond Compliance: Leveraging ISO 27001 for Integrated Data Security Management'. They highlighted the importance of security in the context of AI bringing about rapid changes. M. SRINATH

The Hindu Bureau CHENNAI

Security awareness has to be a continuous activity, and it is everyone's responsibility, Maharajan Suriyanarayan, chief information security officer and vice-president-IT, Navitas Life Sciences, said in Chennai on Friday at *The Hindu* Tech Summit 2026.

The event is hosted by *The Hindu*, presented by VIT, and co-presented Sify Technologies.

Speaking at the session, 'Beyond Compliance: Leveraging ISO 27001 for Integrated Data Security Management', he said security awareness has been created over a period of time by implementing ISO 27001. As for the ways to ensure that security evolves and the steps to be taken to have a security-aware culture within an organisation, he said, "Security awareness has to be creat-

'Security awareness has to be created from top to bottom, and there is a need to be aware of customer data and ways to secure them'

ed from top to bottom, and there is a need to be aware of customer data and ways to secure them. Different kinds of programmes are essential. New threats are coming, and knowledge of such threats needs to be given, from end-users to the top management," he added.

'Disciplined approach'
Culture is not a practice but more of a disciplined approach, Ram S., executive vice-president and chief information officer, Virtusa Corporation, said. "We have also enabled AI to monitor employee behaviour to see if there are any

aberrations," he added.

Balakumar M.N., head, IT, Ucal Limited, stressed the need for a continuous assessment of security-related aspects as well. "We should assess, reassess, and document the process in such a way that we know the root causes and learn from it... due to volatile changes, be it business changes, introduction of new policies, or changes within the organisation. It has to be a cycle. Learn, unlearn, and relearn," he added.

Answering a question on what makes a certified organisation become a secure one, when there is a rapidly evolving threat landscape including AI, Sivaramakrishnan N., senior vice-president, information security, and chief information security officer, M2P, said AI has been bringing about rapid changes. "Now, everyone wants to try the Anthropic

plug-in. Whatever access you give, control the blast radius," he said. While one can be allowed to dabble with a new plug-in, there should be some control on how many get access to it, whether it is approved by their head; the nature and sensitivity of the data has to be monitored, and it should be a timed activity as well, he added.

'Balancing act'

Mr. Ram said security is always a balancing act. "We have deployed AI to track major incidents. We simulate them. We don't wait for an incident to happen. That way, we are protected. It has been a humongous challenge to keep up with [the developments of AI], to understand the AI narrative of the organisation, to upskill ourselves," he added.

Suresh Vijayaraghavan, CTO, *The Hindu*, moderated the session.