**ECPI University**

Unit 2 Research

**"Security Analysis”**

**CIS 212**

**Rafat Khandaker**

**10/15/18**

**Introduction**

As a cyber network security administrator, I have specialized in understanding the importance of valuable assets in an organization and defend it against cyber-attacks. With the increase attempts to breach network security, new companies must follow a standardized compliance to protect itself against cyber threats. These defense tactics will include: defending attacks against cloud services; Ability for a company to recover from cloud breach disasters; Risks associated with offshore hiring; Ability for a company to audit access to cloud services; Ability for a company to monitor growing assets, alongside security; Providing quality of service to our customers. Working alongside our team of 10 Network administration, 20 developers & external HR department, we will be able to scale the needs of this business while ensuring security to its assets.

**Addressing Security Concerns**

Our current company architecture involves providing programmers and consultants access to our infrastructure, cloud services through a DSL (Direct Service Line). This will ensure that our that our programmers maintain maximum up-time and connection to our infrastructure to push updates to projects. In order to stabilize this workflow, providing maximum up time connection to employees, while maintaining a good security architecture. Let us analyze security concerns with offshore employment connecting into cloud services. In an article written in CSO from IDG blogs, Dean Davison addresses the “Top 10 risks of offshore outsourcing.” He explains that companies move into offshore hiring, over exceed their expectation for savings **(Davison, 2004)**. There are many risks associated with Offshore expansion, including Data security protection where we cannot expect IT organizations, offshore, to follow the same standards and robust security practices that are followed internally. Capability Maturity Model, explains a company's readiness to adopt an offshore model **(Davison, 2004)**. This model describes a repeatable model that can track internal process. Loss of business knowledge is a concern for offshore modeling, when employees are hired and dismiss their position. A company should have a secure way of handing information over and restricting access to it the same way, a process known as “Knowledge Transfer” **(Davison, 2004)**. Underestimating how failure to deliver can impact company assets.

Security in our company design should also include the technology used in place. Let us assess all the concerns of hosting a cloud model & network related security. According to "Cloud Computing Fundamentals”, delivered by Kris, Jamsa, are some concerns a company should address when migrating to cloud services. In the text: Cloud hosted environments are limited by the vendor. There are a wide variety of Cloud Services and each vendor has their own compliance structure. Cloud environments give control of our company’s data and internal operations to 3rd party vendors **(Jamsa, 2013)**. Alongside our cloud infrastructure, network security is needed to prevent any potential external attacks between user nodes and the cloud service. According to InfoSec Institute, common Cloud computing attacks through network include: Denial of Service, Malware Injection Attack, Side Channel Attack, Brute forcing, Authentication and MiTM attacks **(InfoSec, 2018)**.

**Providing Security Suggestions**

From my analysis of this company’s business architecture, I suggest we take steps to document the company’s assets, key important information, size of the digitized information, security role groups of individuals and engineer the “principle of least privilege,” approach to distributing business permissions. Let us establish a baseline for our technological security, document what is required from securing minimum assets & what is required from securing high risk assets. Let us a build an infrastructure addressing and take measures for testing our cloud hosted infrastructure, in development and deployment of its services. Let us create comprehensive auditing systems that will keep active logs from users accessing our services. Let us distribute appropriate permissions between project managers and programmers to maintain the flow of workload. Let us make sure that knowledge transfer will not be a problem between offshore employee hires, giving responsibility to senior management to retain and build on transferring knowledge. Let us create documentation, back out procedures and create a home base infrastructure to host our service incase our cloud provider fail to deliver the needs of our business. Let us keep an active back up our own services & provide internal servers to back up data from the cloud deployment. Let us create thorough disaster recovery procedures, from loss of employees, loss of data, loss of provider. Let us generate good reports from weekly/ monthly to yearly progression of our business. Let us provide active feedback surveys from our customers to find suggestions to grow business on a stable security platform.

In conclusion, security compliance in a company will require professionals to think outside the box. Today, cyber-attacks may come in many forms. Attackers today, are willing to work between the lines to penetrate security through physical, psychological and technological attacks. In order for us to combat these attacks, we have to understand the needs of our business, It's important assets and weaknesses in our business protocol. In this particular case study, we have a growing business, that Is operating in an offshore environment where employees will work remotely, accessing a 3rd party cloud environment. The cloud environment will host our company’s assets. So, to tie the knot, the goal of our security analysis is to address the potential risks and provide a stable business solution to ensure the smooth transition between this working architecture.

**References**

**(1)** Kris, Jamsa. (2013). *Cloud Computing.* Cengage

**(2)** Ciampa**,** M.(2016). *CompTIA Security+ Guide to Network Security Fundamentals.* Cengage

**(3)** Davison, Dean.(2004). *Top 10 Risks of Offshore Outsourcing*. Retrieved From: <https://www.csoonline.com/article/2117420/data-protection/top-10-risks-of-offshore-outsourcing.html>

**(4)**  Cloud Computing: Attack Vectors and Counter Measures. (2018)**.** Retrieved from: <https://resources.infosecinstitute.com/cloud-computing-attacks-vectors-and-counter-measures/#gref>