Cloud Storage or Not?

University of the Cumberlands

Dr. Brian Bertrand

Jacob Jeffers

ISOL 536 – Security Architecture and Design

07/30/2021

**Abstract**

In this paper, I am assuming the role of a CISSO of a Major E-commerce Organization. The organization has decided to migrate its entire IT infrastructure and associated processes to the cloud. Considering the ecosystem of the cloud and the ever-present threats, I will work to develop a secure implementation plan which includes the ability for threat modeling and simulations.

**Table of Contents**

Cover Page ………………………………………………………………………………………..1

Abstract …………………………………………………………………………………………...2

Table of Contents …………………………………………………………………………………3

Mid-Term Project ……….………….……………………………………………………………..4

Resources …………………………………………………………………………………………6

**Cloud Storage or Not?**

Chief information systems security officers (CISSOs) are executives responsible for the organization’s information and data security (Fruhlinger, 2021). Their roles include security operations, data loss and prevention, security architecture, identity and access management, and governance (Fruhlinger, 2021). Most large-scale enterprises utilize a CISSO of around 80%, according to Fruhlinger (2021). Most CISSOs job responsibilities are related to IT security; however, they could include physical security and other IT operations.

It is no secret that cloud storage will make the data more accessible and available. Cloud storage allows the organization some flexibility and scalability, provide redundancy in an outage, and provides synchronization throughout the organization (Singh, 2020). I would recommend utilizing a secure cloud vendor for the organization to provide confidentiality, integrity, and availability (Schoenfield, 2015). However, many cloud vendors lack data security and privacy (Singh, 2020). It is essential to detail the services offered by the cloud vendor before deciding. We need to look for intruder detection or prevention tools, firewalls, DDoS attack mitigation tools, and other things to prevent attacks (Singh, 2020).

The first step is to build a robust service-level agreement with the cloud vendor detailing specifics on what services the cloud vendor will provide. Some things to include in this step would be detailing how the data would be stored in transit, in use, and at rest; it would include what encryption methods will be used when moving data, access control, and identity management solutions should also be considered. The next step is for the organization to build the security architecture and establish the design with the cloud vendor. We want to ensure the contracted cloud vendor provides the proper security for the data stored in the cloud. The third step is to ensure that the cloud vendor provides an excellent cloud email solution. Some things we want to include in this solution are antivirus, spam prevention, protection from information leaks, email monitoring, and the ability to edit rules as needed (Watts, 2021).

Once the contract has been negotiated with the cloud vendor, a penetration test should be conducted in a simulated environment using fake data or useless information before transferring the entire organization’s IT infrastructure to the cloud. In this scenario, as the CISSO, I would do everything to authorize a team of the best penetration testers to hack into my simulated environment and write a report on steps needed to improve the cloud infrastructure. I would then seek to remediate all those security risks before moving to the cloud. Once remediated, the architecture should be ready to be moved to the cloud. I would provide security training and instructional training to the employees beforehand.

**Conclusion**

As the CISSO of a large enterprise, there is a ton of responsibility for this individual. They are paid well, but the stresses are high. Information security is one of the most critical aspects of an organization. In this scenario, the enterprise seeks to move its infrastructure to the cloud because it provides flexibility, availability, and scalability. As the CISSO, we are tasked with ensuring the data remains integrity and confidentiality as well. Beginning a search for the right cloud vendor to provide these goals should start with a robust service level agreement then progress to an established security architecture between the organizational goals and what the cloud vendor can provide. In addition to this, a secure cloud email should be developed and implemented. To test the security posture, an intensive penetration test should be conducted, and then the security posture needs to be remediated. After this, users need to be provided training on maintaining a secure environment and using the new cloud-based solution. Doing this should ensure a seamless transition to the cloud.

**References**

Fruhlinger, J. (2021, April 1). *What is A CISO? Responsibilities and requirements for this vital role*. CSO Online. <https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html>.

Schoenfield, B. S. E. (2015). *Securing Systems: Applied Security Architecture and Threat Models*. CRC Press.

Singh, V. (2020, April 28). *10 Benefits of Using Cloud Storage*. Cloud Academy. <https://cloudacademy.com/blog/10-benefits-of-using-cloud-storage/>.

Watts, J. (2021, July 26). *The top 11 email security gateways*. Expert Insights. <https://expertinsights.com/insights/top-11-email-security-gateways/>.