Assuming responsibility for data protection in the cloud

Author: John Michael, CEO iStorage

Given the responsibility to ensure data protection in the cloud, how can organisations encrypt, share and manage data securely?

Data protection is of top priority for business leaders and consumers alike. The implementation of GDPR and the extensive media coverage of major data breaches has made organisations more mindful of their responsibility to ensure data protection. Despite the numerous benefits of cloud usage, many are reluctant to migrate to the cloud as they feel storing data off-premise robs them of the control needed to ensure its security, thus exposing their organisation to the risk of being faced with hefty GDPR fines, job losses or suffering substantial brand damage.

The Liability Clause

A recent study reveals that, alarmingly, only 32% of organisations believe that protecting data in the cloud is their own responsibility. The terms and conditions of major cloud providers includes a "Limitations of Liability" clause which puts data security responsibility on the cloud user. For example, AWS states it accepts no liability in the case of "any unauthorised access to, alteration of, or the deletion, destruction, damage, loss or failure to store any of the user's content or other data."

Those responsible for cloud infrastructure in an organisation generally understand the risks involved with storing data in the cloud. However, all users of the cloud need to be conscious of the severity of protecting data in the cloud.

Hackers are devising many sophisticated methods to target innocent and vulnerable users, making human error prevalent amongst data leakage incidents.

Who guards the encryption key?

It has often been said that data is the new oil. Data can provide valuable insights that drive key business decisions, political campaigns and marketing initiatives. Just as the oil industry has security measures in place to protect against terrorism and maritime piracy, organisations need to establish security measures to ensure the protection of their data. One vital step is encryption.

More than half (51%) of organisations fail to use encryption to protect sensitive data in the cloud. Arguably, most cloud providers will encrypt its customers' data. However, the encryption key is stored in the cloud and thus accessible to hackers and cloud staff – much like leaving your house key under the doormat that half the neighbourhood knows about. Interestingly, Apple was recently pressured by the FBI to abandon its plans to fully encrypt its iCloud backups as it did not give the FBI a backdoor. Recall the liability clause? Full encryption of data cannot be dependent on the cloud provider.

To be a truly secure solution, the user needs full and secure control of the encryption key that is stored away from the data. This will protect the data even if the cloud account is hacked.

"

organisations need to establish security measures to ensure the protection of their data

"

Controlling data shared in the cloud

The more people the data is shared with, the greater the challenge to ensure security. Sharing encrypted data securely allows for instant collaboration in the cloud, saving time in what would be days of posting encrypted USB flash drives to and from colleagues. By keeping the encryption key, which is encrypted itself with a PIN authenticated code, away from the cloud increases the number of security measures from just one authentication, the cloud account login, to up to a five-factor authentication.

Another important step to ensuring data privacy is a central management of data shared. Not being able to efficiently monitor and manage data can have severe implications. For example, an engineer at Raytheon Missile Systems took US missile defence secrets to China, despite warnings from officials not to travel with his laptop. This incident could have been avoided if Raytheon had been able to remotely disable the engineer's access to the confidential files, place geofencing restrictions or monitor file activity.

The cloud is here to stay and shouldn't have to be avoided for security concerns. At an age when sensitive data needs to be stored and shared digitally, businesses and particularly government institutions must assume responsibility for encrypting sensitive data, securing the encryption key and monitoring and managing that data.

Click here to discover your solution to encrypt, share and manage your data in the cloud.

iStorage®

iStorage is the trusted global leader of award-winning, PIN authenticated, hardware encrypted portable data storage & cloud encryption devices. iStorage offers the most innovative range of products to securely encrypt, store and protect data to military standards; safeguarding valuable and sensitive data to ensure compliance with stringent regulations and directives such as GDPR, HIPAA, SOX, NRC, GLB and DHS Initiatives. Today, iStorage products are used by government, military, multinational corporations as well as consumers in over 50 countries, with the mantra that encryption is an essential commodity required by all.