turnitin file.docx

Islington College,Nepal

Document Details

Submission ID
trn:oid:::3618:96611638

Submission Date
May 19, 2025, 9:51 AM GMT+5:45

Download Date
May 19, 2025, 9:53 AM GMT+5:45

File Name
turnitin file.docx

File Size
23.7 KB

16 Pages

3,490 Words

20,547 Characters

12% Overall Similarity

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

Match Groups

- **33** Not Cited or Quoted 9%
  Matches with neither in-text citation nor quotation marks
- **3** Missing Quotations 1%
  Matches that are still very similar to source material
- **6** Missing Citation 2%
  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

7% Internet sources
2% Publications
11% 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.

Match Groups

- **33** Not Cited or Quoted 9%
  Matches with neither in-text citation nor quotation marks
- **3** Missing Quotations 1%
  Matches that are still very similar to source material
- **6** Missing Citation 2%
  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

- 7% Internet sources
- 2% Publications
- 11% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	www.stateregstoday.com <1%
2	Submitted works	De Montfort University on 2025-01-17 <1%
3	Submitted works	Leicester College on 2024-09-25 <1%
4	Submitted works	Northcentral on 2025-03-24 <1%
5	Internet	files.eric.ed.gov <1%
6	Submitted works	California Southern University on 2024-09-29 <1%
7	Internet	www.wvih.com <1%
8	Submitted works	Hong Kong Baptist University on 2023-03-10 <1%
9	Submitted works	Colorado State University, Global Campus on 2024-05-20 <1%
10	Submitted works	American Public University System on 2023-10-19 <1%

11 Internet
hakia.com <1%

12 Submitted works
Singapore Institute of Technology on 2020-02-12 <1%

13 Internet
mortgageorb.com <1%

14 Submitted works
UC, Irvine on 2003-09-10 <1%

15 Internet
www.onlinescientificresearch.com <1%

16 Submitted works
Colorado Technical University Online on 2025-05-13 <1%

17 Internet
aithority.com <1%

18 Internet
dokumen.tips <1%

19 Internet
medium.com <1%

20 Internet
www.khlaw.be <1%

21 Submitted works
New Jersey Institute of Technology on 2025-05-15 <1%

22 Submitted works
SUNY, Binghamton on 2022-04-19 <1%

23 Submitted works
University of Maryland, Global Campus on 2025-03-17 <1%

24 Internet
www.coursehero.com <1%

25 Internet

www.infosecurity-magazine.com <1%

26 Submitted works

Purdue University on 2024-05-17 <1%

27 Submitted works

University of Arizona on 2015-12-06 <1%

28 Submitted works

University of Nottingham on 2012-11-22 <1%

29 Internet

slideplayer.com <1%

30 Submitted works

American Intercontinental University Online on 2010-09-27 <1%

31 Submitted works

Belhaven University on 2022-03-13 <1%

32 Submitted works

Nexford Learning Solutions on 2025-05-15 <1%

Introduction

1.1 Introduction of the Company

Figure 1: Introduction of Capital One

Capital One Financial Corporation is one of the most renowned financial institutions in the United States. It was found in 1994 and based in McLean, Virginia, the company has expanded to offer a variety of services, such as credit cards, banking products, auto loans, and savings accounts. Capital One operates in the U.S., Canada, and the U.K., providing services to millions of customers through both physical branches and digital platforms. As an innovative company, Capital One has adopted cloud computing to improve its efficiency, increase scalability, and provide more flexible services to its customers. By adopting cloud technologies, Capital One has become a leader in the financial sector's digital transformation. However, this move has also made the company more vulnerable to various cybersecurity challenges (companieshistory, 2024).

1.2 Introduction to Cyber Threat and Risks

Figure 2: Cyber Threats

As organizations depend more on digital systems, they are becoming more exposed to a range of cyber threats. One of the most common threats is a data breach, where sensitive information is accessed or exposed without permission. Other types of breaches include phishing, where attackers manipulate individuals into disclosing sensitive information; ransomware, which restricts access to data or systems until a

ransom is paid and malware, which refers to malicious software created to disrupt, damage, or gain unauthorized access to computer systems. Additionally, insider threats, where individuals within the organization exploit their access for malicious purposes, can be especially harmful. As businesses move to the cloud, misconfigurations in cloud settings have become a more frequent cause of data breaches. These misconfigurations create opportunities for cybercriminals to exploit weaknesses in cloud environments, making large amounts of data accessible on the public internet (executech, 2025).

2.Background

2.1 Overview of the Data Breach

Figure 3:Bar Graph: Number of Affected Users (U.S. vs. Canada)

In 2019, Capital One went through one of the biggest data breaches ever that exposed the personal information of over 100 million people in the U.S. and 6 million in Canada. The breach happened because a web application firewall in Capital One's cloud setup, hosted on AWS, was misconfigured. As a result, confidential customer data such as Social Security numbers, credit scores, and banking information was left vulnerable (Newman, 2019).

The types of personal information compromised during the breach included Social Security numbers, bank account information, names and contact details, birth dates and employment information, and credit card information.

Figure 4:Pie Chart – Types of data exposed

2.2 Timeline and Discovery

Interestingly, the breach wasn't noticed until several months after it began. While it began on March 22, 2019 it continued for several months without detection, Capital One was only alerted to the breach in July 19, 2019 after a security researcher noticed suspicious behaviour of Paige Thompson. By that time, Thompson had already downloaded vast amounts of sensitive information. The breach was publicly announced on July 29, 2019, and Thompson was arrested on the same day, marking the resolution of the issue (Wildman, 2022).

2.3 Cause and Methods

So, this breach happened due to the misconfiguration in Capital One's cloud-based infrastructure. The misconfigured Web Application Firewall (WAF), which was supposed to act as a barrier between Capital One's servers and potential attackers allowed unauthorized access to sensitive data stored within the company's AWS environment. Specifically, this misconfiguration enabled a Server-Side Request Forgery (SSRF) attack, which allowed the attacker to exploit the AWS metadata service and extract temporary IAM credentials.

Figure 5: SSRF

While AWS provided the cloud platform, it was Capital One's responsibility to ensure the proper setup and security protocols. Unfortunately, this misconfiguration was overlooked, leading to Thompson's exploitation of the flaw (Kabanov, 2022).

2.4 Similar Data Breaches

The Capital One breach is not an isolated incident it's part of a larger trend of data breaches. For example, in 2017, Equifax went through a massive breach that affected nearly 147 million people, all due to a failure to patch a known vulnerability in their system. Similarly, in 2013, hackers exploited a security flaw in Target's systems, compromising the personal information of over 40 million customers. Both incidents, like the Capital One breach, were caused by security lapses that allowed hackers to access sensitive data. These cases emphasize a common theme despite advancements in technology, poor security practices continue to leave organizations vulnerable to cyberattacks (Fruhlinger, 2020).

2.5 Attacker's Motive

Paige Thompson who was responsible for the Capital One breach, did not seem to have a direct financial motive. With her background as a former AWS employee, she had the technical expertise to identify flaws in cloud infrastructure. Rather than applying her knowledge in legitimate ways, Thompson took advantage of a misconfigured firewall in Capital One's system to access and download sensitive data without authorization.

Her actions appeared to be motivated by curiosity and a desire for recognition within hacker communities, as she shared details of the breach with others. There are also reports suggesting she may have been frustrated with her previous employer, AWS, after being fired from the company. This personal frustration, combined with her insider knowledge, could have influenced her decision to exploit the vulnerability in Capital One's system (Swabey, 2022).

2.6 Consequences and Impact

Figure 6:Graph showing Capital One's stock price before and after

In addition to the damage to its reputation, Capital One was forced to pay $190 million settlement to compensate affected customers. Furthermore, the company was hit with an $80 million fine from U.S. regulators for failing to implement adequate security measures to protect consumer data. On top of this, the breach exposed vulnerabilities in cloud infrastructure, pushing companies worldwide to reassess their security protocols and take stronger measures to safeguard sensitive information. The breach also caused customers to lose trust in Capital One, as they realized the company had failed to protect their personal data (Hua, 2022).

3.Social Issues

The Capital One breach revealed important social issues affecting both individuals and communities. This breach highlights several key social issues about data security, online privacy, and the societal implications of digital technologies.

3.1 Loss of Personal Privacy

When privacy is violated, it affects people’s sense of safety, freedom, and control over their own lives. The breach exposed sensitive personal information including names, addresses, Social Security numbers, and financial data. This not only leads to personal harm but also disrupts societal norms around security, fairness, and equal access to technology (Huang, 2023).

Stakeholders Affected: Customers whose personal data was exposed and the General Public who may feel less secure about online privacy.

3.2 Economic Harm to Individuals

Many individuals faced financial loss, damaged credit scores, and stress from having to prove their identity or recover stolen money. For some this meant years of financial instability or costly legal battles. This turns into a social issue that goes beyond just digital safety as it affects people's ability to participate equally in the economy, deepens financial stress, and worsens inequality, especially for those already struggling (Al-Janabi, 2022).

Affected Stakeholders: Customers who experienced financial loss, credit damage, or emotional stress, especially those already facing economic difficulties.

3.3 Limited Legal recovery options

When justice is not accessible to everyone equally, it reveals deeper issues in how society ensures fairness and recovery for all its members. Even though millions were affected very few got justice or any form of compensation. Legal processes were slow, expensive and complicated, and ordinary people didn't have the resources or knowledge to file lawsuits. That left many victims helpless (Aijaz, 2025).

Affected Stakeholders: Customers who lacked the resources to seek legal help, and regulatory bodies responsible for ensuring fair access to justice.

3.4 Loss of Trust in Financial Institutions

Trust is essential for functioning societies, when it breaks people become disconnected, skeptical, and less willing to engage with essential services. After the breach people's trust in Capital One and similar institutions dropped which made them more cautious about sharing personal information and began to question the reliability of institutions that manage their money and data especially online (Dolan, 2019).

Affected Stakeholders: Customers who lost confidence in Capital One and similar

institutions, and the general public who became more cautious about trusting financial organizations.

3.5 Lack of Transparency from Companies

Although Capital One discovered the breach days before, they did not alert the public immediately after discovering the breach. It shows that companies prioritize reputation over responsibility which weakens the sense of fairness and responsibility that keeps society from running smoothly. When companies hide information, it takes away the public's ability to protect themselves and make informed decisions (Mehta, 2024).

Affected Stakeholders: Customers who were not informed in time to protect themselves, regulatory authorities responsible for oversight, and the general public who rely on transparency from companies.

4.Ethical Issues

The breach brings up several ethical concerns, these ethical questions don't just focus on the person who caused the breach they also look at the system failures that allowed it to happen.

4.1 Flawed setup for cloud-based data

Capital One used cloud systems to store customer's information, but the security in place wasn't strong enough to stop unauthorized access. Reason for breach was weak configurations and poor internal checks. This isn't just a technical mistake it's an ethical issue because people trusted the company to keep their information safe. When that trust is broken due to preventable flaws, it raises serious questions about responsibility, care, and the standards we expect from institutions handling private data (Purdue Global, 2024).

From a deontological perspective, Capital One's failure to secure their cloud setup properly is an ethical breach because the company had a clear duty to protect customer data, and neglecting that responsibility violates fundamental moral obligations.

Affected Stakeholders: Customers whose private information was stored in the cloud, and Capital One as the responsible data handler.

4.2 Failure to Provide Timely and Transparent CommunicationAfter discovering the breach, Capital One waited before informing the public. Choosing to delay the announcement to protect the company's image rather than the people affected raises ethical concerns. When a company holds back critical information, it breaks the trust people place in it and fails to act with transparency and accountability.

Deontology is about doing the right thing based on moral duties and obligations, regardless of the consequences. So, from a deontological point of view, the ethical failure happened the moment Capital One chose not to fulfill its responsibility to be transparent with the people it serves. Even if telling the truth could harm their reputation, that doesn't change the fact that withholding the information was wrong (Rueter, 2023).

Affected Stakeholders: Customers who were left unaware and vulnerable, and the general public who rely on honest communication from institutions.

4.3 Lack of Effective Monitoring SystemsCapital One failed to detect the breach for months, allowing the attacker to access and download sensitive data without being noticed. This delay happened because the internal monitoring systems weren't strong or responsive enough. A company that values integrity and accountability wouldn't just

install systems and forget them. It would continuously check, improve, and monitor it (Richards-Gustafson, 2017).

Virtue ethics focuses on the character and values of the people or organizations involved. In this case, Capital One's failure to detect the breach for months shows a lack of alertness, responsibility, and care. Letting weak systems run unchecked suggests a lack of moral commitment to doing what's right, not just what's required.

Affected Stakeholders: Customers whose data was exposed due to delayed detection, and Capital One's internal security teams responsible for system oversight.

4.4 Insufficient Customer Compensation

After the breach, many affected customers received little to no meaningful support or compensation. When people suffer due to a company's failure, the company has a responsibility to make things right. Failing to provide fair compensation isn't just a business issue it reflects how little value is placed on the people affected.

21 Utilitarian ethics is about creating the greatest good for the greatest number minimizing harm and maximizing well-being. When Capital One offered only limited compensation after the breach, many affected customers were left to deal with stress, fear, and potential financial loss on their own. From a utilitarian view, this response failed to reduce overall harm (peesbox, 2023).

Affected Stakeholders: Affected customers who experienced emotional distress, financial risk, and inadequate support after the breach.

4.5 Ignoring Red Flags or Warning Signals Before the breach, there were signs such as system misconfigurations or unusual activity that something wasn't right. But those red flags were either missed, downplayed, or ignored. This wasn't just a technical

oversight it reflected a deeper issue of not taking threats seriously. When warning signs are ignored, especially in a company trusted with sensitive information, it shows a failure in responsibility, risk awareness, and care (Kubade, 2024).This issue can be best understood through a virtue ethics perspective, ignoring clear warning signals shows a lack of care, responsibility, and common sense. A company that acts ethically would be active and alert, not careless or passive. Ethical behaviour involves being careful, thoughtful, and protective of others qualities that were clearly missing here. Affected Stakeholders: Customers whose data was compromised due to ignored warning signals, and Capital One's security teams who were responsible for identifying and addressing risks.

5. Legal issues

Companies are legally required to protect customer data using reasonable and industry-standard cybersecurity measures. In the Capital One data breach, legal ethics played a huge part in how the company handled things. The breach happened partly because of weak configurations and missing internal controls that should have been caught and fixed which violated the duty of care. (csoonline, 2023).

5.1 Negligence in Cybersecurity Practices:

Capital One's failed to maintain proper cybersecurity measures which violated laws like the Gramm-Leach-Bliley Act (GLBA), which requires financial institutions to protect customer data. This negligence allowed sensitive personal information to be exposed which left customers vulnerable to identity theft and fraud. It also raised issues under the FTC Act for unfair practices which led to regulatory penalties, including an $80

million fine by the OCC for poor risk management (secureworld, 2020).

5.2 Delayed Breach Notification

When Capital One discovered the breach in July 2019, they didn't immediately inform the public or affected customers. This delay in breach notification violates state data breach notification laws, which require companies to notify individuals without unreasonable delay after discovering a breach that compromises personal data. These laws are in place to allow people to take immediate actions, such as monitoring their accounts, to protect themselves. Capital One's delay in reporting also violated the Federal Trade Commission (FTC) Act, which requires businesses to operate honestly and transparently while safeguarding consumer rights (Gavejian, 2018).

5.3 Failure to Protect Personally Identifiable Information (PII)

Capital One's breach exposed sensitive personally identifiable information (PII), such as names, addresses, credit scores, and social security numbers. This failure to protect sensitive data violated laws like the Gramm-Leach-Bliley Act (GLBA), which requires financial institutions to protect customer information. Additionally, it also violated state data protection regulations, which require companies to take reasonable steps to protect PII. The violation not only exposed customers to identity theft and fraud risks but also resulted in regulatory scrutiny, leading to penalties and lawsuits (dataclassification.fortra, 2022).

5.4 Class Action Lawsuits from Affected Customers

Figure 7:Class Action Lawsuits

After the breach, Capital One faced class action lawsuits from affected customers who

claimed that their personal data had been mishandled. These lawsuits state that the company failed to take appropriate steps to protect sensitive information, that violates consumer protection laws. The Gramm-Leach-Bliley Act (GLBA), which requires the protection of customer financial data, is one of the key regulations mentioned. Additionally, state-level privacy laws that protect individuals' data rights were also likely violated. These lawsuits led to a $190 million class action settlement to compensate affected customers (Rivera, 2024).

5.5 Failure to Maintain Proper Internal Controls

Capital One failed to maintain proper internal controls which led to violations of corporate governance regulations, like the Sarbanes-Oxley Act (SOX). While SOX primarily focuses on financial reporting, it requires companies to set up and maintain internal controls to ensure the accuracy of their financial statements. These controls can extend to data protection as well, especially when financial data is involved, as it was in the Capital One breach. If internal controls are insufficient or fail to detect weaknesses in the system, companies may face legal consequences (Bowman, 2025).

6. Professional Issues

A profession is a job that requires special skills, knowledge, and ethical standards to responsibly support society while the professionals are skilled individuals who apply their expertise to carry out these responsibilities effectively. Professional ethics makes sure that individuals working in computing fields behave responsibly, protect user data, prioritize honesty, and minimize harm. Codes of conduct such as the ACM Code of Ethics, the Software Engineering (SE) Code of Ethics, and the British Computer Society (BCS) Code set specific professional standards. The Capital One breach

exposed clear professional failings.

6.1 Lack of Employee Training

Skilled and dedicated employees are essential for a successful company. If employees aren't trained to meet the standards, it can damage their professional reputation, as well as the reputation of the company they represent (skilldynamics, 2023).

Violation of Code of Conduct:

ACM Code 2.2: "Maintain professional competence."

SE Code Principle 3.08: "Ensure adequate training for those under your supervision."

Staff failed to catch a basic cloud misconfiguration, exposing sensitive data. This shows clear weaknesses in employee training.

6.2 Lack of Incident Response Plans

When the breach occurred, the company didn't act quickly enough to contain the damage, notify affected customers, or address the vulnerabilities that allowed the breach to happen in the first place.

Violation of Code of Conduct:

ACM Code 2.5: "Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks."

BCS Code 1(c): "Have regard for the legitimate rights of third parties."

By not having an IRP, Capital One failed to meet industry standards and best practices for cybersecurity, which is a core professional expectation, especially in sectors handling sensitive data (rsisecurity, 2019).

6.3 Poor Third-Party Vendor Management

Capital One trusted a vendor without ensuring strong security practices which lead to

the misconfiguration that exposed sensitive data.

Violation of Code of Conduct:

ACM Code 1.2: "Avoid harm to others."

SE Code Principle 3.10: "Ensure that clients are fully informed about system capabilities and limitations."

Professionals must manage risks not just within their company but also with partners. Capital One failed this duty.

6.4 Failure to Prioritize Cybersecurity Investments

Capital One relied on outdated systems, leaving it vulnerable to attacks. Proper investment in cybersecurity would have allowed for more frequent updates, better threat detection, and more effective defences against hacking attempts.

Violation of Code of Conduct:

ACM Code 2.7: "Improve public understanding of computing and its consequences."

SE Code Principle 3.11: "Ensure adequate testing, debugging, and review of software and related documents."

As a result, the company was unprepared for the breach, showing a lack of planning and responsibility when it came to securing customer data, which is a major professional failure (Shah, 2025).

6.5 Weak Compliance with Security Standards

Figure 8:Compliance with Security Standards

Capital One did not effectively apply international security standards like ISO/IEC 27001 or NIST, exposing gaps in their protection systems (Buker, 2023).

Violation of Code of Conduct:

29 ACM Code 1.3: "Be honest and trustworthy."

24 SE Code Principle 1.04: "Disclose any factors that might endanger the public or the environment."

Compliance with security guidelines is not optional it is an ethical requirement. Capital One's failures showed serious disregard for this principle.

7. Conclusion and personal reflection

9 7.1 Conclusion

The 2019 Capital One data breach showed how a single mistake in cloud security

8 settings can create large-scale problems exposing the personal data of more than 100 million users, caused serious legal, financial, and reputational consequences. This event highlighted the importance of being proactive in security efforts rather than reacting only after a breach occurs. Beyond technical gaps, the breach reflected failures in accountability, transparency, and risk management, pointing out that organizations must balance technology with ethical responsibility.

7.2 Personal Reflection and Recommendations

While preparing this report, it became clear that cybersecurity is not just about technology but also about making ethical choices. Keeping data safe means staying alert, being honest, and taking responsibility. According to the ACM Code of Ethics, computing professionals are expected to “avoid harm,” “respect privacy,” and “uphold the public good.” Applying the methodology for ethical decision-making specifically the

Brainstorming and Analysis Phase several recommendations can be made to prevent and address such incidents:

1.Brainstorming Phase:

- Outline important ethical responsibilities, such as (harappa, 2025):

Protecting personal information

Reporting data breaches truthfully

Accepting accountability for system failures

- Identify all affected stakeholders, including:

Customers

Employees

Shareholders

Regulatory bodies

2.Analysis Phase:

- Examine how the breach affected stakeholders, with attention to (qsstudy, 2025): • Loss of trust • Financial damage • Legal consequences

- Review which ethical duties were overlooked, including: • Lack of regular security audits • Poor oversight of systems • Slow response to the incident