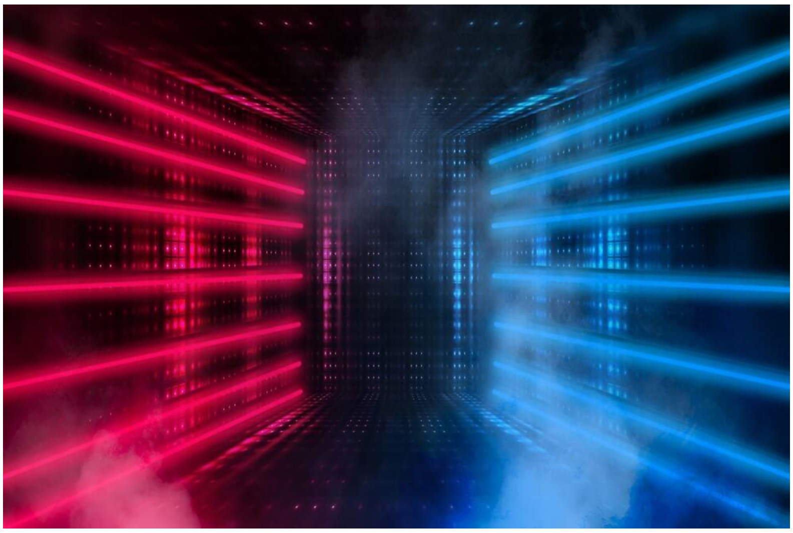
Why most enterprises still fail at data backup?



With cyberattacks and system failures on the rise, poor backup strategies are leaving businesses dangerously exposed. Experts weigh-in on what practices help to avoid data compromises

Despite living in a data-driven era, a startling number of enterprises continue to falter at one of the most fundamental IT practices — data backup. According to a 2024 report by Veeam Software, 76% of organizations worldwide experienced at least one ransomware attack in the past year, but only 55% were able to successfully recover their data without paying the ransom, largely due to inadequate or outdated backup strategies.

The consequences are severe. Global data loss costs reached $4.4 million per incident on average in 2023, as per IBM's "Cost of a Data Breach" report. Yet, shockingly, more than 30% of companies do not test their data recovery plans regularly, and 21% don't have any formal backup strategy in place, according to Gartner. The 2024 Seqrite India Threat Report, compiled by Quick Heal's malware analysis team, revealed that ransomware now accounts for 1 in every 595 detected threats.

"In today's digital-first world, data is the backbone of our lives and businesses," says Vishal Salvi, CEO of Quick Heal Technologies Limited. "Its loss—whether from cyberattacks, system failures, or human error—can be catastrophic. Modern ransomware isn't just about locking systems—it's increasingly designed to steal sensitive data, amplifying the risks of financial losses, operational paralysis, and irreversible damage to customer trust."

Salvi adds that the dual threat of data theft and system lockdown calls for more than just backups—it requires multi-layered cyber resilience. "A robust backup strategy must be reinforced by data encryption, access controls, and regular updates. At Quick Heal and Seqrite, we're committed to making cyber safety a fundamental right."

The common pitfalls in enterprise backup strategies

1. **Misplaced Trust in Cloud and SaaS Providers**
   A large number of businesses still assume their cloud and SaaS data is automatically backed

up. In fact, 74% of organizations believe SaaS vendors are responsible for data protection, according to Backupify. However, these services often offer limited retention policies, creating a false sense of security.

2. **Lack of Testing and Recovery Readiness**
   "Regular testing of backup systems is crucial. The worst time to discover that there is an error in your configuration, or that a setting is incorrect, is right after a ransomware event or when you really need to restore something and can't. Even with easy-to-use systems, companies need to be familiar with how their backup works and should be comfortable with restores—before the pressure is on," warns Parag Khurana, Country Manager, India at Barracuda Networks. He emphasizes that regular testing, malware scanning before restoration, and backing up critical identity systems like Microsoft Entra ID are crucial steps often overlooked.
3. **Human Error and Configuration Gaps**
   As per the Ponemon Institute, 29% of all data loss incidents stem from human error. With increasingly complex hybrid-cloud infrastructures, many enterprises struggle to set up and maintain backup protocols across platforms, leading to gaps and misconfigurations that only surface during a crisis.
4. **Regulatory Blind Spots and Lack of Proactivity**
   "In India, with the implementation of the Digital Personal Data Protection (DPDP) Act, organizations must adopt a proactive approach to data protection," notes Shankar Iyer, Director – Business Strategy, India at Infobip. "Regular backups, end-to-end encryption, and AI-powered fraud prevention are essential strategies to safeguard sensitive information and ensure compliance."
5. **Complexity of Modern Data Environments**
   Hybrid and multi-cloud infrastructures have made backup and recovery far more complex. A recent survey by ESG Research found that 62% of IT leaders struggle to manage data backups across different platforms, from on-premises servers to multiple cloud environments.
6. **Over-Reliance on SaaS**
   Many enterprises mistakenly believe that data stored in services like Microsoft 365 or Google Workspace is automatically backed up. In reality, these platforms have limited retention policies, and 74% of businesses wrongly assume SaaS providers are responsible for long-term data protection, as noted by a 2024 Backupify report.

A wake-up call for Indian businesses

Industry experts are calling for a cultural shift in how organizations perceive data protection. It's not just an IT concern — it's a business-critical strategy. Key recommendations include:

- **Automating backups** and conducting regular recovery drills
- **Allocating dedicated budgets** for data resilience and security
- **Ensuring backup strategies cover all environments** (on-prem, cloud, edge)
- **Training staff** on data handling and the risks of mismanagement

As cyber threats escalate and regulatory scrutiny tightens, businesses that neglect their backup strategies risk not just data loss, but irreparable reputational and financial damage.

"Data isn't just information—it's the backbone of operations," says Zaiba Sarang, Co-founder, iThink Logistics. "Losing it means losing control over supply chains, customer trust, and business continuity. On World Backup Day, let's reaffirm our commitment to intelligent storage and proactive backups that ensure resilience against cyber threats and downtime."

Industry leaders agree data backup is no longer optional, it’s foundational. It must go hand-in-hand with cybersecurity frameworks, employee training, and clear data ownership policies.

Looking ahead: The call to action

Salvi highlights how anti fraud AI tools alerts users when their data is breached, along with enterprise-grade solutions like ZTNA and EPP, to protect both consumers and businesses.

“Let’s prioritize multi-layered protection and a security-first mindset—because preparation today prevents disruption tomorrow,” Salvi urges.

Meanwhile, Iyer points out that data protection is not just a compliance checkbox but a strategic differentiator. “By investing in resilient infrastructure, companies can mitigate risks and drive long-term growth. Ensuring data integrity will be key to building a secure and transparent digital economy.”

As the frequency and sophistication of cyberattacks rises, enterprises can no longer afford to treat backups as an afterthought. From ransomware to regulatory compliance, the risks are real—and the solutions are within reach. But it starts with a mindset shift: from reaction to preparation