

Big Data vs Data Protection – Can the Cloud Be the Answer for Financial Services?

Financial services organisations continually collect increasing volumes of data of greater variety with higher velocity. Back in 2001, Gartner defined big data by those three Vs. This vast collection of sensitive information, which can include bank account details and personally identifiable information (PII), is subject to regulatory compliance, such as the GDPR in the European Union, the recently revised DPA in the United Kingdom, CCPA in California or 23 NYCRR 500 in New York (which all apply to third parties working with businesses based in those locations). Although the cloud can offer excellent storage solutions, caution to comply with data regulations and concerns over cloud security mean many FS organisations are reluctant to make the move.

Failure to keep data stored in the public cloud confidential can be derived from several issues. This can include a lack of secure encryption, human error when sharing data, unauthorised access or inefficient central management of data stored and shared.

Financial Services fall behind the cloud boom

A study reveals that around 70 per cent of financial services organisations' cloud projects are in the initial "trial and testing" stage, lagging behind other sectors. What is the reason behind such hesitation? More than 60 per cent cite security to be the main factor driving cloud deployment decisions, along with data security and compliance as top considerations.

This is of little surprise given the abundance of data breaches regularly reaching headlines. One that may come to mind is Capital One which, in 2019, suffered one the biggest all-time data breaches, affecting approximately 100 million individuals in the United States and around 6 million in Canada. A former Amazon employee stole credit card application data, including around 80,000 bank account numbers and 140,000 social security numbers, which were stored on AWS servers. AWS stated, "the attack occurred due to a misconfiguration error at the application layer of a firewall installed by Capital One." Finger-pointing aside, the attack certainly renewed concerns over cyber security in the cloud.

Is cloud investment a wise move?

Traditional banks struggle to let go of their on-premise legacy systems due to IT complexity. Nonetheless, the cloud remains on the horizon for traditional banks not already using the cloud, keen on the prospect of having a simplified IT infrastructure, lowering costs, increasing agility and boosting innovation.

"

which can include bank account details and personally identifiable information (PII), is subject to regulatory compliance

"

According to research by The Economist, almost three quarters (74%) of experts say the cloud will be a major factor in the banking sector in 2020. A multi-cloud architecture is the preferred approach for more than half of FS organisations, as it can help with application performance and meet regulatory needs. Meanwhile, several challenger banks, including Monzo, Starling and Tandem, are built on the public cloud.

Whilst FS organisations are to be commended for keeping up the digital pace, they are also wise not to hastily follow their lemming gene and rush to the cloud for fear of digital bankruptcy and falling behind competition. Data protection and privacy are critical factors to consider.

Vault data in the cloud

To ensure data privacy when faced with common threats, such as DDoS and malware attacks, data must be encrypted before it is sent to the cloud, in transit and at rest. The EU's own online information on the GDPR advises, "encryption is the best way to protect data during transfer and one way to secure stored personal data. It also reduces the risk of abuse within a company, as access is limited only to authorised people with the right key."

State of the art encryption can make or break a business in the event of a data breach. The terms and conditions of major cloud service providers include a "Limitations of Liability" clause which puts data security responsibility on the cloud user. Since the cloud user is liable, businesses must take their own measures to ensure data protection and privacy. If the data breach in question falls under the GDPR, the authorities must positively consider "any action taken by the controller or processor to mitigate the damage suffered by data subjects" as per Article 83 (2)(c). Simply put, encrypting data to a high standard could potentially knock off several thousand euros off a data breach fine or even avoid one entirely.

A recent study found that an alarming 43% of cloud databases are not encrypted. Whether the confidential information is stored on a local computer, on a local network, sent via email or file sharing service or shared in the cloud, it is essential the data is securely encrypted. For ultra-secure encryption, data should preferably be encrypted with a FIPS certified randomly generated AES 256-bit encrypted encryption key.

Ensuring authorised access to data

In the FS sector, highly sensitive information is shared internationally across branches and offices, as well as with third party organisations. Failing to enforce corporate authentication standards makes it easier for attackers to access the corporate network via a remote office. To be a truly secure solution, the user needs full and secure control of the encrypted encryption key that is stored away from the data. This will protect the data even if the cloud account is hacked.

Keeping the encryption key 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. It is worth noting that multi-factor authentication and encryption are requirements under 23 NYCRR 500.

How can security standards be upheld when sharing data with third parties? Rather than settle with server-side encryption, organisations should provide authorised users a copy of the encrypted encryption key to access files in the cloud. This will oblige all who access the data, whether the individual works remotely or for a third party, to follow a multi-factor authentication security procedure.

A warning example is that of Nedbank. Its own network wasn't compromised, but its marketing contractor's network was. The data breach affected around 1.7 million Nedbank customers. An additional advantage of sharing encrypted data securely is that it allows for instant collaboration in the cloud, saving time in what, alternatively, would be days of posting encrypted USB flash drives to and from colleagues.

"the user needs full and secure control of the encrypted encryption key that is stored away from the data"

A holistic view and central management of data

Controlling authorised access is another challenge when dealing with an extensive and ever-growing amount of confidential information. Returning to the example of Capital One's data breach, though the breach was internal, "the fact still remains that safeguards were missing that allowed for the illegal access of consumers' names, social security numbers, dates of birth, addresses and other highly sensitive, personal information," as noted by the New York attorney-general.

Handing authorised users a physical encrypted encryption key will contribute to reducing the risk of data loss due to human error. Still, this does not eliminate the possibility of human error. For example, an individual may lose the encrypted encryption key or be dismissed and keep the encryption key. This is where central management is needed.

Those responsible for cloud and data security in the organisation should be able to monitor file access, set geo-fencing and time fencing restrictions, encrypt file names and disable users' access to the data remotely. This will go a long way in eliminating security risks in the cloud.

As financial services organisations continue to collect increasingly more data, the cloud can be a viable solution to the big data and data protection dichotomy. However, the cloud will only be useful in this regard as long as surpassing security measures are enforced. Big data and data protection will not contradict each other, but instead should go hand-in-hand. High quality data encryption and effective control of access to sensitive information can subside the consequences of a data breach, avoid hefty fines and earn customer trust. Now more than ever, data is the financial services industry's lifeblood; it is only logical that it is thoroughly protected.



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.