Cyber

# Sensitive Data in the Cloud

New technologies experience growing pains. Capabilities may be initially misunderstood and unanticipated risks emerge. This includes entrusting sensitive data to the cloud environment.

Due to the potential for access to low cost, highly available and flexible computing resources, migration of data into the cloud environment is inevitable. Both providers of and subscribers to these services need to maintain awareness of emerging risks. Subscribers have a responsibility to choose providers who maintain levels of security appropriate to the types of data they entrust to them. Subscribers also need to evaluate the degree of control over authorization of user accounts and definition of roles that will be available as well has how data is protected at rest and in transit. Providers have the responsibility to be as specific and clear as possible about how customer data is handled and protected.[1]

To mitigate the risk associated with entrusting sensitive data to the cloud, the first step is to make sure subscribers and providers are in mutual agreement to the protection provided.

For cloud computing to reach its full potential, flexible provisioning of services must be balanced with the need for isolation of subscriber resources to ensure proper data security. The database environment and data isolation techniques utilized are critical when sensitive data is being handled in a cloud environment.

As detailed by the National Institute of Standards and Technology, examples of cloud database environments include multi-instance and multi-tenant models. Multi-instance models provide a "unique database management system running on a virtual machine instance for each cloud consumer."[1] This model gives the subscriber control over key security features such as user role definition and authorization.

The multi-tenant model is a "predefined environment for the cloud consumer that is shared with other tenants, typically through tagging data with a consumer identifier."[1] This model depends on the cloud provider to provide a secure database environment. Secure encryption of stored data is not typically an option in these shared databases.

There are two ways in which a subscriber could potentially face a data breach through the usage of cloud storage provider; either through a security incident of the subscriber or through a security incident of the provider.

A recent Capital One cyber breach in 2019 highlights how information on the cloud can be accessed through vulnerability on the subscriber's system. Storing personal user information and bank details in the Amazon Web Services cloud system, Capital One's infrastructure was compromised, leading to unauthorized access of this information.[2] AWS was not the system that was attacked. This event affected approximately 100 million individuals in the US and approximately 6 million in Canada.[3]

Apple's iCloud system, which allows Apple users to backup data in their account such as photos, email, contacts, calendars and more, was breached in 2014. As a result of this cyberattack, many users' personal photos, including Hollywood actors, were released publicly. Because of the public status of those who were attacked, it gathered large press coverage, bringing the issue of cloud security to the forefront of the general public eye, and the importance of reinforcing cloud accounts with additional security measures.[4]

The following questions are provided as a means of investigating the exposures and controls related to the handling of sensitive data in cloud environments:

- How is sensitive data protected in transit and at rest?
- If encryption is utilized, are encryption keys managed by the provider or the subscriber?
- Do the provider's employees have access to unencrypted customer data?
- How is provider employee access to subscriber data controlled and monitored?
- What user authentication, authorization and access management capabilities are available? Are these features under the control of the provider or subscriber?
- What specific security controls does the provider agree to in contracts with subscribers? On their website? In their advertising?

These questions are by no means comprehensive but will provide a starting point for an informative dialogue with your clients related to this emerging area of exposure.

For more information, visit cnacanada.ca.

[1] Guidelines on Security and Privacy in Public Cloud Computing (2011) Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

[2] Guest Post: What the Capital One Hack Means for Board of Directors (2019) Retrieved from https://www.dandodiary.com/2019/08/articles/cyber-liability/guest-post-what-the-capital-one-hack-means-for-board-of-directors/

[3] Capital One (2019) Retrieved from https://www.capitalone.com/facts2019/

[4] Forbes (2014) Retrieved from https://www.forbes.com/sites/davelewis/2014/09/02/icloud-data-breach-hacking-and-nude-celebrity-photos/#d1ca2192de72

One or more of the CNA companies provide the products and/or services described. The information is intended to present a general overview for illustrative purposes only. It is not intended to constitute a binding contract. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all provinces and may be subject to change without notice. "CNA" is a registered trademark of CNA Financial Corporation. Certain CNA Financial Corporation subsidiaries use the "CNA" trademark in connection with insurance underwriting and claims activities.