**2019 Capital One Data Breach**

Luis Ruiz

The George Washington University

PSCS 3100: Principles of Cybersecurity

Dr. Hiep D. Tran, PhD

November 17, 2020

Since its founding in 1994, the Capital One Financial Corporation has grown into one of the top banks in the United States of America. This fact has in no doubt been due to their bold strategies and innovative ideas that their other competitors would hesitate to adopt. In fact, according to Golden, their former Vice President in Cloud Strategy they shifted their mindset in 2012 to operate more like a tech company instead of a financial company (Studio 61, 2018). That may be why in 2015, the company unveiled its plans to work with Amazon Web Services and move toward Cloud services and close their private data centers. This type of full migration was not something that the other top banking systems were yet pushing towards due to the potential risks involved. Consequently, Capital One suffered a catastrophic data breach in 2019 after a former Amazon Web Service Employee exploited a known vulnerability that resulted in over 100 million people having their account information leaked.

In July, Capital One publicly announced the data breach that occurred in March that affected hundreds of millions of American and Canadian customers. Prior to their announcement, Capital One’s stock was just under $100, but it later fell to some lows of just under $85 until September (Trefis Team, 2019). Although the backlash Capital One faced in the stock market was harsh, it was not permanent and following September their stock rose to its previous marks, even topping at $106 in January. The data breach only served to momentarily harm Capital One and show that their public support lapsed, the subsequent drop in their stocks had no correlation to this event so we can be unsure whether it would have had any real impact on their stocks. It will be important to know how resilient Capital One is in the market even after frequent bouts of negligence and legal threats. To truly regulate such a large financial institution and have it in check they need to be taken to court otherwise, they will disregard the responsibilities they have to their customers for increased profits in the long term. Therefore, the real impact that Capital One faced on their business was the class action lawsuit levied against them, the fines imposed on them and subsequent court rulings that demanded their reports over the data breach.

Succeeding the breach Morgan and Morgan, a highly successful law firm with experience in data breaches, claimed that Capital One did not take reasonable care to protect the information of their customer’s data (Dellinger, 2019). As such, there were also $80 million dollars in federal charges claiming negligence after having discovered that their board of directors took no action after an internal audit raised security concerns (Gandel, 2020). Preceding the claims and charges, the District Court of Eastern Virginia determined that the data breach reports to litigation as it again failed to follow proper procedures when dealing in legal matters following the breach (Rosenthal, Marciano, & Hutnik, 2020). This issue was all vital to understand how Capital One operates itself as a financial institution or technology company, which shows a lack of due diligence when dealing with vital customer information, disregard for policies and procedures and a confused business impact analysis on how to overcome threats to their business functions and recovery.

In fact, the data breach could have been prevented if Capital One employees were more attentive. The former Amazon Web Service Employee, Paige Thompson, infiltrated the network by bypassing a web application firewall that was not installed correctly. Amazon confirmed their cloud security was not compromised but that an error in the web application firewall caused the breach (Douglas, 2019). This event highlights one of the biggest risks that was associated with Capital One’s migration to the Amazon Web Service’s Cloud, which is an increased risk of insider threats. This data breach wasn’t an unknown hacker or one of Capital One’s employees, it wasn’t someone attacking the network or firewalls trying to gain access, instead it was a carefully orchestrated infiltration by a former Amazon employee that knew exactly how to gain access to Capital One’s cloud servers. These third party services help lower costs of data security by filling those roles with their own trained experts as well as allowing the client to focus on their field of expertise (Siegel, 2019) but, they also come with the drawback that those experts aren’t the client company’s employees, and they don’t have control over them. This type of outward reliance raises the potential for insider threats since now, another company’s employee also has insider knowledge on the inner workings of the client company’s security settings.

Going forward, it is important to note that even by hiring a third-party to provide a more secure service, it is always the client’s sole responsibility to ensure that their costumer’s data is protected. In this case, Amazon was not responsible for how Capital One’s employees configured the firewall nor were they responsible for how Capital One responded to this event. This issue is because only Capital One can manage their employee’s compliance, their own incident response, and the level of insider threats to their business (Cheslock, 2020). Third parties only have the responsibilities cited in their contracts such as providing the cloud service, and the tools to manage it and its security but, how those tools are utilized depends on the client’s strategy. Not understanding the limits of these responsibilities will leave the client unsecure and open to attacks. By rushing to migrate to the cloud and failing to meet their responsibilities Capital One left themselves vulnerable to a breach from the web application firewall.

The data breach and subsequent fallouts that Capital One faced were some of the largest since the Equifax breach, so after failing to control the breach they should have immediately sought to outside consult to prepare for legal litigation to at least control the legal damages incurred on them. In this case, Capital One was quick to hire Mandiant as their retainer for the incident response planning but, this response also ended up being a mistake. Capital One had previously contracted Mandiant for other services that had no correlation to the litigation, however, their statement of work in the litigation was identical to their previous work, which had the courts over-rule their report had protected status (Black, 2020). Typically, when a company creates an incident response report either with their own team or outside consult, it becomes a protected work that cannot be forced to be released to the public. This fact is because the incident response report has sensitive information that refers to their procedures that can be dangerous for other hackers to obtain or learn from, or simply due as a way to shield themselves from even more legal repercussions. Either, or, it is atypical for incident response, reports to be shown to the public for further legal litigation however, since Capital One could not prove that their consult’s plan was any different from their previous work, which was not protected, then the report itself has no legal grounds to be considered protected any longer. Going forward, Capital One has the legal obligation to release their co-operative incident response report that details all their failures that led to the breach. The greatest issue that it presents Capital One with is that they have an impending lawsuit from Morgan and Morgan over the breach, which the details of the report will be provided to. This could have been entirely avoided had they not retained Mandiant but, it will serve as a precedent for all future companies as to how they work with third party security services (Stone, 2020).

With all things considered, Capital One did a very poor job at mitigation the damages incurred after a single person gained access to over 100 million individuals' account information. If we disregard the fact that they didn’t correctly configure the firewall protecting their customer’s sensitive information, they also failed to contain an insider from exploiting that weakness, acting when their directors knew of the issue, and failing to follow proper procedures when retaining outside consult. Capital One should be to stop thinking like a technology company and rushing into radical changes without understanding their full responsibilities. They are a financial institution with millions of people depending on them for their security, by rushing to migrate to the cloud they evidently neglected to take proper procedures to safeguard their customer’s data. In fact, such a large-scale change from a traditional data security methodology to cloud security was a huge undertaking with far too many possible risks that they were not prepared for. For future changes, they should rely on a more gradual phased approach when migrating sensitive data.

Secondly, Capital One needs to enforce policies and compliance for all their directors and employees. Thompson would not have been able to breach their firewall if Capital One IT employees did more penetration testing to make sure that it was installed correctly and had no obvious exploits. It is vital to always test software and hardware for performance before using them to strenuous use, if they cannot pass those tests then they should not be put in use. If their policies do not mandate the testing of their software or hardware before use, then their policy should be revised and monitored for compliance. As for compliance, it is humiliating that their board of directors previously knew about their security flaws after an internal audit but still choose to ignore to the issue. What is the point of having internal audits checking for security flaws if they will simply be ignored? There is no point of having policies and procedures if they will then be ignored. Even when they knew they were going into legal litigation, they failed to follow proper procedure, which led to a court order to release their incident report. Based on their actions, Capital One faced was a systemic negligence of proceedings, and the repercussions for their actions have so far been costly.

Finally, there needs to be more attention placed that their employees do their due care and management does their due diligence. It cannot be overstated how vital the firewall was to protect their customer’s data and there should have been more care into ensuring that it was fully operational before rolling it out. As for management, they need to be diligent in ensuring that there are major issues or security flaws and if there are, that they be addressed immediately. A lack of both traits made Capital One not only vulnerable to Thompson but also Morgan and Morgan. They also need to fully understand the responsibilities that they have and why when it comes to securing their cloud because the responsibility in this case did not fall on Amazon. Client-side security is just as, if not more important than the third-party service, if neglected it undermines the migration for increased security and cost savings.

In conclusion, by trying to rapidly change in order to stay ahead of the game, Capital One began to fundamentally change how they operate which caused a series of systemic issues that led to one of the largest data breaches in 2019. They failed to control each issue which caused a downward slope that lead to $80 million in federal charges, a lawsuit, and a court order to release their incident report to the attorneys that are suing them. In the end, they did manage to move to the cloud but, at the cost of their goal to save money. They focused too much on trying to change how they operate and migrate to the cloud when they should have instead focused on being a financial institution that protects their customer’s data. Moving forward they must revise their policies and procedures to ensure that their customers come first and that their employees and management are complying to those orders.

# Works Cited

Douglas, E. (2019, July 31). *The Capital One breach was preventable, experts say. Here's what to do now.* HoustonChronicle.com. https://www.houstonchronicle.com/business/article/The-Capital-One-breach-was-preventable-experts-14268501.php.

Gandel, S. (2020, August 6). *Capital One to pay $80 million fine for 2019 hack that exposed 100 million accounts*. https://www.cbsnews.com/news/capital-one-hack-credit-card-applications-settlement/.

Siegel, R. (2019, July 30). *Capital One looked to the cloud for security. But its own firewall couldn't stop a hacker.* https://www.washingtonpost.com/technology/2019/07/30/capital-one-looked-cloud-security-its-own-firewall-couldnt-stop-hacker/.

Trefis Team. (2019, September 11). *How Could The Recent Data Breach Affect Capital One's Stock?* Forbes. https://www.forbes.com/sites/greatspeculations/2019/09/11/how-could-the-recent-data-breach-affect-capital-ones-stock/?sh=12a689a937b7.

Dellinger, A. J. (2019, July 31). *Capital One Hit With Class-Action Lawsuit Following Massive Data Breach*. Forbes. https://www.forbes.com/sites/ajdellinger/2019/07/30/capital-one-hit-with-class-action-lawsuit-following-massive-data-breach/?sh=467e7f826b1a.

Rosenthal, P. A., Marciano, T., & Hutnik, A. Z. (2020, June 26). *District Court Affirms Need to Turn Over Data Breach Report*. https://www.adlawaccess.com/2020/06/articles/district-court-affirms-need-to-turn-over-data-breach-report/.

Black, K. D. (2020, July 16). *District Court Finds Cybersecurity Forensics Report is Not Protected Work Product*. https://www.bipc.com/district-court-finds-cybersecurity-forensics-report-is-not-protected-work-product.

Stone, J. (2020, June 12). *Here's what that Capital One court decision means for corporate cybersecurity*. CyberScoop. https://www.cyberscoop.com/capital-one-incident-response-mandiant-decision/.

Cheslock, P. (2020, August 24). *The Top 7 AWS Security Issues: What You Need to Know*. https://www.threatstack.com/blog/what-you-need-to-know-about-the-top-7-aws-security-issues.

Studio 61. (2018, November 29). *Capital One redefines banking for the cloud age*. ZDNet. https://www.zdnet.com/paid-content/article/capital-one-redefines-banking-for-the-cloud-age/.