Designing a Risk Management Field Guide for Cloud Services

Robert J. McShane

Robert.McShane@tufts.edu

Mentor: Ming Chow

ABSTRACT

I am writing this term paper for Computer Science 116 — Introduction to Computer Security. The purpose of this paper is to uncover and present the security risks and potential vulnerabilities that may arise as more companies move to cloud-driven service models. As a secondary focus, I would like to convince the reader that although cloud processing and storage can offer many benefits, companies should approach their transition to the cloud with caution and examine it thoroughly from a security standpoint using a well-thought-out risk management field guide.

TO THE COMMUNITY

Although more and more companies are starting to adopt cloud-service models, the cloud is a new frontier for technology and information management that presents new challenges in terms of security and government compliance. When dealing with this emerging field, IT administrators are often finding themselves to be uninformed about the appropriate security concerns that they should have when transitioning their applications to cloud-service models (Popovic & Hocenski, 2010). For those IT administrators who are informed about the risks involved in transitioning their applications to the cloud, they may have trouble placing values on these risks to determine how likely it is that a certain risk will affect them. Additionaly, security conscious IT administrators often struggle to choose between a number of similar cloud-service providers by looking at their security offerings because they don't have a strong enough background in terms of mitigating risk in cloud environments to figure out exactly what they need to do in order to keep their applications secure and to protect their company from litigation in the case that the security of their cloud applications is compromised (Takabi & Joshi, 2010).

In my research, I have looked at a variety of risk management strategies that may be used to mitigate risk in cloud environments. Using my findings, I have constructed a field guide that helps to assign risk values to common risks that accompany transitioning an application to the cloud and suggests ways in which IT administrators can limit these risks. This field guide will help IT administrators address the relevant concerns that go along with transitioning an application to the cloud, and determine the key security policies that they should look for (or negotiate using a Service Level Agreement) when choosing a cloud-service provider.

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Purpose

The purpose of this paper is to uncover and present the security risks and potential vulnerabilities that may arise as more companies move to cloud-driven service models. As a secondary focus, I would like to convince the reader that although cloud processing and storage can offer many benefits, companies should approach their transition to the cloud with caution and examine it thoroughly from a security standpoint using a well-thought-out risk management field guide.

1.2 Scope

The scope of my research includes: 1) briefly describe the challenges that IT administrators face when they adopt cloud-service models, 2) detail the security concerns that a company should consider when adopting cloud-services models, 3) conceptualize a risk management field guide that IT administrators may consult when deciding to move their applications to the cloud.

Although I will introduce the reader to the basics of cloud-service models, I will not delve into the specific details of how cloud-services function as this information lies beyond the initial scope of my research.

Additionally, in this paper I will introduce the subject of risk transference and relate it to the cloud by alluding to the topic of Service Level Agreements (SLAs). Although I will mention the notion of a SLA, the technicalities that are involved in drafting a SLA with a cloud-service provider lie beyond the initial scope of my research and will not be discussed in this paper.

2.0 CLOUD SECURITY

2.1 Introduction

Although more and more companies are starting to adopt cloud-service models, the cloud is a new frontier for technology and information management that presents new challenges in terms of security and government compliance. When dealing with this emerging field, IT administrators are often finding themselves to be uninformed about the appropriate security concerns that they should have when transitioning their applications to cloud-service models (Popovic & Hocenski, 2010). For those IT administrators who are informed about the risks involved in transitioning their applications to the cloud, they may have trouble placing values on these risks to determine how likely it is that a certain risk will affect them. Additionaly, security conscious IT administrators often struggle to choose between a number of similar cloud-service providers by looking at their security offerings because they don't have a strong enough background in terms of mitigating risk in cloud environments to figure out exactly what they need to do in order to keep their applications secure and to protect their company from litigation in the case that the security of their cloud applications is compromised (Takabi & Joshi, 2010).

2.2 Security Concerns

Security analysts have raised a plethora of concerns about security in cloud environments. These concerns tend to fit into one of the following two categories: 1) System, and 2) Operation. The main sources of concern for each category are broken down in detail below (Tanimoto, Hiramoto, Iwashita, Sato, & Kanai, 2011).

2.2.1 System

Multi-Tenancy:

Cloud providers are able to provide flexible, high-powered, and fully-scalable solutions at relatively low cost. One of the main reasons that they can offer these systems at such low cost is by allocating the same resource pools to a variety of different applications. Cloud providers employ virtualization technology to separate these different applications in spite of their shared physical resources, but if a vulnerability is found that allows an attacker to breach this virtual separation of applications, an attacker whose processes are allocated to the same resource pool as a company's production environment may be able to steal data or disrupt that company's business (Popovic & Hocenski, 2010).

Multi-tenancy can cause a number of security concerns even if an attacker is not given direct access to the same resource pool as a company's production environment. Because different applications call for a wide range of security policies, if any application on a resource pool does not have stringent security policies (a testing environment for example), an attacker may be able to gain access to the application with the less-strict security standard and use it as an attack point to disrupt a company's production environment (Takabi & Joshi, 2010).

Data Deletion:

If a user requests that his or her data be removed from your service and your data storage is managed in-house, unless it is required by law to keep this data for a certain amount of time, it is easy for a company to delete its user data — they merely need to erase all copies of the user's information from their records. When data storage is managed by an external source such as a cloud-service provider, however, data deletion may not be this easy. In many cases, the cloud-service provider holds different goals than the companies that make use of its services. In the circumstance that a company requests the

deletion of their users' data from their cloud-service system, the company aims to completely remove the users' data from their records, where the cloud-service provider aims to keep multiple backup copies so that the service could be restored should they suffer from a disruption. When a company requests that a customer's data should be deleted from their systems, if the data is managed externally (as is the case with cloud-service solutions), the company cannot be sure that the customer's data has been deleted from all backup locations when they request it to be (Morin, Aubert, & Gateau, 2012).

2.2.2 Operation

Compliance and Regulation:

Many companies are required by law to uphold very specific standards in terms of how they operate their business, where they store their users' data, how long they should maintain records of their users' data, who has access to their data, etc... When a company's business operations are governed by compliance laws, they must ensure that they continue to maintain compliance when they move their operations to the cloud. The issue of maintaining compliance in a cloud environment is a huge concern in industries such as banking and various medical fields, and it certainly needs to be addressed when discussing risk management and the cloud (Martens & Teuteberg, 2011).

Managing Confidential Information:

When it comes to managing confidential information, introducing a cloud-service provider as an additional party who has access to that confidential information may be another source of risk. In many cases, a cloud-service provider will guarantee that your confidential information will not be accessed or tampered with, but granting more people access to your data increases the likelihood that a malicious insider will take advantage of it (Tanimoto, Hiramoto, Iwashita, Sato, & Kanai, 2011).

3.0 RISK MANAGEMENT (DEFENSES)

3.1 Introduction

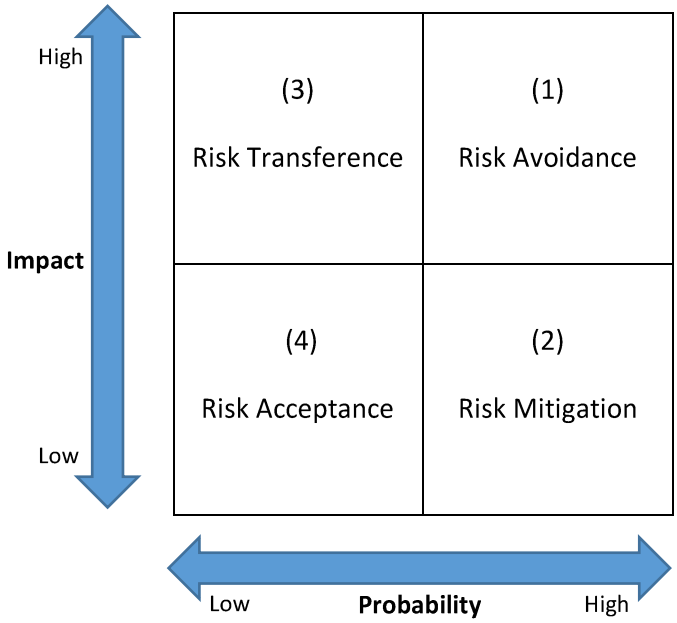
Risk management is defined as "the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events" (Hubbard, 2009). Risk management is a processs that can and should be employed through almost all aspects of business from acquiring a company to implementing a new piece of technology in a company. When considering whether or not to implement a new piece of technology in their company, managers may employ risk management techniques in order to plan for potential future risks or issues that may come along with the use of this new technology (Hubbard, 2009).

The first step involved in technology risk management is the identification of potential risks and/or challenges that may develop when implementing a new technology. This risk management step involves extensive brainstorming and research about the technology that you are going to implement. Once the major risks are identified, each risk should be individually considered and ranked according to the likelihood that this risk could occurr and the negative impact that this risk would have on your company should it be realized. Following this, the likelihood and impact ratings should be used to create a priority ranking for the risks. Finally, once the risks have been prioritized in terms of importance, a strategy should be employed to minimize, monitor, and control the probability that these risks occur.

Risk management is an iterative process that should not be forgotten after its initial consideration during the implementation of a new technology. The risks that are associated with new technologies tend to change often, so it is necessary to re-assess your risk management strategy on a regular basis (Zhang, Wuwong, Li, & Zhang, 2010).

3.2 Mitigating Risk

Risk management provides administrators with a step-by-step process that they may follow in order to identify and control the risks that have the greatest potential to negatively impact their company. After administrators have identified the high-priority risks for their application, they are faced with devising a strategy to mitigate these risks. Coming up with this plan for mitigating risks can be very challenging and is often a daunting task (Zhang, Wuwong, Li, & Zhang, 2010). To simplify the process of creating a strategy to mitigate risk, you can start by reading through your list of high-priority risks and placing them in one of the following four categories based on their likelihood and impact rankings:



(1) *Risk Avoidance:* Avoid the risk completely
(2) *Risk Mitigation:* Decrease the risk level to a point at which the risk can be accepted
(3) *Risk Transference:* Transfer the risk to a third party
(4) *Risk Acceptance:* Accept the risk unconditionally

3.3 Risk Management and the Cloud

The basic concepts of risk management explained in the previous section can be directly applied when developing strategies to mitigate risk in cloud environments. To help IT administrators make use of risk management when transitioning their applications to cloud-service solutions, I have developed a risk management field guide that details the major risks that many companies will face when they move their applications to the cloud and suggests ways in which they might mitigate each risk.

You may notice I suggest that risk transference be used to mitigate many of the risks that are identified in the field guide. The reason for this is many of the major risks that are introduced by cloud-service solutions cannot easily be managed internally due to the fact that the applications will be running on remote technology that is owned by the cloud-service provider. Although your company cannot easily manage these risks internally, it is still possible to protect yourself from these risks by negotiating a Service Level Agreement (SLA) with the cloud-service provider before agreeing to purchase their solution. The technicalities that are involved in drafting a SLA are beyond the initial scope of my research, but if you would like to learn more about SLAs, numerous scholarly articles have been published on this exact topic including the following reference — (Morin, Aubert, & Gateau, 2012).

4.0 SUMMARY

In summary, when deciding whether or not you should move a particular application to the cloud, security should be one of your top concerns. If you decide that it would be worthwhile to employ a cloud-service solution in your existing environment, you should make use of classic risk management strategies to categorize, prioritize, and mitigate the risks that go along with implementing a cloud-service solution. To help IT administrators make use of risk management strategies when they employ cloud-service solutions, I have constructed a risk management field guide that is an aggregate of all of my research on risk management and the cloud.

LIST OF REFERENCES

Hubbard, D. (2009). *The Failure of Risk Management: Why Its Broken and How to Fix it.* Hoboken, NJ: John Wiley & Sons.

Martens, B., & Teuteberg, F. (2011). Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model. *Americas Conference on Information Systems* (pp. 1-10). Detroit, Michigan: AMCIS.

Morin, J.-H., Aubert, J., & Gateau, B. (2012). Towards Cloud Computing SLA Risk Management: Issues and Challenges. *45th Hawaii International Conference on System Sciences* (pp. 5509-5513). Honolulu, HI: IEEE Computer Society.

Popovic, K., & Hocenski, Z. (2010). Cloud Computing Security Issues and Challenges. *MIPRO, 2010 Proceedings of the 33rd International Convention* (pp. 344-349). Opatija, Croatia: IEEE.

Takabi, H., & Joshi, J. (2010). Security and Privacy Challenges in Cloud Computing Environments. *Security & Privacy, IEEE*, 24-31.

Tanimoto, S., Hiramoto, M., Iwashita, M., Sato, H., & Kanai, A. (2011). Risk Management on the Security Problem in Cloud Computing. *First ACIS/JNU International Conference on Computers, Networks, Systems, and Industrial Engineering* (pp. 147-152). Jeju Island, Japan: IEEE Computer Society.

Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010). Information Security Risk Management Framework for the Cloud Computing Environments. *Computer and Information Technology, 2010 IEEE 10th International Conference* (pp. 1328-1334). Bradford: IEEE.