Healthcare, education, manufacturing sectors see nearly half of cyberattacks: Report

New Delhi: The healthcare sector received the highest number of cybersecurity attacks, with education and manufacturing sectors together accounting for nearly 47 per cent of all detections in India between October 2024 and September 2025, a report said on Monday.

The report from Seqrite, the enterprise security arm of cybersecurity solutions provider Quick Heal Technologies Ltd., said that healthcare and pharmaceuticals alone recorded 3.79 million detections, a 14.24 per cent share of all cyberattacks in the country.

Indian hospitals and clinics "saw a relentless wave of cyberattacks that turned healthcare networks into high-value targets for data theft, extortion, and disruption," the report said.

The report underscored how data-rich, always-on environments have become prime targets for cyberattacks.

Trojans and file infectors together formed nearly 70 per cent of all attacks, while remote access Trojans and loader-based malware were used to compromise pharma R&D data and clinical trial information, signalling clear espionage and IP-theft motives.

Ransomware, though representing less than 1 per cent of total detections, had an disproportionate operational impact. Ransomware detections exceeded 0.81 million, peaking in January 2025 with 185 incidents and 1,13,000 detections. Many of these attacks leveraged phishing, cracked software, exposed remote desktop services, or supply chain vectors, which are the same routes used to infiltrate hospital information systems and disrupt care delivery, the report noted.

"Unlike payment data, which can often be reset or rotated, patient records are permanent. Medical histories, diagnostic reports, prescription records, insurance details, and personally identifiable information cannot simply be 'reissued' after a breach," the report explained.

This permanence makes healthcare data extraordinarily valuable on underground markets and in extortion schemes, where stolen records are weaponized for blackmail, fraud, and long-term profiling.

The report warned that a compromised radiology system can delay diagnosis. "Manipulated lab results can impact treatment. Exfiltrated clinical trial data can undermine years of research investment," it flagged.