ET Edge INSIGHTS

Telecom

India’s telecom growth story is now about trust and cybersecurity

Representational Image

By **Govind Rammurthy**
Published May 20, 2026

India’s telecommunications infrastructure has evolved into one of the world’s largest and most dynamic digital ecosystems. As connectivity becomes central to banking, governance, healthcare, and daily life, the focus is now shifting from expanding access to securing the networks and data that power India’s digital economy.

India has come remarkably far from the days when securing a telephone connection from MTNL required years on waiting lists and international calls cost more than monthly salaries. Today, India boasts the world’s second-largest telecommunications network with over 1.2 billion mobile subscribers, the lowest data costs globally at ₹10-15 per GB, and 5G rollout covering hundreds of cities within months of launch. What took decades in Western markets happened in India within years, demonstrating how competitive markets and supportive regulation can leapfrog traditional development timelines.

But the telecommunications story isn’t just about connectivity anymore – it’s about what flows through those connections. When 800 million Indians access the internet daily, when UPI processes 15 billion transactions monthly, when digital healthcare reaches remote villages through telemedicine, the telecommunications network becomes critical national infrastructure requiring protection equivalent to power grids or water systems.

This is where telecommunications intersect uncomfortably with cybersecurity. The same networks carrying birthday wishes and business deals also transmit banking credentials, healthcare records, and government communications. Operation Sindoor in May 2025 demonstrated this vulnerability when attackers launched 200,000 coordinated assaults on India’s power grid, exploiting telecommunications infrastructure to coordinate attacks and exfiltrate data. The telecommunications network wasn’t the target – it was the vector.

The challenge facing India’s telecommunications sector isn’t expanding coverage or reducing costs anymore – we’ve largely solved those problems. The challenge is securing the data flowing through networks that were designed for connectivity first and security second. When cybercriminals send fake traffic challan messages via WhatsApp and dupe vehicle owners in Odisha by tricking them into installing malicious APK files, they’re exploiting telecommunications infrastructure built for openness and accessibility.

Financial services face particular telecommunications security challenges because banking now happens primarily through mobile apps and internet connections rather than physical branches. Finance Minister Nirmala Sitharaman’s recent meetings with bank leaders about AI-powered cybersecurity threats highlight how telecommunications networks carry both legitimate banking traffic and sophisticated attack attempts simultaneously, requiring security solutions that can distinguish between the two in real-time without disrupting service.

Indian telecommunications companies are investing substantially in security infrastructure – network-level threat detection, encrypted voice and data transmission, SIM card authentication improvements, and partnerships with cybersecurity providers to monitor traffic patterns for anomalies. Organizations deploying endpoint detection and response systems now extend that protection to mobile devices accessing corporate resources through telecommunications networks, recognizing that the security perimeter isn’t the office anymore – it’s wherever employees’ phones connect to company systems.

Take, for instance, the Swachh Bharat Abhiyan’s digital hygiene initiative. As part of the same, CERT-In lists eScan as the only provider of a free botnet detection and removal tool for Android devices, addressing the reality that mobile phones – now the primary telecommunications endpoint for most Indians – require the same security attention previously reserved for desktop computers.

Govind Rammurthy, CEO and Managing Director, eScan

The integration of telecommunications and cybersecurity creates interesting technical challenges. Security solutions must operate at telecommunications speed – analyzing millions of connections per second, identifying threats in milliseconds, and blocking attacks without creating latency that degrades user experience. This requires security infrastructure that matches telecommunications infrastructure in scale, speed, and reliability, which is why endpoint security, network security, and data loss prevention systems increasingly function as unified platforms rather than separate products.

India’s telecom sector has already achieved remarkable scale and reach. The next phase of growth will depend on how effectively the country secures the digital infrastructure powering its economy and public services.

The question isn’t whether India can build world-class telecommunications infrastructure – we’ve proven that conclusively. The question is whether we can secure it adequately, because telecommunications networks are only as valuable as the trust users place in them, and trust erodes quickly when networks become conduits for fraud, data theft, or critical infrastructure attacks.