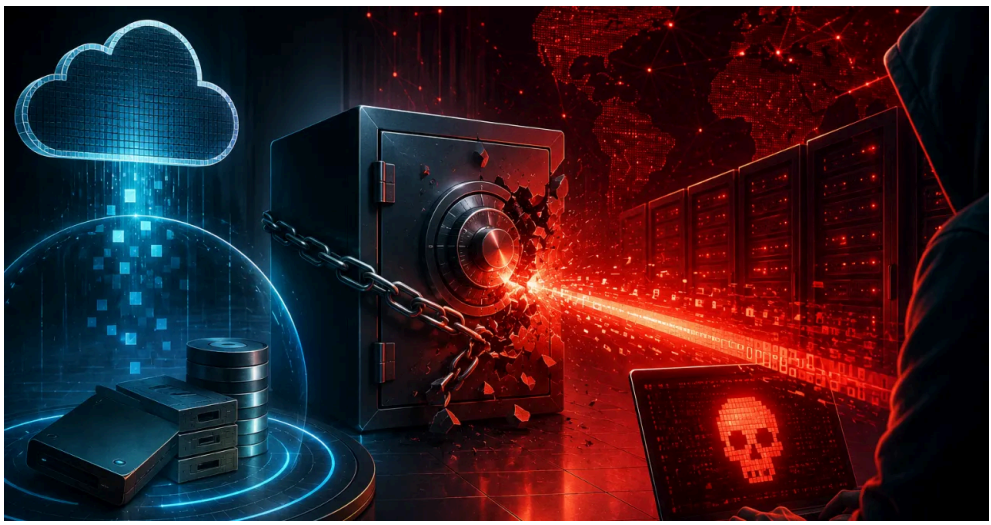
DQ Channels
Solutions for Solution Providers
www.dqchannels.com

Why modern ransomware attacks target backups first - And what organisations miss

India's ransomware attacks rose 55% in 2025 and are expected to rise further. The best defence isn't preventing every attack—it's ensuring recovery via immutable backups, air-gapped copies, and verification.



Why modern ransomware attacks target backups first - And what organisations miss

Ransomware has evolved from an occasional cyber threat into one of the most disruptive business risks facing organisations today. It continues to generate billions in criminal revenue annually while causing greater economic damage through operational disruption, data loss, and recovery costs. India experienced this reality acutely in 2025, with ransomware incidents increasing 55% year-over-year, and the trend shows no signs of reversing.

What makes ransomware particularly insidious is its business model's elegance from an attacker's perspective. Unlike traditional malware that steals data requiring subsequent monetisation, ransomware creates immediate leverage - encrypted files that organisations desperately need back, deadline pressure that prevents careful decision-making, and payment mechanisms through cryptocurrency that obscure money trails. The average ransom demand dropped from 6.00 cr in 2024 to 4.00 cr in 2025, not because attackers became generous but because lower demands increase payment likelihood while maintaining profitability at scale.

Indian organisations make attractive ransomware targets for several converging reasons. First, rapid digitalisation created massive attack surfaces without corresponding security maturity - organisations migrated critical operations to digital platforms faster than they built security expertise. Second, the DPDP Act's regulatory penalties for data breaches create additional pressure to pay ransoms rather than face both recovery costs and regulatory consequences. Third, relatively weak backup practices mean many organisations genuinely cannot recover without paying, which attackers know and exploit.

The statistics paint a sobering picture. AIIMS Delhi suffered ransomware attacks in both 2022 and 2023, disrupting medical education and patient care at one of India's premier healthcare institutions. Jaguar Land Rover's February 2025 attack paused production across multiple facilities. Globally, educational institutions suffered 251 ransomware attacks in 2025, with attackers specifically targeting the education sector because weak backups and assignment deadlines make schools likely to pay rather than rebuild systems during critical academic periods.

Modern ransomware doesn't just encrypt files - it hunts backups first. Attackers spend days or weeks inside networks before deploying encryption, specifically targeting backup repositories, shadow copies, and cloud storage connections. If backup drives remain permanently connected and accessible, they're not really backups - they're just additional targets.

This is where the conversation moves beyond advisory notes about backup importance to practical implementation. The 3-2-1 rule remains valid: three copies of data, on two different media types, with one copy off-site. But implementation details determine whether that backup actually works when ransomware strikes. Automated backups that happen without human intervention, verification testing to confirm backups actually restore successfully, immutable storage that ransomware cannot encrypt or delete, and air-gapped copies that exist entirely separate from network-accessible systems.

Organisations serious about ransomware resilience implement endpoint detection and response systems that identify ransomware behaviour patterns before encryption begins - unusual file access patterns, rapid modification of multiple files, attempts to delete shadow copies, and communication with known command-and-control infrastructure. The goal isn't preventing every ransomware sample from entering the network, which is effectively impossible given attackers' creativity. The goal is detecting and stopping ransomware before it achieves its objective, which requires security infrastructure monitoring of endpoints, networks, and data movement simultaneously.

The conversation about paying ransoms remains ethically and practically complex. Law enforcement agencies universally recommend against payment because it funds criminal enterprises and encourages future attacks. But organisations facing operational shutdown, regulatory penalties, and potentially permanent data loss face decisions that are easy to judge from outside but agonising from inside. The only realistic solution is making payment unnecessary through defence mechanisms that prevent successful attacks and backup systems that enable recovery without giving in to criminal demands.

India's 55% ransomware increase in 2025 suggests we're losing ground rather than gaining it, which means current approaches aren't working adequately. More sophisticated attacks, weaker backup disciplines than organisations admit, security investments focused on prevention rather than resilience, and fundamentally, treating ransomware as a technical problem when it's actually a business continuity problem requiring business-level solutions.

As ransomware attacks continue to escalate in sophistication and economic impact, organisations must ask uncomfortable questions about backup practices, recovery capabilities, and whether they are genuinely prepared for attacks that are no longer theoretical but statistically probable. The best defence against ransomware isn't preventing every attack - it's ensuring attacks fail to achieve their objective because systems recover faster than attackers expect.