Cloud Storage Isn’t As Safe As You Think. Here’s How to Avoid a Costly Data Disaster.

Opinions expressed by Entrepreneur contributors are their own.

Key Takeaways

- Storing data in the cloud does not automatically make it safe. The infrastructure is physical and vulnerable to attacks, failures and human error.
- Cloud providers manage the infrastructure’s security, but customers are responsible for protecting their own data within that infrastructure through backups, recovery tools, encryption, etc.
- Companies must also enforce strict access management and conduct regular audits and inspections.

One of the biggest misconceptions about cloud storage is that if your data is in the “cloud,” it’s safe. Unfortunately, that is not how data security works. A cloud server is not something in the sky that is intangible.

Cloud infrastructure is built on actual servers, physical data storage devices and other hardware components that are as susceptible to attacks and failures.

Therefore, while cloud service providers build and manage the infrastructure, the responsibility for data security, integrity and recovery is not solely on them (read their terms and conditions, and you will be surprised).

Related: Is My Data Really Safe? Your Questions About Cloud-Based Storage, Answered.

Cloud does not always mean automatic safety

Some of the largest cloud providers build their solutions around reliability, ensuring uptime is as close to 100% as possible and making sure their hardware is up to date and fit for purpose.

While GDPR compliance and data protection laws put some pressure on cloud service providers to safeguard your data, recent events have confirmed that this is not enough.

As recently as July 2025, Microsoft servers were attacked, and earlier in the year, Oracle's cloud servers were hacked twice, which led to healthcare information of more than 14,000 people being stolen. Both Microsoft and Oracle claim to have the most robust cloud services with a clientele that includes the world's large corporations and even government agencies.

Global education giant Pearson suffered from a cyberattack, which led to the loss of terabytes of data from their AWS and Google Cloud. Both of these are the largest and the third largest providers of cloud services in the world, respectively.

With so many incidents taking place at such frequency, we have to dispel the myth that simply because your data is on the cloud, you have automatic backups and recovery.

We need to think about shared responsibility and take some direct measures to protect our cloud data.

Threats to cloud data

Threats to cloud data can come in a number of ways. Simple human error plays a huge part; in fact, some studies suggest that human error alone accounts for over 88% of all data breaches, accidental deletions and lost data, making it essential for all companies to have some kind of data recovery tools.

The internet is also full of ransomware and malware that creeps into synced cloud storage and not only attacks main servers, but also spreads to other networks.

According to one study, ransomware attacks cause $57 billion of damage every year.

Ultimately, many companies have lost data simply by choosing an unreliable cloud service provider or have become victims of "revenge attacks" from estranged employees.

Related: Is Your Company's Data Safe in the Cloud? (Infographic)

Your responsibility to protect your own cloud data

1. Understand the shared responsibility model

Start by making sure you work with a reliable cloud provider and become familiar with their shared responsibility model. A shared responsibility model is a cybersecurity framework that establishes who is responsible for different aspects of a cloud computing infrastructure.

The responsibilities are shared between a provider and a customer, and understanding them is important. In a nutshell, this is what it looks like:

Provider's role: Build and manage cloud infrastructure, protect the hardware, and ensure uptimes for customers. This can encompass a lot of other activities, including network maintenance, configuration settings, etc.

Customer's role: Build your own data backups, use and test data recovery tools, use encryption, etc.

All large cloud providers, including Google and AWS, have shared responsibility models as part of their agreements.

2. Data governance

Customers are responsible for their own data governance – a framework that sets the policies and standards for organizations to manage their data as a strategic asset. This basically encompasses an internal set of rules that establishes how data is gathered, stored, secured and disposed of.

While data governance is built around a basic model, every organization manages its data slightly differently depending on the kind of data they have, its importance and the company's overall IT budget.

3. Data encryption

Encrypting sensitive information before uploading it to the cloud is one of the best methods to protect your data. By using either end-to-end encryption tools or client-side encryption, your sensitive data is scrambled and turned into unreadable strings that can only be recovered with a safe key.

This added layer of security is powerful, so much so that if your cloud provider's servers are hacked and your data stolen, it can never be used or be readable to a hacker.

4. Access management against human errors

One of the easiest ways to protect your data is to limit human

error and apply strict access controls. This will include taking several measures, starting by ensuring multi-factor authentication for all kinds of access to ensure ID verification.

Work on role-based access controls, which limit the number of people who have access to specific data, based on their job description. This also allows the possibility of tracking data management under each role, adding an extra layer of scrutiny. This small fix alone might save you tons of money and time.

5. Audits and inspections

Like any other aspect of business operations, it’s important to conduct regular audits and inspections to ensure your cybersecurity is up to date.

This includes testing your backup systems, data recovery tools, and developing and evaluating crisis strategies.

All of this is done to ensure your organization is prepared, your data is protected and you are able to minimize risks and leaks.

According to a recent study by CrowdStrike, attacks on cloud data have increased by 75% in just one year.

Related: Why CEOs Should Absolutely Concern Themselves With Cloud Security

At the same time, for most businesses, the importance of cloud computing has only increased. For some corporations, cloud computing can cost up to 5% of their revenue, while for startup SaaS companies, it can be as high as 90%.

Therefore, financing a bit more to make sure this essential business component is secure, recoverable and safe is the best investment that you can make.

Key Takeaways

- Storing data in the cloud does not automatically make it safe. The infrastructure is physical and vulnerable to attacks, failures and human error.
- Cloud providers manage the infrastructure’s security, but customers are responsible for protecting their own data within that infrastructure through backups, recovery tools, encryption, etc.
- Companies must also enforce strict access management and conduct regular audits and inspections.

One of the biggest misconceptions about cloud storage is that if your data is in the “cloud,” it’s safe. Unfortunately, that is not how data security works. A cloud server is not something in the sky that is intangible.

Cloud infrastructure is built on actual servers, physical data storage devices and other hardware components that are as susceptible to attacks and failures.

Therefore, while cloud service providers build and manage the infrastructure, the responsibility for data security, integrity and recovery is not solely on them (read their terms and conditions, and you will be surprised).

https://www.entrepreneur.com/science-technology/why-storing-data-in-the-cloud-isnt-as-safe-as-you-think/496540