**Prospectus**

**Cyber Security: Behavioral Analytics**

(Technical Topic)

**Actor Network Theory: Relationship between users and companies**

(STS Topic)

By

Jui Tao Tsai

10/31/2019

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: Jui Tao Tsai

Approved: _____ Date _____

Ben Laugelli, Department of Engineering and Society

Approved: Nada Basit Date 05/04/2020

Nada Basit, Department of Computer Science

## Introduction

One of the biggest and most rapidly growing banks, Capital One, has been depended upon to store important information such as credit card or social security numbers. As one of the leaders in the finance industry, Capital One retains millions and millions of data from customers. One of the easiest ways to store data is to use Amazon S3, which is a service offered by Amazon to store and retrieve data from anywhere on the Internet. Such storage is an extremely durable, highly available, and scalable data storage infrastructure with very low costs (Amazon S3 bucket FAQ, 2002). However, a lot of sensitive information from Capital One is stored in a public S3 bucket, which offers a relatively high accessibility. With this approach, it is a lot easier to handle millions of data with a relatively low cost. But at the same time, plenty of sensitive data is at stake and it is a lot more vulnerable to hackers who have a good understanding of AWS security. According to Capital One, an unauthorized user accessed the data stored in AWS S3 buckets and extracted the data and posted information about it on GitHub (The hunt for data analytics, March, 2015). Fortunately, the hacker, Paige Thompson, who made very little effort to hide her identity, displayed her real name on GitHub, which makes it a lot simpler to track a hacker's ID and address (Meet Paige Thompson, 2019). However, it still shows how vulnerable the system can be without being cautious about users, behaviors, and developing secure ways to handle or store sensitive data. There are many potential solutions to this incident such as placing data in a safer place. However, to tackle this problem, one of the approaches I propose is to use User Behavior Analytics (Inside Behavioral Analytics, 2019), which allows companies to provide insights to user behavior; that way, companies such as Capital One would always have an extra layer of security to ensure that users within the system behave normally.

Moreover, it is critical to look at the science, technology, and society (STS) aspect of the problem. Accordingly, I would use Actor-Network Theory to analyze a specific case. Each actor such as the bank whose goal is to store and secure sensitive data, or users within the system play an important role within the network. Understanding the network and figuring out a way to maintain a stable network within the system would help solve the problem of leaking important information. If we only address the technical problem and ignore the socio-technical problem, we may lose the opportunity to see the whole overview of how the role of users may impact how different roles should play out and the impact of those roles that led to this Capital One data breach problem.

To offer an effective solution to the data breach problems, both the technical and social aspects of the problem must be considered. Below, I describe a technical process for a new way of monitoring users to ensure the security within the system. Additionally, I use Actor-Network Theory to analyze how users disrupted a working socio-technical system for Capital One.

## Technical Problem

Cyber Security has always been one of the most important components for technology or finance companies that retain sensitive data or important information. The security protections from each company have been reinforced. Some protection strategies are getting smarter and more accessible such as User Behavior Analytics where companies use Deep Learning to detect suspicious behaviors from a user or cloud services that offers security assistant so that an enterprise would not have to build an entire service to prevent cyber attacks. In particular, User/Behavior Analytics has been a hot topic that has been spread around the cybersecurity industry; through Behavioral Analytics we can develop an understanding of how frequently

certain processes and applications on a device are used, who accesses the asset and how often, what other devices the asset communicates with, and so on (What Exactly are Behavioral Analytics, December 7, 2018). Nevertheless, Behavior Analytics is not widely used as a means of security but more of a way to predict customer trends or activities to increase sales or simply a way to focus on employees to protect data from leaking. One of the most infamous data breaches happened recently to one of the fastest growing financial industry leaders, Capital One, where a hacker stole millions of relevant personal information such as bank account numbers or social security numbers as an unauthorized user (Consequences: Positive). A good practice of Behavior Analytics is one of the options to prevent such incidents from happening. Companies that retain sensitive and important information should be able to monitor users who log trends of suspicious behavior such as attempting to access database. The description indicates the flawed ways of handling data in the Capital One incident and the benefits of using Behavior Analytics. This new technique of monitoring user activities to catch malware or cyber attackers could be beneficial to companies that handle and store sensitive data.

While being able to maintain and store a great amount of data within the bank with low cost appears to be very efficient and maintainable, the cloud service without proper configuration or setup could lead to data breaches, which may seem to be easy to detect; however, statistics indicate otherwise. According to an article in *Cyber Defense Magazine* titled, "Cyber Security Statistics for 2019" studies show that in most cases it takes half a year to detect a data breach. Furthermore, cyber criminals managed to exploit the credit cards of 48% of Americans back in 2016. In Capital One's case in particular, the hacker claimed that she used a special command to

extract files within a Capital One directory stored on Amazon's servers (Detect Security Breaches Early by Analyzing Behavior, June 4, 2015).

The objective of this technical project is to research and propose a hacker detection technique, "User and Entity Behavior Analytics" (UEBA), for companies like Capital One that customers trust with sensitive data. First, UEBA recognizes and learns user and entity behaviors. It establishes baseline behaviors and patterns using historical data. Therefore, normal behaviors would be detected with the help of statistical models and rules to have comparisons between ongoing behaviors and existing profiles. Secondly, UEBA integrates information of different kinds into a security system. Such an information base will offer helpful data such as logs from security information, event management, network flow data, and packet capture data. Last, it presents analytical results very quickly, and companies may utilize this security system to detect patterns and clues of unauthorized access and users as well as any suspicious actions (Detect Security Breaches Early by Analyzing Behavior, June 4, 2015).

## STS Problem

Capital One used S3 bucket that Amazon provides as one of the easiest and most maintainable ways to store a great amount of data. Usually, it is a very secure platform that does not give too much accessibility(How can I secure the files in my Amazon S3 bucket?, May 17, 2019). However, misconfigurations of the firewall allowed the hacker, Paige Thompson, to trick the firewall and get into the system. While it is true that misconfiguration and the lack of security within the system caused the data breach incident, this explanation overlooks some other factors such as user behaviors and the roles of other software platforms like GitHub or Slack. If we just focus on the system within Capital One rather than looking at the role of users and other software

platforms, we will not have an adequate understanding of how all theses in conjunction with software platforms actors like Github and Slack contributed to the data breach. Drawing on Actor Network Theory, I argue that, in addition to the vulnerabilities in Capital One's system, it was the relationship between users and Capital One that caused the Capital One data breach. Actor Network Theory views technology as an interconnected system of various and diverse human and non-human components or "actors" that have been put together by a network builder to establish a stable and integrated "actor network" in order to accomplish a particular goal (Callon 1987). Actor Network Theory will allow me to describe the power dynamics within Capital One's heterogeneous network to identify the actors most responsible for its failure.

## Conclusion

This technical report serves as a design for companies that collect and hold a big amount of data. This design will be centered around Behavioral Analytics, which allows companies to keep track of user activities and detect unusual or suspicious user behaviors. The STS research paper will draw on Actor Network Theory to explain why the Capital One network failed.

The results of the technical project will help offer solutions to the socio-technical issue of keeping companies safe from cyber attacks by analyzing and detecting user behaviors and catching hackers as early as possible. The findings from STS paper will serve as a way to examine the power dynamics between users and set up proper rules within the system to keep companies aware of a variety of factors.

References

S3. (2002). Retrieved from https://aws.amazon.com/s3/faqs/.

Lemos, R. (2015, March). The hunt for data analytics: Is your SIEM on the endangered list? Retrieved from https://searchsecurity.techtarget.com/feature/The-hunt-for-data-analytics-Is-your-SIEM-on-the-endangered-list.

Frankenfield, J. (2019, August 29). Inside behavioral analytics. Retrieved from https://www.investopedia.com/terms/b/behavioral-analytics.asp.

SecurityondmdWEBMaster. (2018, December 7). What exactly are behavioral analytics? Retrieved from https://www.securityondemand.com/news-posts/exactly-behavioral-analytics/

Team, M. (2019, March 21). Cyber Security Statistics for 2019. Retrieved from https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/.

Levy, H. P. (2015, June 4). Detect security breaches early by analyzing behavior. Retrieved from https://www.gartner.com/smarterwithgartner/detect-security-breaches-early-by-analyzing-behavior/.

Colby, C. (2019, August 12). Capital One data breach: What you can do now following bank hack.

Retrieved from https://www.cnet.com/how-to/capital-one-data-breach-what-you-can-do-now-following-bank-hack/.

S3. (2019, May 17). How can I secure the files in my Amazon S3 bucket? Retrieved from https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/2019-05-17

Thesheetztweetz. (2019, July 30). Meet Paige Thompson, who is accused of hacking Capital One and stealing the data of 100 million people. Retrieved from https://www.cnbc.com/2019/07/30/paige-thompson-alleged-capital-one-hacker-stole-100-million-peoples-data.html.

Callon, Michel (1987). Actor Networks, Society in the making: The study of technology as a tool for sociological analysis (pp. 92-99). Cambridge, Massachusetts: MIT Press.

Word count: 1742