TECHCiRCLE

OUR IT INSIGHTS & CONSULTING

Search for... 🔍

TECHNOLOGY ▾   STARTUPS ▾   MONEY ▾   CXO FOCUS   POLICY   ANALYSIS   PEOPLE   THE CIO COMMUNITY   EVENTS

TECHNOLOGY   SECURITY

How CXOs can win the battle against data loss

Photo Credit: Pixabay

Sohini Bagchi | 31 Mar, 2022

[f] [X] [in] [wa]

MOST POPULAR

PEOPLE

Women's Day: Mid, senior-level women techies need more role models, upskilling opportunities

Shraddha Goled   7 Mar, 2023

TECHNOLOGY

AI governance should be an intrinsic part of tech skilling: Geeta Gurnani, IBM

Losing data—whether it's a work project, financial or legal document or some personal information—it can be devastating because it not only leads to inconvenience, but also imposes a great security threat on users.

From hard drive failures or cyber-attacks to human error or theft—data losses can occur in many ways. According to a March 2021 global survey by cybersecurity firm Acronis, over 76% of organisations suffered unexpected downtime and subsequently data loss due to system crashes, cyber attacks or thefts, power fluctuations, and human error, resulting to accidental deletion. All these data suggests the need for organisations to have a robust backup/recovery and a data loss prevention strategy.

Sandeep Bhambure, Vice President, Veeam Software – India & SAARC, a US-based company in the data protection space, said, "It is evident that the dependency of businesses on data, and the amount of data generated by them is consistently growing. This is creating new challenges for organisations of all sizes, making them even more vulnerable to cyberattacks."

He quoted the Veeam Data Protection Report 2022, where Indian organisations were unable to recover 36% of their lost data on average and 90% of organisations were unable to recover at least some of the data they had lost.

Ripu Bajwa, Director and General Manager, Data Protection Solutions, Dell Technologies India, too mentioned that nearly two-thirds IT decision-makers they spoke to lack confidence that they will recover all systems or data to meet SLAs following a data loss. According to him, "With more and more businesses running workloads in a hybrid environment today, it is critical to securely store data in multiple spaces like databases, file servers, and network-attached storage (NAS)."

There are other reasons to be wary about in the digital world as Kumar Vembu, CEO and Founder of Gofrugal, said, "What most of us fail to notice, far less comprehend, is the lurking dangers and sneaking threats that we invite unintentionally. We hardly realise that using our own personal information to create personalised experiences can be a dangerous thing."

SUBSCRIBE TO NEWSLETTERS

Enter email for newsletters | >

There is clearly evident in last year's KPMG survey published in August that reported 86% of consumers are becoming more sceptical and wary about the data collection practices of corporations.

"If not handled in a sensitive, the growing platforms using artificial intelligence (AI) to augment our choices and our preferences can invade data privacy and also amount to data loss," Vembu said, adding that nine out of 10 small and medium size retail and distribution businesses are not even aware of the impact of data loss and its protection today and often the backup methods are not regular. Sometimes even a day's or week's day is lost because of manual methods.

But whether it's a natural event, human error, cybercrime, or provider outage, inability to access data, data loss in general comes at a cost. A 2019 study found the global average cost of data loss was around $3.6 million and cybersecurity and data backup company Datto reported that depending on a company's size, downtime costs can range from $10,000 per hour to more than $5 million per hour.

What is more alarming is that data loss isn't just about financial recovery costs-- there are also a number of consequences that can seriously impact a business' overall finances, reputation, and productivity. If the loss is the result of a breach, you can also add the costs for forensic activities and the expenses associated with notifying customers and regulatory agencies. In the end, it will have a detrimental effect on your revenue and cash flow."

However, there are options in which you can avoid data loss and protect your data, as Rajesh Awasthi, Vice President & Business Head, Global - Cloud, Hosting & Managed Services, Tata communications, believes that IT leaders should update their data protection and recovery practices to keep pace with today's cybersecurity landscape in which we're navigating a distributed and ever-changing world of work. He suggested, businesses should have a robust backup strategy in place that needs to go beyond just preventing or warding off data loss, but guarantees at least 99.9% uptime and shares exhaustive reporting, providing full visibility. In that sense, businesses need to evolve from backing their data up to tapes or managing it onsite

to a cloud-based solution that offers reliability, performance, and most importantly, security and backup at a scale. But again, again companies should evaluate vendors carefully on three aspects: their network, their infrastructure and their security practices.
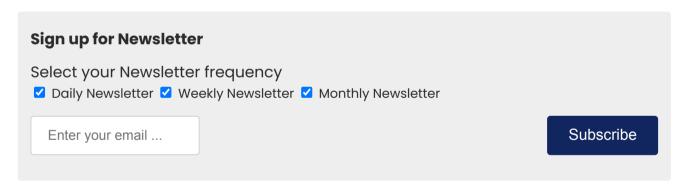
"It is imperative that enterprises invest the time and money into ensuring their protection and backup strategies are at par with the rest of their digital transformation strategy, and not as an afterthought," Awasthi said.

It is also important for security leaders to create a culture that builds trust and confidence among employees and improves security behaviour, by providing people with the support and information they need to make safe decisions at work, he said.

Leave Your Comment(s)

Data Loss, Data Protection, Cybercrime, Data Backup,

❙ TRENDING STORIES