

Army Vision: By 2028, a world-class Army that is a source of national pride.

HEADQUARTERS
PHILIPPINE ARMY
**OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR
COMMAND, CONTROL, COMMUNICATION, AND CYBER SYSTEMS, G6**
Fort Andres Bonifacio, Metro Manila

6/CMB

17 June 2016

CYBERSECURITY BULLETIN

Cybersecurity Bulletin: #60

5 Safety Concerns with Cloud Data Storage, Answered



Still a relatively new innovation, cloud storage has attracted a lot of scrutiny in recent months. Before entrusting sensitive data to third party storage facilities, consumers want to know that their information is going to be stored safely and reliably. And is it? The simple answer is *yes*. Despite scare tactics devised by hackers to undermine consumer perception of the cloud, cloud storage remains one of the safest ways to store your data today. Let's take a look at why.

1. If the Cloud is Secure, How was Apple's iCloud Hacked?

After the well-publicized attack on Apple's iCloud, polls showed an immediate drop in the popularity of cloud storage. Users reported feeling more vulnerable, and began questioning the security of their own personal data. But what really happened? The headlines said that the cloud had been hacked, that nude pictures had been stolen from the private accounts of 26 celebrities. While the photos were indeed stolen from the victims' personal accounts, the important distinction that the popular media never made was that the cloud *wasn't* hacked. The breach was a result of vulnerabilities in Apple's password security system, enabling persistent hackers to guess the passwords and security questions of select users. The cloud itself was never actually breached.

Cybersecurity Bulletin #60

Army Core Purpose: Serving the people. Securing the land.

2. How is the Cloud Protected?

To keep data secure, the front line of defense for any cloud system is **encryption**. **Encryption** methods utilize complex algorithms to conceal cloud-protected information. To decipher encrypted files, would-be hackers would need the encryption key. Although encrypted information is not 100% uncrackable, decryption requires a huge amount of computer processing power, forensic software, and a lot of time. Can it be done? Yes, the only way to keep your data safe for certain is to lock it up in a safe beneath the ground. That being said, your cloud-stored data is generally safer than your locally stored data. Cloud services utilize more complex security methods than the average computer owner is able to devise, giving your cloud-stored data an added level of protection.

3. What Can I Do to Help Keep My Cloud Data Safe?

Keeping your data secure is your responsibility as well as your cloud provider's responsibility. As hackers demonstrated through the celebrity iCloud breach, poor password security can give cybercriminals an all-access pass to your private data. To keep your password safe, avoid using the same password over multiple platforms; add letters, numbers and symbols to your password, and do not utilize a password that is in any way related to your personal life. Any hacker worth his salt will know your address, your husband's name, the type of car you drive and your favorite restaurant.

Data security is a major concern, and although options are currently limited, they exist. The most secure is likely a military grade encryption from providers like *Credeon* (<https://psg.hitachi-solutions.com/credeon/overview>) or *nCryptedCloud* (<https://www.encryptedcloud.com/>). This allows users to encrypt and store data with their own specifications, and securely share files with other parties that can view files with a key management system.

However, the biggest cause of concern for Cloud storage isn't hacked data, it's lost data.

4. Is Cloud Storage Really Reliable?

Your data might be safe if the system that it is stored on has failed, but that won't do much to mollify you in the event of a system outage. While cloud storage keeps your data secure from fires, floods, hurricanes and computer meltdowns, it is still vulnerable in the sense that it is in the hands of a third-party system. Fortunately, since there are no geographical limits to cloud storage, you don't have to use your local cloud services. Before selecting a cloud storage provider, do your research. Top cloud providers can keep your data safe and consistently accessible. If the company you are working with has a history of data loss and security breaches, then it's time to move on to a new provider.

Cloud storage is much more reliable when used in tandem with another storage system, such as Google Drive. As stated earlier, the biggest concern with cloud storage is lost data, not hacked data. But that issue is eliminated if the cloud is used more as a "sharing" platform instead of a "storage" platform. By taking shared

Army Vision: By 2028, a world-class Army that is a source of national pride.

files and storing them into something like Google Drive, you can ensure that if your data is lost, you can easily locate it through the other platform.

5. Who is Currently Using Cloud Storage?

A recent poll stated that 86% of companies not only use extensive cloud storage systems, but multiple cloud storage systems. The survey consisted of companies from 80 different countries and collected data from as far back as 2005, before cloud storage became a hot button issue. 30% of business of 1 storage account, 16% have 2, 12% have 3, 8% have four, and 19% have 5 or more (with 13% having 0 accounts).

So what does this mean? It means that most companies either trust cloud storage enough to incorporate it significantly in their data storage efforts, or that the benefits of cloud storage are so great that it's worth the risk. Nevertheless, the trend is not stopping. Cloud usage has seen an exponential rise every year since 2009.

So although safety seems to remain a concern, despite the guidelines and practices put forth by experts in the field, big companies are still investing resources in acquiring and developing the storage platform. Which means that cloud optimization and security will mimic the rise in its popularity.

Reference:

This was cross posted from:

<http://systemsandsoftware.com/5-safety-concerns-with-cloud-data-storage-answered/>

DO YOU WANT TO KNOW MORE? TALK TO US.

POCs:

a. LTC JOEY T FONTIVEROS (INF) PA – Chief, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0917-6281057. Email: fontiverosjt@army.mil.ph.

b. Sgt Mark Dave M Tacadena (SC) PA – Branch NCO, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0998-5342877.