Increasing Awareness of the Multijurisdictional Nature of Cloud Computing

Kara Nance, University of Alaska, Fairbanks and *Amelia Phillips,* Highline Community College, Seattle WA

Abstract – Tasked with a goal of increasing profits for their shareholders, corporations are fleeing to the cloud to help defray some of the costs of doing business. Unfortunately, much of this mass migration is being done without adequate consideration for the security implications of moving to a potentially multijurisdictional environment. In this paper, we explore cloud service consumers from an educational perspective and provide discussion of some scenarios that can be used in an academic setting to increase awareness of some of the important security considerations that should be investigated prior to making a move to a cloud platform. While scenarios in this realm can take many forms, including cloud simulations with load balancing in virtualized environments, this scenario is presented in a discussion format in order to minimize the associated technical support required, while maximizing the range of courses into which the exercise can be incorporated.

Index terms – Information assurance curriculum, cloud computing, security education

I. Introduction

As usage of the cloud has become increasingly commonplace, it is our responsibility as educators to increase awareness in our students about the inherent security issues associate with cloud usage. It is a challenging concept to teach, especial to students who have a US-Centric worldview that doesn't include or appreciate the truly global nature of the cloud environment. The following exercise was developed to help student realize, in a protected environment, some of the complex multicultural and multijurisdictional issues associated with the cloud that can come into play when an individual or organization chooses to use cloud resources.

II. Background

As instructors, we have asked a simple question in a large class of students: "How many of you keep important data in the cloud?" Sometimes a few hands are raised, but for the most part, students do not view the cloud as something that they use. A second question generally gets more results: "How many of you use Gmail?" A follow-on question of "Where exactly does your Gmail inbox reside and who can read your mail" starts them thinking, and the discussions as they realize they are active cloud consumers can be quite interesting. After running this exercise at numerous talks and in courses, we developed a more in-depth discussion-based exercise to guide students towards increased awareness of issues associated with being a security-conscious cloud consumer. The scenario can be taught in 200 level classes or higher that are focusing on business processes, risk assessment, network administration and network security. It can also be used in computer or digital forensics classes. The scenario has been used in a 200 level UNIX/Linux systems administration class. It is being incorporated into a 200 level Network Scripting class that actually uses cloud load balancing.

III. Scenario

This exercise was developed around a hypothetical, yet realistic, cloud environment in which a cloud service provider offers services. Students were charged with making a series of choices and then evaluating the outcome when they were provided with additional information or results stemming from their previous actions. It is important to note that students are not given any advance information about the cloud service provider in the scenario nor about the physical layout of the cloud. Further they are not even told that cloud services are being evaluated. From their perspective, they are merely making decisions in response to a risk analysis audit for an organization. One issue sited in the audit report is a warning about the lack of an enforced, corporate backup plan. Since the loss of data without backup is given a very high risk impact score, this is the first part of the audit that will be addressed. The apparent objective of this part of the scenario is to develop a backup strategy to mitigate this risk in an organization. This paper discusses four discussion points that were addressed during the scenario: initial placement, load balancing, insider threat, and cloud service provide selection.

A. Cloud Service Provider Selection

To set the scene, the organization is a mid-size business with approximately 120 employees and 250 clients. Students are provided with some data regarding three backup plans that the organization is considering including the following:

- Local System Backups with Offsite Storage (Highest Cost)
- Local System Backups with Onsite Store (Medium Cost)

ISBN 1-933510-96-X/$15.00

- Cloud Backup and Storage (Lowest Cost)

The amount of information presented regarding the options above can be minimal or significant. Regardless of the amount of ancillary data provided, invariably, the cloud backup and storage option is selected. From a purely financial standpoint, this solution makes sense.

Once the decision is made to choose the cloud service provider as the backup option, discussion can begin about the impacts of the decisions. The objectives at this point are to demonstrate three specific issues that demonstrate multijurisdictional nature of the cloud and the impact that choosing this option to reduce organizational risk, may have opened the floodgates to a plethora of new risks.

Further, this is the solution being made by many businesses around the world. The US government released a policy to move several agencies to the web in an effort to better serve the American public and make the same services available nationwide. In February of this year, they released the Federal Cloud Computing Strategy [1]. The savings are in the billions of dollars. The policy states *"The three-part strategy on cloud technology will revolve around using commercial cloud technologies where feasible, launching private government clouds, and utilizing regional clouds with state and local governments where appropriate."* [2]. each government agency has 18 months to move 3 services to the cloud. Google has already begun negotiations. One of the biggest issues is keeping any data from a government cloud client located on a server physically in the US. What would be the ramifications if government documents backups were in another country?

The second step is to choose a cloud service provider. The students are provided with a list of four hypothetical potential service providers, their associated costs, the level of control and access they will have for their data, and copies of the cloud service provider policy statements. These are actual cloud service provider policy statements, but have been modified slightly for demonstration purposes. (An ancillary lesson here is that most people do not read through policy statements thoroughly although it can greatly affect your rights as shown in section II.E.)

B. Scenario Evolution 1 – Initial Configuration

After the cloud service provider has been selected, students are provided with a description of some of the data items that are being backed up including the following:

- John Smith's Child Porn collection
- Jim Donovan's Family Photo Collection
- ABC Bank's Financial Records
- Archives of Cosmopolitan Magazine
- Professor Newman's Hard Drive Backup
- Your corporation's marketing plan
- Dental Office Patient Archives

An important note here is that many organizations are blissfully unaware of the data that resides on their computers. Whether part of their organizational mission or not, there is generally a great deal of data that can cause issues when moved outside of the organization's perimeter.

For the scenario, it is assumed that the initial configuration has the cloud data being backed up from the organization to a server farm in a nearby state. One of the biggest fears in the cloud is that your company does not know the identity or trustworthiness of the other companies, persons, or entities on the physical server. In the first scenario, John Smith has child porn stored in his file account. This is already a federal offense which has just been compounded by crossing state lines. Because your account just happens to be stored on the same physical server with his, your data may have to be examined as they build a case against him. Imagine that you are about to launch the next phase of marketing for your new product. The person doing the backups for the investigator just happens to have a cousin in the same line of business and they mention your ideas to them. Your company trade secrets were just leaked because you have no control over who sees your data.

HIPAA compliance and the cloud present another host of issues. The students are given the hypothetical question "If you were to ask your dentist if your records were encrypted, what answer would they give?" Most would not expect their dentist to know what encryption is much less the cloud. Now give them the situation that their dentist has decided to use a cloud provider. A patient has rights under HIPAA and even with *compliance in the cloud*, but what guarantees does the patient have? As a patient, you have the right to your records on demand. In a recent article in the HIPAA compliance journal, the question was raised as to the responsibility to keep backups for an extended period of time and have the backups available. The article states:

> *However, online backup services have often failed to meet long-term commitments. There have been several online backup services, including those run by very large companies such as Hewlett-Packard which have been unable to meet long-term storage strategies.* [3]

There have been numerous lawsuits in which patients have sued because insurance companies and clinics did

not provide them with their histories in a timely manner. And the patients won. So what happens when the local dentist stores his data on the cloud and it is then moved to another state? The issue becomes that the dentist is subject to the rules and regulations and codes etc. of HIPAA, but the cloud provide is NOT. What will the dentist have to do to protect him or herself? In a risk analysis, that will be one of the primary issues when someone in the medical profession chooses to use the cloud.

The next scenario will hit the students where they may be quite sensitive – their wallet. ABC Bank is storing their backups on the cloud. Sarbanes Oxley and the Gramm-Leach-Bliley Act come into play here. What does the bank do when the auditors show up and they can't produce seven or even three years of data because the server farm in the next state over has had a power outage and never really tested their backup procedures. What happens to the audit trail? What rights do the clients of the bank have? Now the bank is forced to close its doors because it is out of compliance. The domino effect can cause one to reel.

C. Scenario Evolution 2 – Load Balancing

Corporations exist to make money for their shareholders. The cloud service provider in this scenario is no different. In order to reduce costs, load balancing algorithms are applied which result in data being stored in many jurisdictions. The students will need to look at where some of the more popular cloud service providers such as Google and Amazon house their servers. The first thing that should jump out at them is that while they may be able to find out the countries and possibly even the cities the servers are located in, the actual location is classified. The locations are closely guarded secrets to the point that even large corporations such as the Fortune 50 who house data with them are not granted access.

So the more general task will be simply to let the students go onto the Amazon or Google cloud websites and determine where the facilities might be located. They can look at user blogs and other resources to get an idea. Load balancing shifts the data indiscriminately from a busy node to a less busy or faster accessing node. On one popular cloud, the company or entity data could be in Los Angeles, London, New York, Singapore, Siberia or other location. Let's look at a few scenarios that can be built from those listed in Section II B.

The definition of child pornography is standard throughout the US, true or not? Have the students examine the various state laws and find what the age cut off is. In some states the age is 14; in some it may be older or younger. What happens if a person is accused of having child pornography in the state of New York where the age is 16 and the data is stored in a state where the cut off for child porn is 12? Ask the students what the legal age for marriage is in the US. How many are aware of the fact that in some states with parental consent, a child can be married at the age of 12? Does it become a federal case because it crossed state lines or does it remain in the original state? Let's reverse the situation. Smith's pictures are of children ages 14 to 16 which is legal in his state. The data – namely his pictures – are moved due to load balancing to a state like New York where anyone under the age of 16 performing sexual acts is considered child pornography. Should he now be arrested? Regardless of how the students may feel on the matter, what is the law? Whose jurisdiction prevails?

The archives of Cosmopolitan Magazine may be considered rather benign to American or western Europeans. However, what happens if the archives are rotated to a conservative country where women are to remain covered? Has the cloud provider violated the law or has the owner of the data violated the law of the country the data is residing in? The students can also be made to look at data in transmission. If the physical wires are located in a country and the data is transmitted using that medium, does that country reserve the right to examine said data if they suspect it violates their laws?

In another scenario, Professor Newman is a research scientist who is mild mannered but brilliant and very loyal to his country. However, he likes to travel a lot and is rather absent minded. He stores much of what he works on in the cloud. Many of his projects have export restrictions. What is the probability as an ordinary citizen using services like Google Docs or DropBox that his data may be shifted offshore? What are the consequences for him and for his employers? Who is ultimately at fault? Does he have any recourse? These are all questions that need to be addressed. Take the situation a bit further, Professor Newman is a government employee and he works on items of national security. Now what conclusions can be drawn if he did this of his own accord? In Section II A, it was mentioned that the US government has mandated that government agencies begin using the cloud. Professor Newman used the cloud provider as instructed, but the data was moved offshore anyway. Who is at fault? What are the implications?

Reconsider the Smith scenario where the pictures are of children 6 years of age or younger. The FBI is closing in on him. He decided to get everything off his physical hard drive and store them with a cloud provider that he knows almost exclusively uses servers in countries where this is not a crime. He shoots and burns the hard drive of his laptop beyond recovery. What laws would have to be in place or what would have to happen for the FBI to be able

to convict? The cloud introduces convenience that goes both ways.

Jim Donovan regularly takes pictures of his family. He and his wife take the usual pictures of their kids in the pool, at the beach, in the tub and just enjoying family life. One of the cloud providers' internal auditors, in an attempt to prevent the use of their services for mal intent, uses a forensics program that searches for skin tones. They run across several pictures of Jim's kids in the tub naked smiling up at the camera. He gets reported to the FBI. Meanwhile, as the FBI gets the subpoena, the data is transferred to a country that does not even remotely consider such pictures pornography.

Load balancing can create many challenges. Have the students look at the EU privacy laws. It is a hefty fine per person for transmitting their data across borders without their permission. Multinational corporations have grappled with this law when their backups within their own physical network were located in another country. Now compound that when backups are crossing borders multiple times every day or week.

D. Scenario Evolution 3 – Insider Threat

For this portion of the discussion, the tables are turned. The cloud service provider is an enemy agent who has invested millions of dollars and much time over the past 10 years in trying to gain access your digital assets. They have sent agents to talk to your employees, they have attempted to hack your system, and they have tried to get you to hire their agents to work in your organization. All of these attempts have been unsuccessful – until now. You have provided your enemy with ALL of your organization data. Everything you upload to the cloud is mirrored at their site for their agents to analyze. They can do anything they want with the data including the following:

- ABC Bank's Financial Records - Sell the bank information to the highest bidder, ruin credit rating of individuals, sell identity attributes to identity theft, generate fake bank credit and debit cards.
- John Smith's Photo Collection – Blackmail Jim Smith into providing them with cash, or access to organization, or his contacts that he sells the pictures to so they can blackmail or extort them as well.
- Professor Newman's Hard Drive Backup – Sell the secret formula from Newman's hard drive to your enemies who use it to create a weapon that will be used against you.
- Dental Office Patient Archives – Use dental records to fake someone's identity, or death, or use data for insurance fraud.
- Personal data files – Because the user linked their user id to their cell phone number, they can use GPS data to track the person, stalk them, harass them and cause other problems.

The possibilities here are endless and when students are set loose to discuss malicious activities that can result from an enemy obtaining an organization's digital assets, the resulting discussion is eye-opening.

E. Revisiting the Cloud Service Provider Policy

At this point in the exercise, students are generally quite frustrated. Their frustration magnifies when you revisit the cloud service provider policy statement, which specifically includes language that makes all of the above, including the Advanced Persistent Threat issues completely legal.

Students should be encouraged to examine what the legal profession is saying about cloud contracts. The most consistent words of advice were summarized here [4]

- *Identify protected customer information that the service provider processes and stores.*
- *Identify specific security procedures to which the provider must adhere.*
- *Make clear that the customer is owner of the data.*
- *Require transparency with regard to data location.*
- *Provide means of verifying and monitoring data integrity.*
- *Provider must be required to undergo independent security audits.*
- *Include a process for timely breach notification.*
- *Include a means for contract termination and secure disposition of data.*
- *Restrict limited liability on part of service provider; Nizer said providers should be responsible to make the customer "whole" if it's responsible for a breach or loss of availability.*

The list should make the students cringe. The idea that you may not be the owner of the data that you store there will affect many. As shown throughout the paper, knowing where your data is physically located can be paramount to success or failure. The paper began looking at backups. A critical item of backups is to be able to restore your system whether it be corporate, government or personal. If the cloud provider does not guarantee data integrity, what is their purpose? The last bullet goes to

ISBN 1-933510-96-X/$15.00

tort law. The companies are limiting their liability in the event of the failure of their system. This action borders on the insurance companies wanting to deny claims that were due to a terrorist act [5]. It may also be their own negligence for never testing or verifying the backup integrity.

Students will be quick to admit they click through End User License Agreements (EULAs) like the rest of humanity. When it comes to cloud providers, people may be giving up more than they planned or even realized. The question becomes – do you really want to trust them with all your data? Risk management should dictate other alternatives or backup plans to the cloud. As the cloud industry grows and matures, the questions and concerns will also.

IV. Assessments

In the initial portion of the scenario, presented in section III.A, the students have to compare four fictitious cloud service providers. The assessment would be an evaluation in which the students have to compare the cost, level of control and carefully examine the policy statements of each provider.

The next section allows the students to select the topic that most interests them. Some may focus on HIPAA; others may want to explore the implications of the Gramm-Leach-Bliley Act in the cloud or the EU privacy laws. Once the students have picked which policy they want to focus on, they have to prepare a report based on accounts similar to the ones listed in section III.B. They must address at least three of the ones listed and the impact the law would have on such an investigation.

The acquisition of one's digital assets can be devastating. Section III.C has the students explore how easily things can go wrong if an entity such as a cloud service provider has in their policy that they can view your data at will; the vulnerability of corporations and customers is exponential.

The final assessment has them look at the legal profession's view of the cloud. In this they can reexamine the cloud service provider's policies that were obtained in section III.A to the legal advice given. The students can determine how many clouds actually protect the customer or provide no protection at all.

For the type of class introduced in section III, most of the assessments are papers and research. However, that need not always be the case.

V. Impact and Future Uses

This type of exercise lends itself to being easily blended as a module in a variety of classes. Because it forces students "out of the box" and does not have a preset answer, it requires critical thinking.

While instructors attempt to teach students to work on their own and deal with problems as they come up, much of what is taught is step by step. Even with operating system installations, unless something goes very wrong, students may or may not learn anything other than point and click.

Scenario building requires that the students deal with things that are not cook book and that they may encounter in everyday life while on the job. As the ubiquitous cloud grows and new technology emerges on the scene, the students need tools and approaches that may help them deal with the unknown.

As mentioned in section II, the scenario is being tested in a network scripting class that includes load balancing in the cloud. In this type of class, the students have to become aware of the type of data that is being transferred. For example, if the arrangement by the US Government offices is that their data must remain in the lower 48, how does that affect the load balance equations? Does it affect what servers are used? How does it affect the business model of the cloud?

Again, the classes that can use such a module comprise a large percentage of information assurance classes and network administration.

VI. Summary

This exercise has been interesting to evolve as has the evolution of the students who have participated. Following the exercise, some students have been asked what they would do differently if they were again tasked with developing a risk mitigation strategy for backups. Subsequent discussions have quickly helped students realize the complexity of this globally connected virtual world that we are a part of and how there are no easy answers in this realm.

The students who would benefit the most from this type of exercise are in the 200, 300 and 400 level classes. However, graduate students new to the field, would also benefit from it. Whether the class is theory or hands on, the applicability of these exercises is broad.

VII. References

[1] Washington Policy Brief, *US Government Releases Cloud Computing Strategy*, 01 March 2011, retrieved on 14 March 2011 from http://www.arma.org/policy/policy/washingtonpolicybrief/11-03-01/U_S_Government_Releases_Cloud_Computing_Strategy.aspx

[2] CIO.gov, *IT Reform Series:"Federal Cloud Computing Strategy" Published, 2011,* retrieved on 14 March 2011 from http://www.cio.gov/pages.cfm/page/IT-Reform-Series-Federal-Cloud-Computing-Strategy-Published

[3] Blog, *Cloud Storage and HIPAA Compliance*, HIPAA Compliance Journal, 27 May 2009, retrieved on 14 March 2011 from http://www.hipaacompliancejournal.com/2009/05/cloud-storage-and-hipaa-compliance/

[4] Savage, Marcia, *Cloud Computing Contracts: Tread Carefully*, SearchCloudSecurity, 16 February 2011, retrieved on 14 March 2011 from http://searchcloudsecurity.techtarget.com/news/2240032214/Cloud-computing-contracts-tread-carefully

[5] Ryan, Dan, *SCADA Systems*, podcast lecture retrieved 11 March 2011 from www.uaf.edu Blackboard.

ISBN 1-933510-96-X/$15.00