BW BUSINESSWORLD

India's Cyber Threat Expands Beyond Banks, Healthcare As Critical Sectors Digitise

Cyber threats are spreading across India's digital economy, putting manufacturing, energy, telecom, and other critical sectors in the crosshairs

A government response tabled in Parliament showed that cyber threat detections targeting India's financial and healthcare sectors in the first half of 2026 had already crossed 60 per cent of the total recorded across both sectors through all of 2025. Banks alone faced 17 targeted intrusion campaigns during the period, while malicious scanning and probing incidents in the financial sector touched 3.09 lakh.

But the threat is spreading beyond these traditional targets. Manufacturing, power and energy, telecommunications, government infrastructure, defence, logistics and education are emerging as significant targets in 2026, as the expansion of connected systems creates new points of exposure.

Manish Chasta, Co-Founder & CTO, Eventus Security, said manufacturing, government and public infrastructure, energy and utilities, telecommunications, defence, logistics and transportation are becoming attractive targets. He attributed the shift to India's digital

transformation and the convergence of cloud platforms, connected devices, operational technology (OT) and traditional information technology (IT) environments.

The wider threat is reflected in the more than 29.44 lakh cybersecurity incidents handled by the Indian Computer Emergency Response Team (CERT-In) in 2025. Attackers are using ransomware, phishing, credential theft, supply chain compromise, distributed denial-of-service (DDoS) attacks and vulnerabilities across IT and OT environments, Chasta said.

Data Theft To Operational Disruption

The bigger change is not simply where attacks are occurring, but what attackers are trying to achieve. As industrial and critical infrastructure becomes more digitally connected, a successful breach can affect production and essential services rather than only expose information.

“What makes the risk particularly serious is that attackers are no longer focused only on stealing data. They are increasingly seeking to disrupt operations,” Chasta said. An attack on a manufacturing facility, power utility, telecom network or logistics provider can interrupt physical processes and delay essential services, he added.

Govind Rammurthy, CEO & Managing Director, eScan, said critical sectors offer attackers greater leverage because disruption can be monetised. He identified critical infrastructure status, legacy systems operating alongside new cloud infrastructure and supply-chain dependencies as key factors increasing the attractiveness of these industries.

“Disruption pays. Blackmail works when you can shut down a power plant or disrupt a critical service,” Rammurthy said. The potential for operational disruption gives attackers another way to pressure organisations beyond conventional data theft.

Where The Entry Points Lie

Phishing emails, compromised vendor accounts, weak access controls and cloud misconfigurations can provide attackers with an initial foothold. From there, attacks can escalate as organisations' digital and operational environments become more interconnected.

Tarun Wig, Co-Founder, Innefu Labs, noted that ransomware remains the most common threat and is often combined with data theft to increase pressure on victims. “It usually starts small, a phishing email or a compromised vendor account, and builds from there,” he said.

AI-generated phishing has become more convincing, while DDoS attempts against power and telecom infrastructure have also picked up, Wig said. Cloud misconfigurations and weak access controls are recurring problems as organisations migrate to the cloud faster than they can govern it.

The vulnerabilities are particularly visible in industrial environments. Rammurthy said eScan has seen manufacturing plants with OT networks connected to corporate IT without proper

segmentation, as well as machines within corporate networks connecting directly to the internet without firewall protection.

Energy facilities are deploying Internet of Things (IoT) devices without proper authentication, while telecom organisations are relying on third-party vendors with weak security controls. Government organisations are also rushing cloud migration without adequately addressing data residency and security requirements, Rammurthy said.

Legacy Systems Meet New Pressure

The underlying weakness is a combination of older infrastructure and newer digital systems. IoT and OT equipment was largely designed for reliability rather than resistance to modern cyber threats, leaving gaps in basic controls such as strong authentication and regular patching.

Many of these industries are also newer to structured cybersecurity practices than banking, while third-party vendors add another layer of exposure. As a result, dedicated monitoring capabilities and other security measures are still being developed across parts of the industrial and critical infrastructure landscape.

Independent data points to the breadth of the threat. Seqrite's India Cyber Threat Report 2026, drawing on telemetry from more than 8 million endpoints between October 2024 and September 2025, found education accounted for nearly 24 per cent of detections nationally, ahead of finance and healthcare when measured individually.

Regulation Begins To Catch Up

Policy is beginning to respond to the growing exposure of critical infrastructure. Wig pointed to the Central Electricity Authority's new cybersecurity rules for the power sector, which require physical separation between IT and OT networks and incident reporting to CSIRT-Power and CERT-In within six hours.

“That’s a strong signal that critical infrastructure is being brought under the same kind of scrutiny finance has had for years, and it’s a welcome step,” Wig said. Industry data also shows manufacturing accounts for a notable share of malware detections nationally, with OT and industrial control system attacks concentrated in states with heavy manufacturing activity.

For Chasta, the response needs to move beyond preventive controls towards continuous resilience. This includes 24×7 monitoring, intelligence-led detection, strong identity controls, visibility across IT and OT environments and regular simulations of real-world attack scenarios.

Organisations must assess not only whether a system can be compromised, but how quickly they can detect, contain, respond to and recover from an attack. As India's physical economy becomes increasingly connected, cybersecurity is consequently shifting from protecting information to preserving operational continuity.