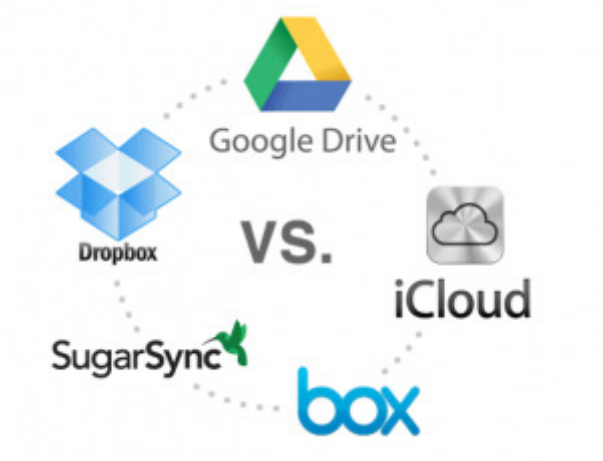
# Vulnerabilities and Security Risks of Cloud Storage Services


144 South Beach Street
Daytona Beach, FL 32114
386.248.0000
info@daytonanetworks.com

*Business News Daily* reports that by 2014, cloud computing is set to grow into a promising $150 billion industry. That's a lot of data and a whole lot of empowered users syncing, sharing, and collaborating on various web-based files. There's a price, however, that comes with the convenience of having real-time access to your files through a variety of internet-enabled mobile devices. The security of your data can be compromised by the inherent vulnerabilities of cloud storage services. The more you know about the security risks, the better you can protect your important data in the cloud.




**Two User Activities that Can Weaken the Security of Your Cloud Storage Account**

Three of the most popular cloud storage vendors–**Google Drive, Microsoft SkyDrive, and Dropbox**–were studied by a team of researchers from the A*STAR Institute for Infocomm Research based in Singapore. Their findings were detailed in a paper that appeared in a 2013 issue of the journal, *IEEE Pervasive Computing*. The researchers discovered that all three cloud storage services possess potential security loopholes that can be worsened by two specific user activities–*file-sharing through private URLs and using shortened URLs*.

There are many advantages to sharing files compared to working with email attachments. When you share files via your cloud storage account, you are not often bounded by file size restrictions. You can also set a file's access level to public, private, etc. The researchers from the A*STAR Institute for Infocomm Research, however, found out that sharing secret URLs can undermine the security of cloud storage accounts. This is because URLs end up being saved in browsing histories, bookmarks, and network-based servers, thereby giving numerous third parties access to what should have been private data.

In addition, the use of URL-shortening services poses a security risk. According to the researchers, when a URL is shortened–even if the URL leads to a file that is privately shared through a cloud storage account–the address is rendered into a plain text format that is stripped of encryption. URLs of this kind are then made vulnerable to brute-force attacks. Thus, it is best to retain the original URL each time you share files with your friends and colleagues.

**A  Cloud Environment Cannot Be Completely Guaranteed**

Business and individual users who upload and backup sensitive data to their cloud accounts are comforted by service provider claims declaring complete xonfidentiality–meaning, the cloud storage vendor's own employees have no ability to access or view client data. This confidentiality is typically asserted by providing encryption to users' files before they are uploaded to the cloud servers.

According to the findings of two researchers from the Johns Hopkins University's Information Security Institute, complete confidentiality cannot be guaranteed by cloud storage vendors. Computer scientists Duane Wilson and Giuseppe Ateniese uncovered that complete confidentiality is only possible for users who don't share data with other users through the cloud storage service. The moment a client shares data, the service provider is granted a loophole for which to access and view the said client's information. The complicated mechanism of how file-sharing creates a breach in what is supposed to be a zero-knowledge cloud environment is detailed in this archived 2014 paper arxiv.org/pdf/1404.2697v1.pdf.