Date: 28 / 03 / 21

Strategy Cybersecurity Roadmap/Plan for the Board

ACCG8086: Cybersecurity, Governance Frameworks and Ethics

Student Name: Mohammed Sadiq Abuwala

Student ID: 45921407

Abstract

Organisations are increasingly incorporating digital technologies in order to make business operations more efficient, and to reach more consumers. Early adoption of digital technologies may provide an organization with significant advantage over their competitors. Capital One is one of the foremost financial firms in the U.S. known for adopting cloud technologies into their platform. Their goal was to achieve more efficient and cost effective scaling in and out, and offer additional smart features to their customers. But the rapidly evolving nature of technologies constantly introduces new attack vectors. Hence, the amount of risk that a business needs to assess and manage also increases. In 2019, Capital One suffered a data breach relating to their cloud technologies affecting approximately 106 million customers. This report discusses the actors involved, attack vector, organisational response, and recovery method used. Finally, a cyber security roadmap is proposed that Capital One could have implemented in terms of the Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 National Institute of Standardsand Technology (NIST) to prevent such an attack.

1. Introduction

1.1. NIST Cybersecurity Framework

NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The Critical Infrastructure Cybersecurity Version 1.1 National Institute of Standardsand Technology (NIST); henceforth referred to as NIST Cybersecurity Framework was developed to help organisations of all sizes to better understand and manage their cybersecurity risks. Compliance under the framework is only mandatory for businesses working under the federal supply chain. Yet, many organisations outside the federal supply chain also strive to comply with the NIST Cybersecurity Framework because it represents best practices for an organisation (Understanding the NIST cybersecurity framework, 2021).

Various other frameworks / best practices are used around the world such as the European Cybersecurity Certification Framework for ICT products in the European Union (EU). For the purpose of this report, we will focus on how Capital One's compliance with the NIST Cybersecurity Framework may have prevented this particular data breach from occurring.

1.2. Rationale for selecting Capital One data breach, 2019

In order to build our cybersecurity roadmap in relation to the NIST Cybersecurity Framework, we have chosen to focus on the Capital One data breach which occurred in 2019 for several reasons. Firstly, it was one of the largest data breaches of 2019 which involved sensitive data such as a customer's banking information, transaction history, credit scores, account linked home / office addresses, phone numbers, and Social Security Numbers (Kirk, 2019). Additionally, it was important to have access to sufficient public records regarding the data breach in order to understand how it occurred and the failures in security controls that lead to the incident. Due to the severity of this incident as discussed above, credible sources of information exist such as reports provided by Capital One to U.S. Security and Exchange Commision, FBI investigation report, and legal testimonies.

2. Case Study : Capital One data breach, 2019

2.1. Actors

According to the criminal complaint by the United States Department of Justice, a former software engineer, Paige Thompson was charged with computer fraud and abuse for her role in accessing data stored by Capital One. "Thompson posted on the information sharing site GitHub about her theft of Information from the servers storing Capital One data" (United States v. Paige Thompson, 2020). A GitHub user who saw the post acted as a tipster and alerted Capital One about the possibility that it may have suffered a data breach. The organization and subsequently the FBI were able to investigate and identify Paige Thompson as the person who had published the post on GitHub regarding the theft of information. This was possible because the profile linked to the published post had a reference to her real name. Furthermore, they were also able to identify her user account on Slack in which she admitted to the crimes (McLean, 2019).

2.2. Timeline of Incident

A timeline of the events that occured gives us a finer idea about the cybersecurity incident and hence noted below:

- ❏ 22 March 2019 - 23 March 2019 : Capital One breach occurs.
- ❏ 17 July 2019 : Tipster alerts Capital One.

❏ 19 July 2019 : Capital One determines an intrusion has occurred (Almost 4 months after the breach occurred) and alerted the FBI.

❏ 29 July 2019 : The actor, Paige Thompson is arrested by law enforcement.

2.3. Technical aspects of the incident

One of the first questions that need to be answered when a data breach occurs is how it was allowed to take place. If the attack pathway is not identified, there is no way to surely know if unknown vulnerabilities still exist in the system. Fortunately, investigators have been able to identify the steps the attacker took to gain access to Capital One's cloud storage. Furthermore, significant passage of time since the breach occurred has also allowed more information to come to light regarding the cyberattack. Upon receiving a tip about a possible data breach, Capital One immediately began their investigation They determined that:

1. The cyber attacker had created a scanning tool that allowed her to identify cloud based web application firewalls that are misconfigured. Once the vulnerable Capital One cloud server was identified, it allowed the cyber attacker to execute commands in order to try gaining access to the server. The attacker was able to first run a command which upon execution, provided the security credentials for an administrator account of a web application firewall known as *****-WAF-Role (Kirk, 2019).

2. The attacker was then able to use this administrator account to gain access to certain Capital One folders stored on the cloud. Capital One was using Amazon Web Services (AWS) at the time of the incident to host their data. "Large enterprises like Capital One build their own web applications on top of Amazon's cloud data so they can use the information in ways specific to their needs" (Flitter and Weise, 2019).

3. Upon gaining access to these folders on the cloud, a "List Buckets" command was used. Upon the command execution, the returned result displayed all the folders and buckets of data in the folders that the particular administrator account (*****-WAF-Role) had permission to access.

4. Finally, a third command ("Sync Command") was used to extract a copy of the data from the folders that the attacker had gained access to.

3.0. Consequences

3.1. Data stolen

Based upon the report released by Capital One, the cyber attack affected approximately 100 million individuals in the United States and approximately 6 million in Canada (Capital One, 2019). The majority of the data stolen consisted of credit card application data from the period of 2005 - 2019. This includes personal information such as names, home addresses, phone numbers, reported incomes, email addresses, and postal codes. Beyond credit card application data, leaked information also consisted of:

- ❏ Personal information of customers holding a credit card such as credit scores, credit limits, payment history, and balances from the period of 2005-2019.
- ❏ Approximately 140,000 Social Security numbers of customers originating in the United States.
- ❏ Approximately 1 million Social security Numbers of individual customers in Canada.
- ❏ Approximately 80,000 bank account numbers of customers holding a credit card.
- ❏ Certain portions of transaction information totalling a duration of approximately 23 days from 2016-2018.

3.2 Costs related to data breach and loss of reputation

Capital One reported that costs associated with the data breach would reach approximately $100 million - $150 million in the period of 2019. “Expected costs are largely driven by customer notifications, credit monitoring, technology costs, and legal support (Information on the Capital One Cyber Incident, 2019). Capital One does possess insurance to cover cyber security events and it is expected to cover a portion of these costs. Their stock also went into decline for a period of time which resulted in additional losses. In 2020, the organisation was also ordered to pay $80 million as civil penalty. Finally, the data breach, subsequent investigations, and civil penalties caused a significant negative impact on the reputation of the organisation.

4. Capital One response to cyber attack

The organisation had to undertake various measures when notified about the breach. Firstly, it immediately patched the vulnerability to prevent further unauthorized access using the same attack vector.

Apart from its own investigation, it also notified law enforcement and the public within 10 days of becoming aware of the breach. A number of measures were taken to mitigate risks associated with its customers. Individuals affected would be notified and free identity protection and credit monitoring was also to be provided. Customers were also made aware of the possibility of receiving phishing emails and calls due to their personal information being compromised. Customers were also notified to enrol for text/email alerts to keep track of activity. Furthermore, an email address was provided to affected customers to report suspicious activity. Affected customers were also notified not to share their Social Security Number/account/card information over email or via phone as the organisation would never explicitly request it.

5. Analysing the data breach

5.1. What Capital One did right?

Although a huge trove of personal information was stolen, the majority of sensitive data such as Social Security Numbers were tokenized and hence inaccessible to the cyber attacker (Stupp and Rundle, 2019). Tokenized data can only be unlocked via a separate system.

The organisation also had a disclosure and incident response program in place and this resulted in its quick pace with which it conducted its investigation, notified law enforcement, and subsequently the public. Since receiving a tip about the possibility of a data breach, the investigation, public announcement, and arrest of the cyber attacker by law enforcement took place within a span of 10 days.

5.2. Where did Capital One go wrong?

Capital One admitted that unauthorized access to its company data stored on the cloud was made possible due to misconfiguration of their web applications firewall. Upon investigation, it was revealed that this vulnerability existed approximately from the period of March 22, 2019 - July 19, 2019. Hence, there was also a failure to detect this vulnerability for a minimum period of four months.

The cyber attacker used the Anonymous Tor Network to carry out the intrusion. It is a common platform used by cyber attackers to conduct their operations. Thus, Capital One’s platform should have been configured to prevent Tor network sessions from connecting to their platform. We can now start to get a view that issues existed in inadequate risk assessment of their platform and vulnerability detection.

6.0. Cyber security roadmap

A plan is now proposed entailing how such a cyber security incident can be prevented in the future if specific controls noted in the NIST Cyber Security Framework are implemented. The framework core consists of five main functions: Identify, Protect, Detect, Respond, Recover. The proposed controls are mapped to these functions in order to create our cyber security roadmap. The table below demonstrates the core component of the framework:

COMPONENT	RECOMMENDED CONTROL	HOW CONTROL COULD HAVE PREVENTED DATA BREACH
IDENTIFY	**ID.AM-4 :** External information systems are catalogued.	The framework consists of controls that focus on documenting both internal and external systems and flow of its data. As the threat originated from an outside source, we only need to select controls from the framework which focus on external systems for our roadmap.
PROTECT	**PR.PT-1:** Audit/log records are determined, documented, implemented and reviewed in accordance with policy.	The data breach was not discovered by the organisation. It was only discovered after a tipster alerted the organisation. This shows that insufficient or inefficient auditing occurred due to which the intrusion was not detected. The mentioned control would mitigate this risk.
	PR.AC.1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.	The data intrusion originated from an external source. Only authorized users from authorized devices should be permitted to gain access to their cloud storage.
	PR.AC-3: Remote access is managed.	Remote access was used to transfer data away from the organisation's cloud storage. This control would mitigate that risk.
	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	In this particular event, the attacker was able to gain access to an administrator account which allowed direct access and transfer of data. Setting up accounts with least required functionalities/access could have minimized the data/functionalities that could have been

		accessed.
	PR.DS-5: Protections against data leaks are implemented.	During the data breach, the cyber attacker was successfully able to transfer data from the organisation’s cloud storage. Hence, the following control is proposed in order to gain protection against data leaks.
	PR.IP-12: A vulnerability management plan is developed and implemented.	Capital One determined that a breach had occurred 4 months after the attack had occurred. Furthermore, it was only discovered after receiving a tip. This shows that Capital one needs to develop and implement a more efficient vulnerability management plan than the one they currently possess.
DETECT	**DE.CM-1:** The network is monitored to detect potential cyber security events.	A plan should be prepared where the network is continuously monitored for suspicious activities.
	DE.DP-5 : Detection processes are continuously improved	Continuous steps must be undertaken to improve detection processes in order to keep up with rapid advancement in technologies. Clearly, a failure in detection allowed the cyber attack to be carried out over a period of time in this event.
	DE.CM-6: External service provider activity is monitored to detect potential cyber security events.	Sufficient monitoring of activities carried out by external service providers would have enabled Capital One to detect this particular intrusion while it may have been occurring.
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	Even though the cyber attacker used an administrator account to access data, the device used originated from an external source. Remote access was also used to transfer data for personal use. Furthermore, a scanning software was also used to detect the misconfigured web applications firewall of Capital One. Monitoring software and connections from devices would mitigate this risk in the future.
	DE.CM-8: Vulnerability	Steps should be undertaken to detect

	scans are performed.	vulnerabilities earlier. In the case of this event, the intrusion was detected approximately 4 months after it occurred. Performing more routine and efficient vulnerability scans would detect such a vulnerability / intrusion earlier.
RESPOND	N/A	Capital One reported that they already had a breach disclosure and incident response management plan in place during the time of the incident (Information on the Capital One Cyber Incident, 2019). We have already analyzed that this particular cybersecurity event was made possible due to failures in detection and monitoring. Hence, no controls in this tier are recommended.
RECOVER	N/A	Vulnerability was immediately fixed. Hence, the recovery plan was executed successfully. Public and law enforcement were immediately notified. Recovery activities were also notified to customers. This shows that the organisation communicated well with external shareholders and law enforcement. Hence, no further controls in this tier are recommended.

7.0. Conclusion

An analysis of the Capital One data breach displayed that while the organisation responded and recovered quickly and efficiently from the incident, insufficient security controls existed which enabled the cyber attack to take place. This shows that large organisations such as Capital One who have invested significantly in technology still face the threat of cyber attacks. The study also demonstrates the significant impact data breaches can have on an organisation in terms of reputation, recovery costs, and penalties. Finally, the cyber security roadmap proposed in this report also demonstrated that complying with the NIST Cyber Security Framework could have prevented this data breach from taking place.

References

Federal Trade Commission. 2021. *Understanding the NIST cybersecurity framework*. [online] Available at: <https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/nist-framework> [Accessed 4 April 2021].

Kirk, J., 2019. *Woman Arrested in Massive Capital One Data Breach*. [online] Databreachtoday.com. Available at: <https://www.databreachtoday.com/woman-arrested-in-massive-capital-one-data-breach-a-12852?highlight=true> [Accessed 4 April 2021].

United States Department of Justice. 2020. *United States v. Paige Thompson*. [online] Available at: <https://www.justice.gov/usao-wdwa/united-states-v-paige-thompson> [Accessed 4 April 2021].

McLean, R., 2019. *A hacker gained access to 100 million Capital One credit card applications and accounts*. [online] CNN. Available at: <https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html> [Accessed 4 April 2021].

Kirk, J., 2019. *Capital One: Where Did the Bank Fail on Defense?*. [online] Data Breach Today. Available at: <https://www.databreachtoday.com/capital-one-where-did-bank-fail-on-defense-a-12858?highlight=true> [Accessed 4 April 2021].

Flitter, E. and Weise, K., 2019. *Capital One Data Breach Compromises Data of Over 100 Million (Published 2019)*. [online] The New York TImes. Available at: <https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html> [Accessed 4 April 2021].

Capital One, 2019. *Capital One Announces Data Security Incident*. [online] Available at: <https://www.capitalone.com/about/newsroom/capital-one-announces-data-security-incident/> [Accessed 4 April 2021].

Capital One. 2019. *Information on the Capital One Cyber Incident*. [online] Available at: <https://www.capitalone.com/digital/facts2019/> [Accessed 4 April 2021].

Stupp, C. and Rundle, J., 2019. *Capital One Breach Highlights Shortfalls of Encryption*. [online] Wall Street Journal. Available at: <https://www.wsj.com/articles/capital-one-breach-highlights-shortfalls-of-encryption-11564738200> [Accessed 4 April 2021].