Experts Warn of Global Breach Risk from Indian Suppliers - Against Invad

Data: 2025-09-25 23:36:51

Autor: Inteligência Against Invaders

Global supply chains could be at risk after a new report revealed a surprisingly high share of Indian

vendors have suffered a third-party breach over the past year.

SecurityScorecard first identified 10 industries in which Indian businesses make key contributions to global supply chains, including semiconductors, electronics, pharmaceuticals and outsourcing. It then singled out 15 Indian companies which are among the top exporters or service providers for foreign businesses and consumers.

The resulting report, *Third-Party Cyber Risks to Global Supply Chains: An Assessment of Key Indian Suppliers,* found that 53% of Indian vendors experienced at least one third-party breach in the past year.

Outsourced IT operations and managed service providers accountedfor 63% of all third-party breaches in the report.Separately, pharmaceutical firms accounted for 42% of publicly reported breaches and 38% of ransomware incidents studied.

Read more on breaches at Indian suppliers: Tata Technologies Hit by Ransomware Attack.

By “third-party breach,” the report means either breaches at these vendors which led to data/infrastructure compromise at one or more other organizations, or that a compromise at another organization exposed data/infrastructure at these vendors.

“In other words, it includes breaches in which the companies on our sample were both unwitting enablers, as well as those in which they were on the receiving end of third-party risk,” the report noted.

Each vendor was given a grade based on their scores across multiple security risk factors, including patching cadence, DNS health, IP reputation, and endpoint, network and app security.

Indian Vendors Show Mixed Cybersecurity Ratings

Almost 27% of Indian vendors were given an “F” cybersecurity rating, the largest share in any SecurityScorecard report to date. However, a quarter (25%) were awarded an “A,” illustrating that best practice does exist in certain organizations.

Networksecurityissues, mismanaged certificates and poor patching were the most common reasons for low ratings.

“India is a cornerstone of the global digital economy,”said Ryan Sherstobitoff, field CTO atSecurityScorecard.“Our findings highlight both strong performance and areas where resilience must improve. Supply chainsecurityis now an operational requirement.”

SecurityScorecard recommended that organizations:

- Continuously monitor third- and fourth-party ecosystems for emerging threats
- Prioritize certificate management and patching, which were the most common areas of weakness
- Pay attention to IT and managed service providers, which are among the highest-risk vendor categories globally
- Use cybersecurity ratings to guide procurement, vendor oversight and ongoing risk management