Cloud security is tight, but it's not infallible. Cybercriminals can get into those files, whether by guessing security questions or bypassing passwords. But the bigger risk with cloud storage is privacy. Even if data isn't stolen or published, it can still be viewed.

Security issues:-

1. Data Breaches

Cloud computing and services are relatively new, yet data breaches in all forms have existed for years. The question remains: “With sensitive data being stored online rather than on premise, is the cloud inherently less safe?”

A study conducted by the Ponemon Institute entitled “[Man In Cloud Attack](http://go.netskope.com/rs/netskope/images/Ponemon-DataBreach-CloudMultiplierEffect-June2014.pdf)” reports that over 50 percent of the IT and security professionals surveyed believed their organization’s security measures to protect data on cloud services are low. This study used nine scenarios, where a data breach had occurred, to determine if that belief was founded in fact.

After evaluating each scenario, the report concluded that overall data breaching was three times more likely to occur for businesses that utilize the cloud than those that don’t. The simple conclusion is that the cloud comes with a unique set of characteristics that make it more vulnerable.

2. Hijacking of Accounts

The growth and implementation of the cloud in many organizations has opened a whole new set of issues in account hijacking.

Attackers now have the ability to use your (or your employees’) login information to remotely access sensitive data stored on the cloud; additionally, attackers can falsify and manipulate information through hijacked credentials.

Other methods of hijacking include scripting bugs and reused passwords, which allow attackers to easily and often without detection steal credentials[. In April 2010 Amazon](http://www.theregister.co.uk/2010/04/20/amazon_website_treat/) faced a cross-site scripting bug that targeted customer credentials as well. Phishing, keylogging, and buffer overflow all present similar threats. However, the most notable new threat – known as the [Man In Cloud Attack](https://www.skyfence.com/blog-new-cloud-threat-for-2015/) – involves the theft of user tokens which cloud platforms use to verify individual devices without requiring logins during each update and sync.

3. Insider Threat

An attack from inside your organization may seem unlikely, but the insider threat does exist. Employees can use their *authorized* access to an organization’s cloud-based services to misuse or access information such as customer accounts, financial forms, and other sensitive information.

Additionally, these insiders don’t even need to have malicious intentions.

A study by Imperva, “[Inside Track on Insider Threats](https://www.imperva.com/lg/lgw.asp?pid=477)” found that an insider threat was the misuse of information through malicious intent, accidents or malware. The study also examined four best practices companies could follow to implement a secure strategy, such as business partnerships, prioritizing initiatives, controling access, and implementing technology.

4. Malware Injection

Malware injections are scripts or code embedded into cloud services that act as “valid instances” and run as SaaS to cloud servers. This means that malicious code can be injected into cloud services and viewed as part of the software or service that is running within the cloud servers themselves.

Once an injection is executed and the cloud begins operating in tandem with it, attackers can eavesdrop, compromise the integrity of sensitive information, and steal data. [Security Threats On Cloud Computing Vulnerabilities](http://airccse.org/journal/jcsit/5313ijcsit06.pdf), a report by the East Carolina University, reviews the threats of malware injections on cloud computing and states that “malware injection attack has become a major security concern in cloud computing systems.”

5. Abuse of Cloud Services

The expansion of cloud-based services has made it possible for both small and enterprise-level organizations to host vast amounts of data easily. However, the cloud’s unprecedented storage capacity has also allowed both hackers and authorized users to easily host and spread malware, illegal software, and other digital properties.

In some cases this practice affects both the cloud service provider and its client. For example, privileged users can directly or indirectly increase the security risks and as a result infringe upon the terms of use provided by the service provider.

These risks include the sharing of pirated software, videos, music, or books, and can result in legal consequences in the forms of fines and settlements with the U.S. Copyright Law reaching up to $250,000. Depending on the damage, these fines can be even more cost prohibitive. You can reduce your exposure to risk by monitoring usage and setting guidelines for what your employees host in the cloud. Service providers and legal entities, such as CSA have defined what is [abusive or inappropriate behavior](https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf) along with methods of detecting such behaviors.

6. Insecure APIs

Application Programming Interfaces (API) give users the opportunity to customize their cloud experience.

However, APIs can be a threat to cloud security because of their very nature. Not only do they give companies the ability to customize features of their cloud services to fit business needs, but they also authenticate, provide access, and effect encryption.

As the infrastructure of APIs grows to provide better service, so do its security risks.  APIs give programmers the tools to build their programs to integrate their applications with other job-critical software. A popular and simple example of an API is YouTube, where developers have the ability to integrate YouTube videos into their sites or applications.

The vulnerability of an API lies in the communication that takes place between applications. While this can help programmers and businesses, they also leave exploitable security risks.

7. Denial of Service Attacks

Unlike other kind of cyberattacks, which are typically launched to establish a long-term foothold and hijack sensitive information, [denial of service](https://www.imperva.com/learn/application-security/denial-of-service/) assaults do not attempt to breach your security perimeter. Rather, they attempt to make your website and servers unavailable to legitimate users. In some cases, however, DoS is also used as a smokescreen for other malicious activities, and to take down security appliances such as web application firewalls.

8. Insufficient Due Diligence

Most of the issues we’ve looked at here are technical in nature, however this particular security gap occurs when an organization does not have a clear plan for its goals, resources, and policies for the cloud. In other words, it’s the people factor.

Additionally, insufficient due diligence can pose a security risk when an organization migrates to the cloud quickly without properly anticipating that the services will not match customer’s expectation.

This is especially important to companies whose data falls under regulatory laws like PII, PCI, PHI, and FERPA or those that handle financial data for customers.

9. Shared Vulnerabilities

Cloud security is a shared responsibility between the provider and the client.

This partnership between client and provider requires the client to take preventative actions to protect their data. While major providers like Box, Dropbox, Microsoft, and Google do have standardized procedures to secure their side, fine grain control is up to you, the client.

As Skyfence points out in its article “[Office 365 Security & Share Responsibility](https://www.skyfence.com/blog-aws-security-shared-responsibility/),” this leaves key security protocols – such as the protection of user passwords, access restrictions to both files and devices, and multi-factor authentication – firmly in your hands.

The bottom line is that clients and providers have shared responsibilities, and omitting yours can result in your data being compromised.

10. Data Loss

Data on cloud services can be lost through a malicious attack, natural disaster, or a data wipe by the service provider. Losing vital information can be devastating to businesses that don’t have a recovery plan. Amazon is an example of an organization that suffered data loss by permanently destroying many of its own customers’ data in 2011.

Google was another organization that lost data when its power grid was struck by lightning four times.

Securing your data means carefully reviewing your provider’s back up procedures as they relate to physical storage locations, physical access, and physical disasters.