ET Edge INSIGHTS

Cyber Security

Why educators and students still don’t back up data and why it matters

Representation image

By Govind Rammurthy
Published April 3, 2026

India’s education sector faces an average of 8,487 cyberattacks per week – nearly twice the global average of 4,368 incidents per organization, according to Research data from January 2026. Yet conversations with students and faculty reveal a striking disconnect: everyone knows backups matter, almost nobody maintains them.

This gap between awareness and action creates an invisible crisis across Indian campuses. Research papers get lost. Dissertations disappear. Years of fieldwork evaporate. And increasingly, ransomware attackers deliberately target educational institutions primarily because their backup practices are weak and they are easy targets.

Why Indian institutions are prime targets

When Unacademy suffered a data breach in 2020, 22 million user accounts were exposed through an unsecured database–and, as per independent sources, subsequently sold on the dark web for just Rs 2 lacs. In 2023, the government-operated Diksha app leaked 1.6 million teachers’ personal information through misconfigured AWS S3 buckets. These weren’t sophisticated state-sponsored attacks – they were opportunistic exploitation of weak security practices and inadequate backup operating procedures.

The 2022 AIIMS Delhi ransomware attack disrupted not just patient records but also medical education. Lecture materials, examination papers, and student assessment data became temporarily inaccessible during a critical academic period. The hospital recovered, but the incident highlighted how academic institutions – despite serving thousands of students – often have backup infrastructure weaker than mid-sized businesses.

According to Research, India's education sector faces 7,095 cyberattacks per organization every week, placing it above government bodies and consumer goods companies in target priority. Student data from these attacks increasingly appears on dark web marketplaces, creating long-term identity theft risks for an entire generation.

The false comfort of cloud sync

Most students believe they're protected because their documents exist in Google Drive or OneDrive. This isn't backup – it's synchronization. When a student accidentally deletes a file, or when ransomware encrypts their local folders and those changes sync to the cloud, the "backup" becomes a perfect copy of the corrupted or deleted data.

Cloud platforms do maintain version history, typically for 30 days. But discovering that critical academic work was accidentally overwritten usually happens during final submission chaos, often weeks after the damage occurred. By then, recoverable versions are gone.

Consider an illustrative scenario: A final-year engineering student at a Bangalore university loses three months of research data because their laptop hard drive fails two weeks before thesis submission. When asked, fewer than 20% of their classmates have any backup system in place for their own academic work. The response is uniform: "That's why you should have backed up." But nobody actually does.

Why educators face worse risks

Faculty members accumulate even more critical data over decades: lecture materials refined over years, student grades and evaluations, research datasets that took months to collect, unpublished papers under review. Yet institutional backup policies rarely extend to individual faculty computers, creating a gap where a decade of academic work exists only on aging laptops.

In an illustrative case, a chemistry professor at a Delhi university loses Friday's exam questions because they were only on the office computer that crashed. A humanities researcher loses interview transcripts because the backup drive sat next to the laptop that was stolen – making it not a backup at all, just an additional target.

The problem compounds because educators frequently work across multiple devices: office desktop, personal laptop, home computer. Important files scatter across locations with no systematic backup connecting them.

The ransomware threat nobody discusses

Modern ransomware doesn't just encrypt your files – it actively hunts for backups to destroy first. Attackers spend days inside networks before deploying encryption, specifically targeting backup repositories, shadow copies, and cloud storage connections. If your backup drives are permanently connected and accessible, they're not really backups – they're just additional targets.

Globally, ransomware gangs took credit for 251 attacks on educational institutions in 2025, with over 3.96 million records breached. Average ransom demands in education dropped 33% from 2024 to 2025 – from 6 crores to around 4 crores – not because attackers became generous, but because lower demands increase the likelihood of payment. Over 241 TB of data was allegedly stolen across all 251 attacks.

Educational institutions face a cruel calculation during placement season or final submissions: pay the ransom to recover student records immediately, or spend weeks reconstructing data while students miss critical deadlines. Many institutions quietly pay rather than admit their backup failures.

The 3-2-1 rule for academic data

The solution remains straightforward: three copies of your data, on two different types of media, with one copy off-site. For students and educators, this translates practically:

- **Primary copy**– Your working files on laptop or desktop
- **Second copy**– Automated local backup to external drive (disconnected when not backing up)
- **Third copy**– Cloud storage (google drive, one drive, dropbox, etc.) with versioning

The key word is "automated." Manual backups fail because humans forget, especially during exam weeks or research deadlines when data loss risk peaks. Many modern security solutions include scheduled backup features as part of their anti-malware protection – configure them once, verify quarterly, and let automation

handle the rest.

Making backup part of digital literacy

Govind Rammurthy, CEO & Managing Director, eScan

Perhaps the real solution needs “educating the educator” to treat backup literacy as essential as plagiarism awareness or citation practices. First-year orientation should include not just college tours and integrity lectures, but practical sessions on protecting academic work. Show students how to configure automated backups. Explain why cloud sync isn’t sufficient. Demonstrate recovery procedures.

With phishing emails surging 224% in the education sector during 2024, and AI-generated phishing showing a 1,265% increase since generative AI tools launched, backup isn’t a precaution **–** it’s essential infrastructure. Colleges invest in learning management systems and digital libraries. Similar investment in ensuring students and faculty can actually protect the work they create would prevent far more data loss than expensive storage infrastructure.

The statistics are clear: India’s education sector faces over 7,000 weekly cyberattacks, student data appears on dark web marketplaces, and ransomware demands average nearly a crore of rupees. The question isn’t whether an institution will face a data loss incident. The question is whether the backups will actually work when they need them.