**ECPI University**

**Unit 5**

**“Current Topics in Cloud Security”**

**CIS 142**

**Rafat Khandaker**

**11/05/18**

**Introduction**

There are many risky precautions that should be taken into consideration when migrating to cloud services. Some of this includes the limitations by governance and law, changes in network regulation, threats from outsourcing resources, data privacy breach & etc. History of events that triggered changes in privacy laws from the U.S, creating new regulations in network and cloud computing technologies. Changes in Net Neutrality laws that can determine the bandwidth preference from certain providers. Internet censorship laws, limiting the amount of data that can be placed on citizens. Importance of risk management and negligence to protect consumer data penalty. Finally, considering the risks of moving into an offshore model.

**Passing of Legislation in Different Countries**

According to Branko Vlagin, he wrote in an article; passing legislation in the US and other countries that can have an impact on cloud security. Net Neutrality & the patriot Act gives the US intelligence, rights to retrieve US citizen data off foreign servers **(Branko, 2018)**. Europe & France are known to disregard privacy laws and spy on their citizens, passing Investigatory Powers Act. Internet censorship law, passed in 2012, allows Russia to limit where their citizen data can be placed **(Branko, 2018)**. In Australia, data retention laws require citizen’s metadata. In the US, Trump passed CLOUD act that allows the US to retrieve data from foreign jurisdiction to put under view for unlawful acts of behavior **(Branko, 2018)**.

**Importance of Risk Management**

Risk management is important to prepare a company for the worst-case scenarios and provide a way for business to continue operations after a major catastrophe. It is a part of the business security model to report threshold of damage that a business can endure and work to recover from. According to the article, Cyber Security contains a global standard which can fine organizations an administrative fee: (20,000,00 EU for breaches made on European public sector), for example **(National Conference, 2018)**. Homeland security has established national security laws to standardize business security model, including notification laws that force organizations to report any data breaches that pose a threat to the public sector, state by state **(National Conference, 2018)**. Homeland security also published a Cyber Security strategy plan in order to improve cyber security standards across federal and non-federal entities across the nation by 2021. This shows that government is also becoming more aware and acknowledging the threats associated with technology.

**Data Breach Raising Concern in Network Security**

According to an article written by Branko Vlajin, he explains how recent breaches of public privacy gained more interest for US policy makers to invest into National Cyber Security enforcements. Such events like Equifax data breach, exposing 142 million citizenship data or Cambridge Analytica scandal. The effect of these kind of scandals can have a huge effect on a company's assets. The risks are even more uncertain when migrating to a centralized cloud model. A deeper look into the Cambridge Analytica scandal: The federal Trade Commission opened an investigation into Cambridge Analytica. The voter profiling company, accessed data from 50 million Facebook users. Which alarmed the GOP-controlled Senate Commitee **(National Conference, 2018)**. Facebook lost 12% of their stocks over the weekend **(National Conference, 2018)**. In the event, A developer created an app based off Facebooks API, that allowed users to take a personality quiz. He built a profile of the data collected from the app and stored it into a private database. This event was mis-used the term "Breach." None of fakebook's technology or data was hacked, users voluntarily gave data away to a 3rd party entity. Mark Zuckerberg and his team had to immediately launch an investigation and address the Senate and European union of the event **(National Conference, 2018)**. If Facebook is a centralized solution that provides API service for third party usage, imagine the potential risks with other 3rd party services on the cloud.

**Outsourcing Expectations**

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.

**Conclusion**

In conclusion, there are concerns that have to be addressed that threatens the Cloud network solution model. This includes recent events in national security, that has changed legislation to allow government to monitor citizen privacy. Risk management and concerns when a breach occurs, companies may be subject to fines and penalties. False hopes and expectations from outsourcing model into the cloud. Concerns about data breach incidents that has drastically effected company assets.

**References**

**(1)** Jamsa, K. (2013). *Cloud Computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security, and More*. Burlington, MA.: Jones & Bartlett Learning.

**(2)** Top Cloud Hosting Requirements. (2015). SelectHub. Retrieved From: <https://selecthub.com/cloud-technology/top-cloud-hosting-requirements/>

**(3)** Vlajin, Branko. (2018). *Cloud Laws and Regulations*. Retrieved From: <https://www.cloudwards.net/what-you-need-to-know-about-cloud-laws-regulations/>

**(4)** 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>

**(5)** *Security Breach Notification Laws*. (2018). National Conference of State Legislators. Retrieved From: [http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (Links to an external site.)Links to an external site.](http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx)

**(6)** *U.S. Department of Homeland Security Cyber Security Strategy.* (2018). Retrieved From: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy\_1.pdf

**(7)** Robinson, Meyer. (2018). *The Cambridge Analytica Scandal, in 3 Paragraphs*. Retrieved From: [https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/ (Links to an external site.)Links](https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/)