DQ Channels
Solutions for Solution Providers

**Seqrite Report flags the rise of human-targeted attacks**

Cyber attackers are using smarter tools, but Seqrite's latest findings show that the easiest openings can still come from people. Social engineering, shoulder surfing and digital deception are putting human behaviour back at the centre of cybersecurity.

Cybersecurity threats are becoming more automated and AI-assisted, but Seqrite's latest findings point to a simpler weakness that remains difficult to secure: people.

The Seqrite report, part of its India Cyber Threat Report 2026, says social engineering remains the top attack vector reported by organisations in India, ahead of malware and web-application attacks. The finding highlights how attackers continue to rely on trust, fear, attention and everyday habits to get past technical defences.

Shoulder surfing shows how simple attacks can start

Shoulder surfing India risks are easy to overlook because they do not necessarily begin with malware or a sophisticated exploit. Someone watching a user enter a PIN, password, UPI credential or sensitive information in an office, café, airport or public transport can collect fragments that may later support a larger fraud or intrusion attempt.

Even a visible notification, employee ID, meeting detail or tax document can become useful when combined with public information and social engineering.

Human-targeted attacks are becoming more convincing

The report also highlights Human-targeted attacks that can begin without traditional malware. Digital honey traps use AI-generated profiles, realistic images and carefully built conversations to establish trust before seeking workplace information, internal documents or private content.

Other campaigns imitate familiar government services and brands. Fake traffic-challan and High-Security Registration Plate websites and apps can push users to share OTPs, payment details, personal identifiers or device permissions. Urgent messages such as "final notice" or "account blocked" are designed to encourage quick action.

Security needs to account for behaviour

The Seqrite report does not suggest that technology is becoming less important. Instead, its findings point to the need for security controls that work alongside human judgement.

Seqrite says behaviour-based technologies detected more than 34 million anomalous events during the reporting period. At the same time, it recommends continuous awareness programmes, phishing and vishing simulations, role-based training, phishing-resistant MFA and behaviour-driven access policies.

For organisations, the practical lesson is that Cyber attack vectors now span both systems and everyday behaviour. Clear-screen practices, privacy filters, device locking and caution while entering credentials in public spaces can reduce exposure to shoulder-surfing security warning risks.

As attacks become more automated, strengthening the human layer becomes part of the security architecture itself. The challenge is not simply stopping malicious software, but making it harder for attackers to turn ordinary human behaviour into their entry point.