

Article Date	Headline / Summary	Publication
05 Jul 2026	AI rewrites cyber risk as India's enterprises and insurers race to keep up	Fortune India

AI rewrites cyber risk as India's enterprises and insurers race to keep up



Cyberattacks in India are getting faster and harder to predict, and the tools behind them are getting cheaper to use.

India's cyber insurance market is worth an estimated \$580-750 million, a fraction of the global market's \$14.2 billion, according to industry estimates. Meanwhile, CERT-In recorded over 2.04 million cybersecurity incidents in India in 2024 alone, according to a 2025 EY India report on the sector.

Why enterprises still aren't buying

Ask insurers why adoption remains low, and the answers point to how Indian companies think about cyber risk in the first place. "Most Indian companies still approach cyber primarily as an IT issue or a security issue, whereas cyber insurance requires it to be viewed as an enterprise or a business risk," says Evaai Saiwal, head of Cyber & Liability Insurance at Policybazaar for Business. She says a common misconception is that strong cybersecurity removes the need for insurance. "In reality, the two are more complementary in nature. Cybersecurity is designed to reduce the likelihood of an event... It is where cyber insurance is intended to be purchased, and it manages the financial impact."

Amarnath Saxena, chief technical officer – Commercial at Bajaj General Insurance, points to a mix of factors holding the market back. "Many Indian firms, especially small and mid-sized organisations, perceive cyber insurance premiums as high relative to their budgets," he says, adding that companies often prefer to spend on security tools instead of insurance, seeing the two as substitutes rather than complements.

Pallavi Malani, India leader, Insurance Practice at BCG, disagrees that awareness is the real issue anymore. "The awareness problem is largely solved, most boards in India have cyber on their risk register," she says. "The penetration problem persists for a different reason: the product itself is still hard to buy. Pricing is inconsistent across providers, policy wording is not standardised, and India lacks a deep enough bench of actuaries and underwriters trained specifically in cyber risk to price it with credibility."

Some of this is changing. Saiwal says demand has broadened well beyond banks and IT firms since the pandemic, with manufacturers, logistics companies and engineering firms now buying cover too, often because customers or lenders now ask for it as a contract condition.

How a cyber insurance claim actually works

Few enterprises understand what happens once an incident is reported, and that is where the gap between expectation and reality tends to show up.

"In my experience conducting gap assessments, it is common to find that, on paper, a client believes 80–90% of potential loss scenarios are covered," says Bhranti Shah, chief insurance officer at Mitigata Cyber Resilience. "In reality, once sub-limits, waiting periods, business continuity provisions, silent exclusions, and standard policy exclusions are applied, the actual coverage is often significantly lower. One of the biggest reasons is that policy wordings are difficult to interpret, and insurers use different base policy forms."

Saiwal explains that a cyber claim doesn't work like a typical insurance claim. Unlike a fire or theft, where the damage is visible immediately, a cyberattack needs to be investigated before anyone can even say what was lost. Once a company reports an incident, insurers bring in forensic investigators, breach coaches, legal counsel and PR advisers together, not one at a time. The priority in the first hours is containing the attack and preserving evidence, so that the cause and the financial loss can be established properly before a claim is settled.

Saxena adds that manufacturing has become a clear example of why this matters. "One of the most important aspects of cyber-attacks on enterprises is the massive business interruption losses that they incur," he says. "Depending on the severity of the attack, it may take businesses weeks or even months to bounce back to the pre-cyber-attack level of business operations. Having a cyber insurance policy of adequate limit is perhaps the only way these losses can be made good." The EY report backs this up, saying that India ranks second globally in ransomware volume, with average downtime of 21 days per incident.

A threat landscape insurers are still learning to price

Cyberattacks are also changing in a way that is testing how insurers set prices in the first place. "It is changing the frequency curve much faster than most Indian insurers' actuarial models have been able to adapt," Shah says. "Insurers are still relying largely on historical loss data from the pre-AI era... premiums are still underpriced relative to the actual risk." Malani makes a similar point from a different angle. "AI breaks a foundational actuarial assumption--that attack frequency is relatively stable and severity is the main variable to model."

The EY report adds context on where this exposure is concentrated: 61% of breaches in 2023 were linked to third-party vendors, meaning a single weak supplier can affect several companies at once, a growing concern as insurers try to price supply chain risk into policies.

Two cybersecurity firms add sharper, narrower observations. Dr. Sanjay Katkar, joint managing director at Quick Heal Technologies, points out that "AI-enabled attacks are making phishing campaigns more convincing, automating reconnaissance activities, and scaling social engineering attempts with unprecedented speed and precision." Parag Khurana, country manager, India at Barracuda Networks, offers a check on how much of this is genuinely new: "AI allows more cyberattackers to find and exploit more security gaps, faster. AI is a force multiplier rather than a revolution."

How insurers are adapting

Insurers say they are responding by looking well beyond the size of a policy when deciding what to charge and what to cover. "Cyber insurance underwriting practices are evolving in response to the changing landscape of cyber risks," Saxena says. "Insurers now consider several factors, including the exposure of IT systems, their vulnerability to attack, and the coverages selected, not just the policy's sum insured." He adds that enterprises today expect more than a payout: "enterprises now expect insurers not only to indemnify losses but also to provide incident response support, access to vendor networks, and proactive risk assessments."

Raghavendra BV, partner, Cyber Security Consulting at EY India, describes this as part of a wider convergence between security and insurance, with companies increasingly using cyber risk quantification to decide how much cover to buy and insurers using the same data to price it. The EY report notes that premiums rose 50% in 2023 amid rising losses, with insurers becoming more selective about who they cover.

Whether that recalibration keeps pace with how fast attacks are evolving is likely to shape how quickly India's cyber insurance market grows from here.