Business Standard

Indian cybersecurity product firms may generate $6 bn revenue in 2026: DSCI

India's cybersecurity product companies are projected to generate nearly $6 billion in 2026, up from $4.46 bn in 2025, even as AI-driven attacks and sophisticated threats reshape security landscape

The country is now home to more than 400 cybersecurity product companies that have grown at a compounded annual growth rate (CAGR) of 34 per cent over the last five years. (Representative Picture)

India’s cybersecurity product firms are expected to generate nearly $6 billion in revenue in 2026, up from the $4.46 billion generated in 2025, the Data Security Council of India (DSCI) said in a report on Thursday.

The country is now home to more than 400 cybersecurity product companies that have grown at a compounded annual growth rate (CAGR) of 34 per cent over the last five years. In 2020, the combined annual revenue of these companies stood at $1.05 billion, according to the DSCI Indian Cybersecurity Product Landscape Report.

Nearly 55 per cent of these companies operate in global markets, with clients primarily in north America, west Asia and southeast Asia. These regions have emerged as significant markets for these firms, the report said. However, despite clients for these companies in international markets, many operate through channel partners as only 17 per cent have physical offices in these geographies.

In India, Karnataka, Delhi-NCR, and Maharashtra continued to be the primary hubs driving the growth of these companies, the DSCI said.

Incidentally, Maharashtra, Gujarat and Delhi emerged as the states most affected by cybersecurity incidents in India, according to another report by Seqrite, the enterprise arm of cybersecurity products and services company Quick Heal Technologies.

In the India Cyber Threat Report 2026, launched on Thursday, Seqrite reported detecting 265.52 million cybersecurity incidents between October 2024 and September 2025, translating to over 505 incidents detected every minute.

“This reality underlines how, in the midst of India’s fast-paced digital transformation, cyber threats are growing in scale and sophistication, reshaping threat patterns, entry points and the strategic priorities of security leaders,” Deep Chanda, the chief executive officer of cybersecurity firm Ampcus Cyber, said.

Overall, nearly 31 per cent of these cybersecurity attacks involved artificial intelligence (AI)-driven supply chain compromises and coordinated vector operations. In comparison, roughly 29 per cent stemmed from autonomous malware and AI-powered zero-day exploitation techniques, DSCI said in another report launched on Thursday.

“Adversaries are using generative AI to craft convincing phishing lures, automate malware, and probe misconfigurations at machine speed, making traditional perimeter-led security obsolete,” Chanda said.