

Businesses Failing to Protect Sensitive Data in the Cloud, Report Reveals

A new [global study from Thales](#) and research from the [Ponemon Institute](#) has revealed an increasing difference between a company's security approach to sensitive data and speedy growth of data storage in the cloud.

The latest research showed that nearly half of corporate data is stored in the cloud - a 35% increase from three years ago. However, only a third of organizations use a secure approach to data storage.

It also found that 31% of organizations in eight countries—Australia, Germany, UK, Brazil, France, India, Japan, and the US—take responsibility when it comes to protecting data stored in the cloud.

Increased usage of multi-cloud, but it comes with risks

Though 35% of organizations believe that cloud-based services largely bear the responsibility for sensitive data security, they are becoming more dependent on cloud providers and do not consider security a major factor in selecting them.

Nearly half of businesses possess solutions from the top three multi-cloud strategies—Amazon Web Services (AWS), Microsoft Azure and IBM—while over 28% are using four or more. The study also found that 29 cloud applications are being used on average, compared to 27 two years ago.

Additionally, 46% of over 3,000 IT and IT security practitioners shared that consumer data storage in a network of remote servers makes it more of a security risk, and 56% stated that it posed a compliance risk.

Not knowing where the data is stored may leave firms at risk, making it impossible to protect the stated stored in the cloud. Though businesses put the responsibility to cloud providers, only 23% say security is a key factor in handpicking them.

Encryption is increasing, but businesses are handing over keys to cloud providers

Regardless of the provider, various organizations still seem to be taking responsibility for the security of their data. They're insufficiently addressing data security despite the options a new cloud offers. The majority of those that still do not use encryption for data security make up 51% of organizations. More than half (66%) of German organizations were revealed to be the most advanced when it comes to the use of encryption.

Approximately 44% of cloud companies provided the encryption keys to cloud providers when data is already converted in the cloud, followed by in-house teams (36%) and third parties (19%). But 53% are self-controlling these keys, and 78% say it's important to retain ownership of the encryption keys.

Over half of businesses increasingly cited that cloud storage makes it difficult for them to securely protect data that is sensitive. Organizations also seem to struggle to reduce the complexity of managing privacy and data protection regulations, according to more than 70%. Two-thirds say they struggle when applying conventional security methods in the cloud.

The study also revealed that the three biggest amounts of data stored are: customer information (60%), customer emails (48%) and consumer data (46%).

<https://www.forbesmiddleeast.com/businesses-failing-to-protect-sensitive-data-in-the-cloud-report-reveals>