# Top 7 Risks of Cloud File Sync & Share

The proliferation of consumer mobility, media tablets, and bring your own device (BYOD) programs in the enterprise is increasing adoption of file synchronization and sharing (FSS) offerings.

However, employee-led adoption of cloud-based FSS services is a great thing until it runs into the security risks of cloud computing. According to a Cloud Security Alliance survey, 91% of industry experts rank data breach and data loss as critical threats to cloud security.

All too often, unauthorized Shadow IT projects move sensitive and proprietary data to the cloud without understanding all the security implications.

> **91% of industry experts rank data breach and data loss as critical threats to cloud security.**
>
> Cloud Security Alliance
> "The Notorious Nine"

## Bypassed data security

Like most IT professionals, you've put a lot of time and resources into planning and implementing your security strategy. Often, organizations have adopted a layered security approach that includes data leak prevention (DLP) solutions and other data security controls that protect the company's confidential information. But, when corporate data is pushed to cloud FSS solutions, this security protection is turned upside down with a complete bypass of your protection controls. Whether accidental or intentional, if your company data is stored in the cloud, there's an increased exposure to data loss.

## Data theft made easy

Cloud-based FSS applications make it easy for employees to readily flow data out of the organization. And it happens so fast, as an IT admin, you rarely have the knowledge it occurred or the time to react. The recent Lyft lawsuit is an example of this risk. Filed in November 2014 against former exec, Travis VanderZanden, Lyft claimed VanderZanden transferred the company's most sensitive documents to his personal Dropbox account in the weeks and months before his departure to join top competitor, Uber.

## Your data is no longer yours

When you put your company's data in the cloud, it can be accessed by the application-as-a-service vendor. The reality is, a third-party vendor now has your company's data, and often, there's no contract or agreement disclosing the policies on how and when your data can be accessed on their servers.

In fact, the US Patriot Act gives the government unfettered ability to access data stored by US cloud service providers. And, what about a lawsuit? If Dropbox or Google Drive, for example, receives a subpoena by law enforcement, they could decrypt your data and hand it over without you or your company knowing about it.

## Risks to compliance

When your employees move company data to the cloud, they expose the organization to significant risks to compliance. Any Patient Health Information (PHI) shared via a cloud-based FSS service could expose healthcare organizations to HIPAA violations. This risk holds true for finance companies and any other regulated industry; moving your data outside the firewall to third-party servers can expose your organization to HIPAA, FINRA, SOX, and other compliance violations.

## Mobile data security nightmare

When an employee loses a device that's being used for both work and personal purposes (or if someone steals it), the company faces a security risk. And, if the employee is accessing company confidential information from a cloud vendor's mobile app, the risks are compounded.

With the phone in the wrong hands, it takes less than five minutes to access the cloud FSS account and syphon off the company confidential information stored there. In addition, many company security breaches result from lost or stolen devices.

## Uncertain security posture

Of course, it's important to acknowledge that cloud-based file synchronization and sharing companies are aware of the security concerns. And, many have made efforts to incorporate security into their design, including such technologies as encryption and mobile device management (MDM).

While this might make them seem like a safe route to take, the biggest issue persists – there's no way to know if the vendor is comprehensive in their security approach or if they're protecting your data holistically. The best way to make sure your data is secure is to manage it yourself within your organization.

## Mixed personal and professional data

Shadow IT adoption of cloud FSS offerings has led to mixed use by the employee for both their personal and professional data. It's not uncommon, for example, that an employee account will have pictures from the last family holiday along with corporate files on a current project.

These fluid boundaries (or total lack of boundaries) can lead to inappropriate sharing and puts each data set at risk. For example, an employee engaged in a personal lawsuit might have to provide both sets of data to attorneys managing the discovery process. And, with the fast pace of life, it's far too easy to inadvertently share a corporate folder with a friend or a folder storing personal photos with an employer.

**ABOUT AEROFS**

AeroFS delivers highly secure, enterprise-class file sharing and synchronization solutions that enable enterprises to better control and secure their data and increase collaboration among users. Like Dropbox and other online file-sharing offerings, AeroFS allows users to simply drag and drop files into a folder to sync and share them with colleagues and external partners. Unlike those offerings, however, AeroFS is deployed on the enterprise's own infrastructure, and so enterprise data always stays under company and IT control. Files are shared directly between users' devices, and enterprise data never resides on AeroFS servers. The company is funded by blue-chip investors, including Avalon Ventures, Andreessen Horowitz, Y Combinator, NHN Investment, and others.

Learn more at aerofs.com.