NASCIO Representing Chief Information Officers of the States

NASCIO Cloud Computing Series

Capitals in the Clouds

Part V – Cloud Security: Advice from the Trenches on Managing the Risk of Free File Sharing Cloud Services

NASCIO Contacts:
Erik Avakian
Chief Information Security Officer
Commonwealth of Pennsylvania

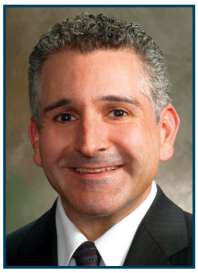
Chad Grant
Senior Policy Analyst
NASCIO

NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States. For more information visit www.nascio.org.

201 East Main Street, Suite 1405
Lexington, KY 40507
Phone: (859) 514-9153
Fax: (859) 514-9166
NASCIO@AMRms.com
www.NASCIO.org

The growth of consumer-grade information technology solutions invading state government has been widely reported. Cloud-based file sharing solutions are very popular and certainly a growing and significant part of this mix. It is easy to see why these services are attractive to state government users. With a wide variety of choices in the market, these solutions are easy to access, configure and use. They support multiple devices (especially mobile), and data in multiple formats. The most important consideration for state employee users – these file sharing services are free! Despite security guidance, policies or directives describing the risks and prohibiting the use of file sharing cloud services, state employees will opt for convenience of free and ready.

Since the release of the 2012 NASCIO and Deloitte Cybersecurity Study, more security and policy questions have been raised on the use of free cloud services by states. In addition to the May 2012 Capitals in the Clouds IV guidance on rogue cloud users, states have continued to seek out leading practices on how to put the proper controls in place, meet security standards, craft acceptable use policies, and identify the open records and legal concerns regarding terms of service. In addition, State CIOs understand they must support the business objectives of their agency customers and offer enterprise alternatives to free cloud services. To address these concerns and take a deeper dive into the topic, NASCIO interviewed IT security expert and the Commonwealth of Pennsylvania Chief Information Security Officer (CISO), Erik Avakian.



NASCIO - Do you prohibit the use of free cloud services in Pennsylvania?

Avakian - Yes. In general, free cloud storage services are risky from a data security standpoint and we try to steer agencies away from using them and suggest several "enterprise" service offerings first.

NASCIO – What are the some of the reasons the Commonwealth of Pennsylvania prevents agencies away from using free cloud services?

Avakian - There are many reasons why we prohibit the use. Despite definite strides in improving the security of these types of solutions, providers still face security shortcoming and have historically experienced major breaches. Some have suffered significant breaches over the past several years and some have experienced some form of downtime and security problem and/or breaches. Because of tight margins on price, users of these services can never really be sure of what level of security a certain providers is implementing to secure user data on their solutions.

Additionally, some providers do not guarantee user ownership or return of data once service is terminated, or where that data will reside (and it may be in servers outside of the United States). A user's data sits on servers that are shared by many different customers and this increases the risk of mismanagement, theft, or loss of data over in-house managed storage. There is significant risk of sensitive data being placed in these services and subject to potential breach and monitoring and preventing such instances is very difficult since these services are managed solely by the providers. Most providers completely disclaim responsibility for what happens to data, and none guarantee its integrity, even when the services operate without apparent problems.

NASCIO – In addition to security risks, are there legal issues with the use of free cloud services?

Avakian - Absolutely. Acquisitions of this kind (i.e.; of software, or software-as-a-service, and even for open-source software) generally require agreement to some terms, either via a shrink-wrap agreement, an agreement based upon "first use," or via a click-through agreement. These kinds of "agreements" present problems both relative to form (they are not agreements executed consistent with the Commonwealth Attorneys Act) and substance (they often contain unacceptable terms and/or terms that are not authorized by law). These terms can also present significant risks. The decision to do business through this type of agreement is ultimately a business decision. The agency should, however, consult with its Office of Chief Counsel to ensure that it is aware of the risks related to not having an actual agreement in place, or in accepting the terms of an agreement which has terms that are not otherwise acceptable.

NASCIO - Should states consider a blanket policy in place or are there factors that should we consider for certain providers?

Avakian - The risk and legal ramifications of using such services needs to be evaluated on a provider by provider basis. Service providers that allow dual factor authentication and user provided encryption keys should be favored. All use cases and data types that would be placed in these environments needs to be classified as sensitive or public/non-sensitive especially with respect to Personally Identifiable Information (PII). The aggregate risk and total cost (hard and soft) of a potential breach of this data needs to be understood and accepted by the Secretaries and CIOs of the agencies that permit such use. Furthermore the potential name-brand damage to the Commonwealth must also be considered with the increased breach risk.

NASCIO - Do you actively block access to free cloud services?

Avakian - Yes. We currently use our enterprise web filtering solution that explicitly blocks the "Cloud Storage" category at the Enterprise level. However, since there are always potential business needs for use, if an agency requires access, they can enter a waiver request as to who needs it and why, and the waiver process enables the agency "head" to sign a document accepting the risks for use and if the waiver may be granted, they can have access to the sites. Going forward, we will be implementing an Enterprise Data Loss Prevention (DLP) solution at the network perimeter to not only help prevent against data breaches or the inadvertent or intentional loss of sensitive data, but to "Enable the business" by enabling the use of these cloud storage technologies without having to block these types of solutions. The network DLP implementation will be able to inspect inside "encrypted" files and web content, analyze the content for sensitive data, report and alert on infractions. So if anyone is publishing sensitive data to a free cloud data storage service provider account we will know.

NASCIO - Are you providing a state government alternative for employees such as limited free cloud storage from IT services?

Avakian - Yes, we have internal solutions that we try to steer the agencies towards using. We have internal solutions we are implementing and also have enterprise secure file storage for agencies to leverage. Agencies must explore these options first. In not all cases however, do the enterprise solutions meet the business needs of the agencies. In such cases, the waiver process is used.

NASCIO - Have you negotiated with the cloud service provider for an enterprise solution with favorable government terms of service?

Avakian - No. However, recommendations are for the commonwealth to pick one or two of the top providers and enter into favorable contracts to enable the business and let the agencies leverage the contracts. This could only be acceptable if the proper Terms and Conditions (T's and C's) are in place. Without a contract in place with proper T's and C's, the use of free cloud storage is not a recommended option. Here is the current guidance we are providing to agencies these days inquiring about these services:

Regarding free cloud storage, there are several options which should be explored in the following order to determine which would best meet the agency business needs.

Option 1) The Enterprise Data Center offers "Enterprise" file hosting services which can be utilized to host or share data with external entities. This option should be explored first and is recommended.

If there is a business requirement to utilize "external" on-line or cloud storage sites then Option 2 and option 3 apply:

Option 2) The agency "contracts" with a vendor who provides these types of on-line storage services in this space. The contract will ensure valid Terms and Conditions (T's and C's) and confidentiality, integrity and availability (CIA) of the data and services. This option is recommended. A waiver request would be required listing the users and sites which would be needed for access. The contract would accompany the request. Our web filtering provider would then receive the completed approved request, and ensure the appropriate users have access to the sites.

Option 3) If the agency does not wish to contract with a vendor and instead wishes to utilize "free" on-line or cloud storage services.

a. A waiver would be required listing the users and sites which would be needed for access.

b. The agency would be required to take certain action to acknowledge and accept the risk allowing for the use of and allowing user access to free on-line cloud storage sites. OA/OIT would need to receive a signed "letter of acknowledgement and acceptance of risk" document of the use of free non commonwealth storage containers. It is a legal binding document - required and approved for use by the CIO and OA Chief Counsel - that would need to be signed by the requesting Agency Head, Agency CIO, and Agency Chief Counsel. The signed document would accompany the waiver request.

c. Our web filtering provider would then receive the completed approved waiver request, and then ensure the appropriate users have access to the sites.

   The legally binding letter which the agency head signs are then kept on file.

A generic example of this letter is as follows:

ACCEPTANCE OF RISK

OA/OIT has been made aware that the Department of X has a business requirement in allowing for the use of and access to "free" cloud storage sites for a number of agency end-users. The use of "free" cloud storage sites is generally not permitted for use unless a current contract is in place with the issuing agency and the cloud storage provider.

Department of X is requesting the use of such free cloud storage sites and is seeking a waiver to the restriction. A waiver is offered under the following conditions:

Department of X must take certain action, and must acknowledge and accept the risk allowing for the use of and access to "free" cloud storage sites in the manner indicated below.

1. Department of X acknowledges that the use of such free cloud storage sites potentially places commonwealth data at risk of data breach because there may be no enterprise technical controls currently available to limit or prevent users from uploading of commonwealth data to such sites.

2. Department of X and/or its contractors, not OA, will be solely responsible for any costs related to any data breach as a result of the use of such sites.

3. Department of X, in order to exercise this waiver, must notify its Executive Staff (including its CIO, Agency Head, and Office of Chief Counsel) of the content of this waiver, and must provide OA/OIT with a signed acknowledgement that the Executive Staff understands and accepts the risks (both legal and technical) as outlined above.

I have read the information above:

_____

Agency Head, Department of X

_____

Department of X Office of Chief Counsel

_____

Department of X CIO