



CS5071NI - Professional and Ethical Issues

100% Individual Coursework

2024-25 Spring

Credit: 15 Semester Long Module

Student Name: Navraj Rajak

London Met ID: 23047346

College ID: NP01NT4A230040

Assignment Due Date: Monday, May 19, 2025

Assignment Submission Date: Sunday, May 18, 2025

Word Count: 3275

Submitted to: Aadesh Tandukar

I confirm that I understand my coursework needs to be submitted online via MySecondTeacher under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a marks of zero will be awarded.

Similarity Check Report

23047346 Navraj Rajak.docx

 Islington College, Nepal

Document Details

Submission ID

trn:oid::3618:96508941

Submission Date

May 18, 2025, 6:25 PM GMT+5:45

Download Date

May 18, 2025, 6:26 PM GMT+5:45

File Name

23047346 Navraj Rajak.docx

File Size

22.5 KB

19 Pages

3,275 Words

19,593 Characters



Page 1 of 23 - Cover Page

Submission ID trn:oid::3618:96508941







Page 2 of 23 - Integrity Overview

Submission ID trn:oid::3618:96508941




11% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

-  **25 Not Cited or Quoted 8%**
Matches with neither in-text citation nor quotation marks
-  **14 Missing Quotations 3%**
Matches that are still very similar to source material
-  **0 Missing Citation 0%**
Matches that have quotation marks, but no in-text citation
-  **0 Cited and Quoted 0%**
Matches with in-text citation present, but no quotation marks

Top Sources

- 5%  Internet sources
- 0%  Publications
- 9%  Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Abstract

Capital One Breach 2019 is one of the significant cybersecurity failures in the financial institution. It exposed the information of over hundreds of millions of customers. The attack was caused by a misconfiguration of web application firewall in its Amazon Web Services (AWS) environment. This case study examines the technical, social, ethical, legal, and professional dimensions of the breach.

The case reveals inappropriate implementation of least privilege access, monitoring, and breach disclosure. The incident highlights the direct violation of data protection laws and non-compliance to cybersecurity best practices along with industry standards, that led to regulatory fines and settlements.

It demonstrates the importance proper implementation of cloud security measures and management. The institutions should perform system configuration securely, perform regular monitoring for identifying any anomalies behavior in the system conduct periodic vulnerability assessment and penetration testing. The organizations must adhere to cyber security best policies and practices, NIST Cybersecurity Framework, ISO 27001, data protection laws and maintaining accountability.

Table of Contents

Abstract	iii
Part 1: Introduction and Background.....	1
1.1. Introduction.....	1
1.1.1. Introduction to the Company	1
1.1.2. Introduction to Cyber Threats and Risks	1
1.2. Background of the Scandal	3
1.2.1. Overview.....	3
1.2.2. Past Similar Breaches	3
1.2.3. Technical Details.....	4
1.2.4. Timeline	6
1.2.5. Intention	6
1.2.6. Impacts.....	7
Part 2: Social Issues	8
2.1. Background.....	8
2.2. Identified Issues	8
Part 3: Ethical Issues.....	10
3.1. Background.....	10
3.2. Identified Issues	10
3.3. Comparison with Ethical Theories.....	11
Part 4: Legal Issues	12
4.1. Background.....	12
4.2. Identified Issues	12
Part 5: Professional Issues	14
5.1. Background.....	14

5.2. Identified Issues	14
Part 6: Conclusion and Reflection	16
6.1. Conclusion	16
6.2. Personal Reflection	16
6.2.1. Identifying Stakeholders	16
6.2.2. Analysis Phase	16
6.2.3. Decision	17
6.2.4. Recommendation	17
Part 7: References	18

Table of Tables

Table 1: Past Similar Breaches	4
Table 2: Comparison with Ethical Theories.....	11

Table of Figures

Figure 1: Timeline of the attack	6
--	---

Part 1: Introduction and Background

1.1. Introduction

1.1.1. Introduction to the Company

Capital One Corporation was established in 1994 as a financial institution. Capital One ranks as one of the top US financial institutions which operates its credit card division alongside consumer banking and commercial lending operations. It maintains \$478 billion in assets while employing approximately 52,000 personnel who serve over 100 million customers. This institution holds a spot among the first ten banks in the United States. As a part of their business expansion, Capital One made a major step by announcement of a \$35.3 billion acquisition of Discover Financial Services (Capital One Corporation, 2025). All of Capital One's data processing and storage utilizes **AWS (Amazon Web Service)** as its primary cloud infrastructure base.

1.1.2. Introduction to Cyber Threats and Risks

Cyber threats refer to the potential attacks in order to damage, steal, or disrupt information system. These can be carried out by threat actors with malicious intent such as hackers, criminal organizations, insider, or even state-sponsored (Canadian Centre for Cyber Security, 2022). These can be aimed at individuals, organization or nations.

Cyber risks refer to the potential losses that results from cyber threats. The risk represents the impact of a successful cyber-attack on an organization or individual. The potential damage that could be caused by a successful cyberattack can be categorized as financial losses, reputation damage, operation disruption or legal and regulatory issues (The Institute of Risk Management (IRM), 2014).

There are different sophisticated techniques and mechanisms being employed to find and exploit vulnerabilities in systems, processes, or human behavior. One must be well-aware on different types of breaches for implementing effective cyber security measures.

1.1.2.1. Types of Cyber Breaches

- i. **Data Breaches:** It refers to the state when sensitive, confidential or protected information is accessed, stolen or exposed without authorization.
- ii. **Ransomware attacks:** It is a type of attack where a malware encrypts files or locks the user out of their system until a ransom is paid.
- iii. **Phishing Attacks:** It involves tricking humans into revealing sensitive information such as login credentials or financial details, by posing as an official entity.
- iv. **Denial of Service Attacks:** It involves overwhelming a system with traffic more than that system can handle, making it unavailable to legitimate users.
- v. **Insider Threats:** It refers to the malicious or negligent actions by employees, contractors or other trusted individual within an organization.
- vi. **Zero-day exploits:** It is the attack on an unknown vulnerability in software or hardware that has not been patched.
- vii. **Supply Chain Attacks:** It refers to targeting third-party vendors to gain unauthorized access to organization internal network.
- viii. **Credential Stuffing:** It involves using stolen login credentials from one breach to attempt access to other accounts.
- ix. **Social Engineering:** It is the technique employed to manipulate humans into revealing their confidential information or performing action that may lead to security breach.

1.2. Background of the Scandal

1.2.1. Overview

The misconfiguration of web-application firewall integrated with its cloud technology, introduced vulnerabilities that lead to a major data breach in 2019 known as **Capital One breach**. This breach compromised the personal information of over 106 million consumers. Paige Thompson, a former software engineer at AWS, exploited this vulnerability and accessed sensitive client information, that includes Social Security numbers, bank account details, and other personal data (CERT-EU, 2019).

The attacker employed command injection technique to access the cloud storage where customer credit applications, Social Security numbers, and bank account details were stored. The breach took place in March 2019 but publicized on July 2019. The corporation faced \$190 million in customer settlements and an \$80 million in regulatory fine (Office of the Comptroller of the Currency, 2020).

The legal officials linked the breach to her online alias “**erratic**”, through her chat logs and social media post. Authorities executed a search at her residence, found evidence linking her to the crime and arrested her. (Federal Bureau of Investigation, 2019)

1.2.2. Past Similar Breaches

Several financial institutions and tech companies have faced similar data breaches in the past. Most of them are because of misconfiguration, insider threats, and poor security practices.

Company	Year	Records Exposed	Cause
Yahoo	2013 - 2014	3 billion accounts	Stolen credentials

JPMorgan Chase (Bank)	2014	76 million households	Unauthorized access to servers
Equifax (Credit Bureau)	2017	147 million records	Unpatched vulnerability
Marriott Hotels	2018	500 million guest records	Unauthorized access to the database
Facebook	2019	540 million records	Misconfigured cloud storage
Capital One Bank	2019	106 million customer records	Misconfigured cloud firewall (WAF)

Table 1: Past Similar Breaches

These reveal some of the most common cybersecurity mistakes that includes poor vulnerability management, lack of monitoring, and misconfigured systems.

1.2.3. Technical Details

Its infrastructure was primarily hosted on Amazon Web Services (AWS), which included the use of the Amazon EC2 (Elastic Computer Cloud) for virtual servers and Amazon S3 (Simple Storage Service) for data storage. The company also used Amazon WAF (Web Application Firewall) to protect its web applications from malicious traffic.

- i. **Exploitation of Server-Side Request Forgery (SSRF) Vulnerability:** The Capital One's web application contained a SSRF vulnerability that the attacker used for exploitation (Martini, 2019). The application server transmitted unauthorized commands to internal resources because of this malfunction. The attacker gained unauthorized access to the AWS EC2 instance metadata service through this opportunity to obtain security credentials.

- ii. **Unauthorized Access to AWS EC2 Instance Metadata:** The SSRF attack enabled the attacker to execute requests against the AWS EC2 metadata service located at <https://169.254.169.254/latest/meta-data/> (Martini, 2019). The instance metadata service revealed details which including IAM role credentials to the attacker. The attacker retrieved the temporary credentials which led to an IAM role granting access to system operations within the AWS environment.
- iii. **Misconfigured IAM Roles:** An IAM role controlling the compromised EC2 instance owned permission to query S3 buckets containing sensitive data for listing and accessing their contents (Martini, 2019). Such configuration failure led to a violation of the principle of least privilege which delivered unauthorized users access to sensitive information.
- iv. **Data Exfiltration Process:** The attacker performed a list operation and data download of S3 buckets using the stolen IAM credentials (Martini, 2019). The exposed information consisted of Social Security numbers, bank account details and others. The data was then exfiltrated and, in some instances, posted on public platforms.
- v. **Detection and Response:** In July 2019, the breach was publicly announced when an external cybersecurity researcher altered Capital One after finding exposed data on GitHub. The legal officials linked the breach to attacker's online alias "**erratic**", through the chat logs and social media post. Authorities executed a search at her residence, found evidence linking her to the crime and arrested her (Martini, 2019). Under Computer Wire Fraud Act, the attacker was sentenced to five years in prison.

1.2.4. Timeline

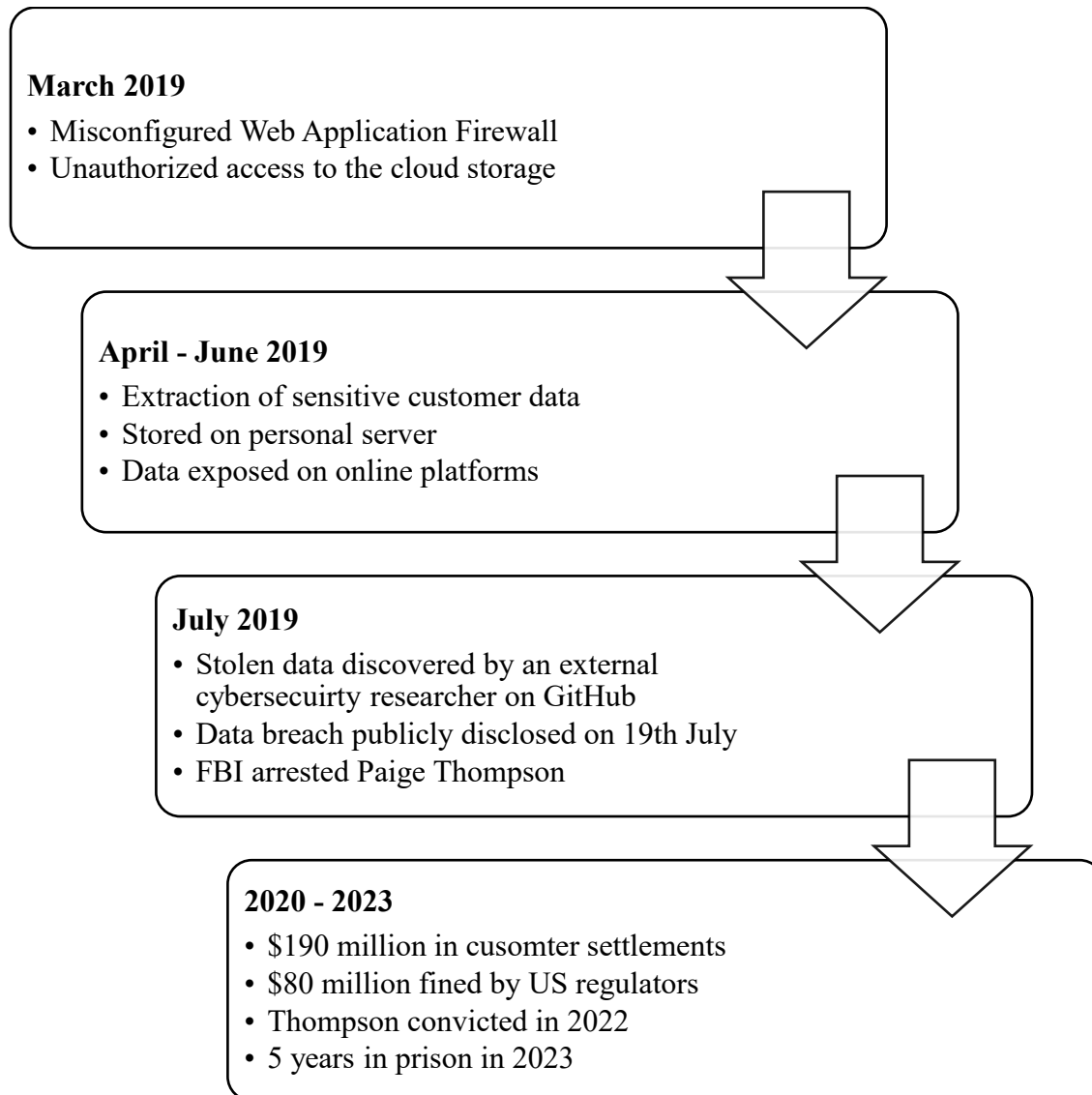


Figure 1: Timeline of the attack

1.2.5. Intention

The breach was motivated by the submission to recognition. Unlike most cyberattacks, it was not for financial gain. Thompson did not attempt to sell any of the data. She was interested to prove her hacking skills and gaining recognition in online hacker communities. She openly bragged about her accomplishment on Github and social media

platform. She was also a former employee at AWS, possibly disgruntled, exposing flaws in AWS security.

1.2.6. Impacts

The corporation had to face serious consequences, both financially and reputationally due to the data breach. The corporation had to pay **\$190 million** in legal customer settlement and **\$80 million** fine imposed by U.S. regulators for failure to protect customer data (Avery, 2022). It lost customers trusts as they feared identity theft. The corporation's stock price experienced a significant drop. Before the public disclosure (**July 26, 2019**), the stock price was **\$95.58** per share. After the public disclosure, the stock price dropped by **6%**, closing at **\$89.50** per share.

Part 2: Social Issues

2.1. Background

Cybersecurity incidents such as the capital one affects the company in every aspect. It affects the companies financially as well as leads to dealing with many social consequences. The exposures of any sort of personal data leads to distrusting, so be it a text message or their social security numbers, bank information or else. undermines trust in digital systems, disproportionately harms vulnerable groups, and reshape industry practices. It creates feeling of fear and stress among those whose data is exposed, mostly the vulnerable group – unable to defend themselves in time of legal matters. The breach left its impact 106 million people, making it one of the significant cases. This has also led to concern about the relationship between technology and societal well-being.

2.2. Identified Issues

- i **Loss of Public Trust:** The failure of Capital One as a major finance firm to safeguard customer information dissolves public trust both towards the institution and digital system everywhere. This led to people start doubting security practices and mechanisms as well as financial entities capability to handle sensitive information securely.
- ii **Increased risk of Identity Theft:** The breach exposed names, addresses, birthdates, credit scores, social security numbers along with other information. This kind of data allows malicious actors to commit identity fraud or open unauthorized accounts, potentially damaging victims credit and personal lives for years to come (Federal Trade Commission, 2020).
- iii **Psychological Impact on Victims:** The victims endure both emotional distresses coupled with fear of monetary loss as well as worry regarding data exploitation. Statistical studies demonstrate that people who experience data breaches tend to face lasting emotional difficulties when their identity leads to fraudulent behavior (European Union Agency for Cybersecurity, 2021).
- iv **Disproportionate Impact on Vulnerable Populations:** Certain groups, such as low-income individuals, immigrants, or the elderly, are often less equipped to deal with the consequences of identity theft, making them more vulnerable to financial and

emotional exploitation (Organisation for Economic Co-operation and Development, 2022).

- v **Ethical Concerns:** The breach revealed a misconfigured Web Application Firewall in Capital One's AWS-hosted environment. This raises ethical questions about the **oversight and shared responsibility model** of cloud providers and clients. Companies may adopt advanced tech for cost-efficiency without fully understanding or mitigating associated risks (Office of the Comptroller of the Currency, 2020).

Part 3: Ethical Issues

3.1. Background

In 2019, Capital One suffered a data breach which raised multiple major ethical concerns exceeding typical technical flaws. One of the major ethical concerns in cyber security involves the responsibilities of data protection as well as action taken by employees and the roles of organization in protecting user data. Companies that handle abundance of user private data must protect this information both legally and morally since improper management can result in severe consequences. Decisions implemented by individuals together with the corporation breached fundamental ethical requirements during this particular event.

3.2. Identified Issues

- i **Negligence In Data Protection:** Despite holding the resources needed for data protection, Capital One neglected to secure its sensitive client information (Office of the Comptroller of the Currency, 2020). A misconfiguration of firewall equipment serves not just as a single mistake but demonstrates complete indifference toward protecting customer trust. The violation of **deontological ethical principles** becomes apparent because neglect demonstrates a refusal to protect rights belonging to others specifically data and privacy rights.
- ii **Unethical Delay in Disclosure:** Capital One was unaware about the data breach for four months, before publicly announcing in July 2019. The customers could not take measures for their protection because of the prolonged period of non-disclosure (Federal Trade Commission, 2019). According to **utilitarian ethics**, the time-delayed notification failed to produce positive outcomes for the stakeholders involved. The late disclosure runs counter to two fundamental elements of social corporate responsibility which consist of honest and transparency.
- iii **Abuse of Privileged Access:** Paige Thompson worked at AWS as a software engineer. Through her experience, she managed to take advantage of Capital One's cloud system architecture. Insider knowledge about AWS architecture provided her with malicious information which she exploited from her position as an insider (Federal Bureau of Investigation, 2019). This action stands in violation of two fundamental ethical principles

of **virtue ethics** since it breaks both personal integrity principles and tech field professional standard.

- iv **Uniformed Data Collection:** The data breach made most individuals lose track of their data ownership status with Capital One since many were unaware the company continued to hold their information regardless of actual customer status. Data retention ambiguities create problems with obtaining valid consent from individuals (GAO-19-196, 2019). This act violates **positive-rights-based** ethics because people need to have knowledge and authority regarding data usage.
- v **Minimal Ethical Oversight in Cloud Migration:** The migration to cloud infrastructure place rapid implementation above ethical concerns as well as security considerations. A process to evaluate ethical risks should have been included as part of the project planning stage. Under **social contract theory**, corporations must discharge their responsibilities to their society members instead of choosing profit or convenience as priorities,

3.3. Comparison with Ethical Theories

Ethical Issue	Ethical Theory	Explanation
Failure in data protection	Deontology	Violated moral duty to safeguard users' private data
Misuse of insider knowledge	Virtue Ethics	Displayed poor moral character and lack of professional ethics
Delay in disclosure	Utilitarianism	Allowed harm to escalate rather than minimizing negative consequences
Lack of transparency on data retention	Rights-Based Ethics	Undermined individual rights to privacy and informed consent
Unethical cloud adoption without safeguards	Social Contract Theory	Failed to act in the public's best interest when adopting risky technologies

Table 2: Comparison with Ethical Theories

Part 4: Legal Issues

4.1. Background

The Capital One data breach, publicly disclosed in July 2019, exposed sensitive personal information of over 106 million individuals across the U.S. and Canada. The incident resulted in severe legal ramifications for both the company and the perpetrator, Paige Thompson, highlighting major compliance and regulatory failures under U.S. laws concerning data protection.

4.2. Identified Issues

- i **Violation of the Computer Fraud and Abuse Act (CFAA):** The CFAA is a US federal law enacted in 1986 to combat cybercrime. It has criminalized unauthorized access to computers and networks, involving personal, government, financial or protected system (U.S. Department of Justice, 2011). Paige Thompson was charged under the CFAA - 18 U.S. Code § 1030 for unauthorized access to Capital One's system (Martini, 2019).
- ii **Penalization by the Office of the Comptroller of the Currency (OCC):** OCC is a US federal agency that regulates and supervises national banks and federal savings institutions. Its role is to ensure the financial institution operate safely and comply with the banking law, and issue fines to those in case of violation. It penalized Capital One amounting \$80 million for failure to establish effective risk assessment process (Office of the Comptroller of the Currency, 2020).
- iii **Class-Action Settlement:** U.S. District Court for the Eastern District of Virginia approved Capital One's \$190 million settlement for violating state level data protection laws (United States District Court for the Eastern District of Virginia, 2022). This compensated to those affected by the breach, individuals for documented losses, credit monitoring, and identity restoration services.
- iv **Non-compliance with Gramm-Leach-Bliley Act (GLBA):** GLBA is a U.S. federal law enacted in 1999 A.D. It mandates financial institutions to protect customers' non-public personal information (NPI) and requires them to share information sharing practices with the customers (Senate and House of Representatives of the United States of America, 1999). The non-compliance with GLBA included lack of risk assessment, access control measures, failure to protect the customer NPI. This led to a fine of \$80 million.

- v **Senate Inquiry into Capital One's Data Breach Response:** The U.S. Senate Committee questioned the institution's transparency and consumer protections after the breach had occurred. The committee expressed concerns over the company failure to establish a dedicated hotline and clear process for consumers to request free credit monitoring (Brown, et al., 2019). The raised questions of additional customers affected beyond disclosed, requested details on when the breach notification letter was sent to the affected customers.

Part 5: Professional Issues

5.1. Background

The Capital One Breach 2019 revealed a systemic professional failure across IT security teams and cloud management. The incident was caused mainly because of a single misconfigured firewall in their AWS system. This allowed persistent undetected unauthorized access for 4 months. These lapses violate multiple professional codes of conduct.

5.2. Identified Issues

- i. **Cloud Misconfiguration:** Capital One failed to properly secure its cloud infrastructure, especially the Web Application Firewall (WAF), that led to exploitation (Martini, 2019). Professionals managing this system failed to follow the best practices and apply thorough configuration checks and testing. This violated **ACM Code 2.9**, which requires building and configuring systems to protect privacy. Proper configuration as per **NIST SP 800-53** could have prevented this.
- ii. **Inadequate IAM Policy Enforcement:** The AWS Identity and Access Management policies were improperly configured (CERT-EU, 2019). These provided a pathway for privileged escalation. The system administrators are expected to enforce the principle of least privilege; however, they failed to comply with this principle. This contradicted **NIST SP 800-171** and **ACM Code 1.6**, which tells to focus on privacy and responsible handling of data.
- iii. **Failure in Security Monitoring and Incident Response:** The breach went undetected for 4 months (Martini, 2019). This reveals poor security monitoring practices. As per **ACM Code 2.5** and **IEEE §6.7**, professionals must ensure that all the required systems are monitored and resilient. Appropriate monitoring methods as outlined in **NIST CSF** could have evaded this breach.
- iv. **Lack of Compliance with Industry Standards:** As a financial institution, Capital One was supposed to be fully compliant with industry standards, however was found non-compliant with standards like **PCI DSS** and **NIST CSF**. The breach indicated weak compliance implementation, a critical professional lapse in regulated industries (Office of the Comptroller of the Currency, 2020).

- v. **Insider Threat Failures:** The breach revealed professional negligence in insider threat management. Thompson's exploitation of her AWS knowledge violated **IEEE §7.1** confidentiality rules, while Capital One's failure to revoke access or monitor privileged users showed non-compliance with **NIST SP 800-171** and **ACM Code 1.7**. Proper access controls and behavioral monitoring could have prevented this.

Part 6: Conclusion and Reflection

6.1. Conclusion

The Capital One breach 2019 was one of a major cybersecurity failure at corporate level. It was caused by a misconfigured web application firewall and weak IAM policies. This allowed the attacker to steal data of over 106 million users. The breach exposed flaws in cloud security infrastructure and management, that includes poor access controls and delayed incident response time. The attack led to a total amount of \$270 million in fines and lawsuits, and caused severed reputation damage. The attack proves that even a large corporation can experience security breach due to simple misconfiguration and mismanagement of the security practices and policies.

6.2. Personal Reflection

The breach emphasizes the need for integrating ethical decision-making into organization's cybersecurity practices. An evaluation of the breach was conducted using a structured ethical decision-making methodology as mentioned below.

6.2.1. Identifying Stakeholders

The key stakeholders involved included the customers, Capital One itself, regulatory bodies, clouds service provider (Amazon Web Services) and cybersecurity professionals. Each of the stakeholders was impacted, identity theft risk for individuals, reputational and financial damage to the company and cybersecurity professional negligence to adhere with professional standards and best practices.

6.2.2. Analysis Phase

This phase revealed failures of governance, transparency as well as non-compliance with professional standards such as BCM, ACM, and NIST. Issues such as misconfigured firewalls, IAM policies, and delayed breach discourse shows a lack of non-adherence to industry best practices and questions their accountability.

6.2.3. Decision

From an ethical standpoint, decisions regarding cloud migration, access control, and breach discourse were misaligned with principles of public interest, integrity and responsibility outlined in professional codes of conduct.

6.2.4. Recommendation

In order to prevent such breaches in future, companies should firmly integrate ethical frameworks into their cybersecurity strategies. This includes periodic vulnerability and risk assessment, least privilege access, and real-time monitoring and intrusion detection. The breach also depicts the importance of proper system configuration, maintaining transparency in breach disclosure. The company should also adopt methodologies like ACM Code of Ethics Decision Making Framework to confine professionals making responsible adequate decisions within a certain boundary.

Part 7: References

Avery, D., 2022. *CNET*. [Online]

Available at: <https://www.cnet.com/personal-finance/capital-one-190-million-data-breach-settlement-today-is-deadline-to-file-claim/>

[Accessed 7 4 2025].

Brown, S. et al., 2019. *United States Senate Committee on Banking, Housing and Urban Affairs*. Washington, DC: United States Senate Committee on Banking, Housing and Urban Affairs.

Canadian Centre for Cyber Security, 2022. *An Introduction to the Cyber Threat Environment*. Ottawa: Canadian Centre for Cyber Security.

Capital One Corporation, 2025. *Capital One Corporation*. [Online]
Available at: <https://investor.capitalone.com/news-releases/news-release-details/capital-one-and-discover-stockholders-approve-capital-ones>

[Accessed 7 4 2025].

CERT-EU, 2019. *Massive breach at Capital One, purportedly due to a cloud misconfiguration*, s.l.: CERT-EU.

European Union Agency for Cybersecurity, 2021. *ENISA Threat Landscape 2021*, s.l.: European Union Agency for Cybersecurity.

Federal Bureau of Investigation, 2019. *Federal Bureau of Investigation (2019) Criminal Complaint: United States v. Paige A. Thompson*, s.l.: Federal Bureau of Investigation.

Federal Trade Commission, 2019. *Privacy & Data Security Update: 2019*, s.l.: Federal Trade Commission.

Federal Trade Commission, 2020. *Consumer Sentinel Network*, s.l.: Federal Trade Commission.

GAO-19-196, 2019. *Consumer Data Protection*, s.l.: United States Government Accountability Office.

Martini, J., 2019. *United States v. Paige Thompson*, Seattle: United States District Court for the Western District of Washington at Seattle.

Office of the Comptroller of the Currency, 2020. *In the Matter of Capital One*, Mclean: Office of the Comptroller of the Currency.

Office of the Comptroller of the Currency, 2020. *Office of the Comptroller of the Currency*, s.l.: Office of the Comptroller of the Currency.

Office of the Comptroller of the Currency, 2020. *Semiannual Risk Perspective*, s.l.: Office of the Comptroller of the Currency.

Organisation for Economic Co-operation and Development, 2022. *OECD Policy Framework on Digital Security*, s.l.: Organisation for Economic Co-operation and Development.

Senate and House of Representatives of the United States of America, 1999. *Public Law 106–102*, Washington, DC: Senate and House of Representatives of the United States of America.

The Institute of Risk Management (IRM), 2014. *Cyber Risk Resources for Practitioners*. s.l.:The Institute of Risk Management (IRM).

U.S. Department of Justice, 2011. *Computer Fraud & Abuse Act of 1986*, s.l.: U.S. Department of Justice.

United States District Court for the Eastern District of Virginia, 2022. *Capital One Consumer Data Security Breach Litigation, Case No. 1:19-md-02915 (E.D. Va.)*, Alexandria: United States District Court for the Eastern District of Virginia.