THE TIMES OF INDIA

How to continuously protect data

Sanjay Katkar

In today's digital age, data backup is crucial for businesses to protect their valuable information from loss or damage due to various threats, such as cyberattacks, hardware failure, and natural disasters. However, with the increasing frequency and sophistication of cyber threats, data privacy has become an equally critical aspect of any backup strategy.

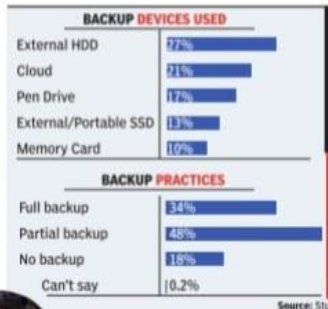
MARCH 31:
WORLD BACKUP DAY



Knowing where personal identifiable information (PII) is used and stored is a crucial aspect of any backup strategy, as a breach or leakage of such data is liable for prosecution or fines under various data privacy regulations. At the same time, it's extremely important to ensure that your data is encrypted and is not stored in multiple places, making it prone to attacks. Therefore, businesses must not only focus on backup and recovery, but also ensure the protection of PII data.

Continuous data protection (CDP) offers real-time or near-real-time backup and recovery of data, providing continuous protection against data loss or corruption. CDP captures every change made to the data and stores it in a separate location, ensuring businesses have access to the most up-to-date version of their data in case of data loss or corruption. CDP also offers faster recovery times and a higher level of data integrity by capturing every change made to the data.

BACKUP DEVICES USED

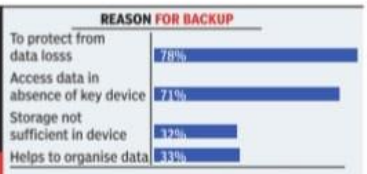


BACKUP PRACTICES

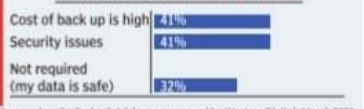


HOW INDIANS BACKUP DATA

REASON FOR BACKUP



KEY REASONS FOR NOT BACKING UP



Source: Study on data storage habits of PC users done by Feeback Advisory, sponsored by Western Digital; March 2023

Knowing where personal identifiable information (PII) is used and stored is a crucial aspect of any backup strategy.

Implementing a clear and comprehensive data backup policy that outlines the frequency of backups, the types of data to be backed up, and the storage location is essential. Regular testing of backups should also be conducted to ensure they are working correctly and can be used to recover data in case of data loss or corruption.

Businesses should train their employees on the importance of data protection and best practices for data backup and recovery. It's also essential to monitor who has access to data and ensure that only authorised personnel can modify or delete data. Like I said earlier, data must be encrypted at all times and must not be stored at multiple endpoints. Additionally, businesses must comply with data privacy regulations such as GDPR and CCPA to protect PII data adequately.

Sanjay Katkar is joint MD & CTO of Quick Heal Technologies