From backup to resilience: A 2026 data strategy imperative

By **Express Computer** On **Mar 31, 2026**

Govind Rammurthy, CEO and Managing Director, eScan

By Govind Rammurthy, CEO and Managing Director, eScan

Every year, World Backup Day reminds us to back up our data. Every year, most people ignore it. Then ransomware hits, a laptop gets stolen, or a hard drive simply decides it's done working, and suddenly that family photo collection or client project file becomes permanently inaccessible.

The statistics are seriously sobering. India saw a 55% increase in ransomware incidents in 2024, with AIIMS Delhi learning this lesson twice when attacks shut down hospital operations in 2022 and 2023. The February 2025 Jaguar Land

Rover ransomware attack paused production across multiple facilities. These weren't small organisations with amateur IT teams, they were major institutions that still got caught unprepared.

What actually gets backed up?

Here's the uncomfortable truth: most backup strategies fail not because the technology doesn't work, but because people don't understand what they actually need to protect until it's gone.

Your operating system can be reinstalled. Your applications can be downloaded again. Your family photos from 2015, the novel you've been writing for three years, your company's customer database – irreplaceable. Yet when IT teams configure backup systems, they often default to backing up everything or nothing, missing the nuance of what actually matters.

The 3-2-1 rule remains relevant: three copies (or backups) of your data, on two different types of media, with one copy off-site. It sounds simple, but implementation is where most organisations stumble. That external hard drive sitting next to your computer isn't off-site – it's just another device waiting to be encrypted by the same ransomware that hits your primary system. The always-connected and online cloud drive is again a resource waiting to be encrypted. An organisation that had a Microsoft OneDrive subscription backed up data regularly to the cloud. But when ransomware struck, it encrypted all files not only on the local hard drive but also in the cloud OneDrive, as the cloud storage was kept connected to the system!

The ransomware reality

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.

This is why air-gapped or, what we call, "immutable" backups matter. Whether it's a physical drive you disconnect and store elsewhere or cloud storage with versioning that ransomware can't delete, the key is "separation". When a

pharmaceutical company lost access to its distribution network during a 2025 ransomware attack, the difference between a 2-day recovery and 2-week paralysis was whether their backups were truly isolated.

What about cloud storage?

Cloud platforms like Google Drive or OneDrive provide convenient storage, but they're not automatically disaster recovery solutions. If ransomware encrypts your local files and those changes sync to the cloud, you've just backed up the encrypted versions. Version history helps – most platforms retain previous versions for 30 days – but only if you notice the problem before that window closes.

The solution isn't avoiding cloud storage; it understands its limitations. Cloud backup works best when it's part of a layered strategy: local copies for quick recovery, cloud copies for geographic redundancy, and critically, scheduled backups that create point-in-time snapshots rather than just syncing whatever exists on your computer right now.

Making it automatic

The best backup strategy is the one that happens without you remembering to do it. Whether you're using dedicated backup software, cloud services with scheduled snapshots, or security solutions, like eScan, that include automatic backup capabilities, the critical factor is automation with verification.

That last part matters. Running backups is pointless if you never verify they actually work. Schedule quarterly recovery tests. Pick a random file and restore it. Make sure the backup isn't just creating empty archives or syncing corrupted data. A backup you've never tested is a backup you can't trust when ransomware arrives at 2 AM on a Friday.

World Backup Day exists because backups remain the most effective defence against data loss—but only if they're configured correctly, truly isolated, and regularly verified. The question isn't whether you'll need them. It's whether they'll actually work when you do.