LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

CS5071NI - Professional and Ethical Issues

100% Individual Coursework

2024-25 Spring

Credit: 15 Semester Long Module

Student Name: Shuva Shree Adhikari

London Met ID: 23049013

College ID: NP01CP4A230134

Assignment Due Date: Monday, May 19, 2025

Assignment Submission Date: Monday, May 19, 2025

Word Count: 3305

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.

23049013 Shuva Shree Adhikari CW Ethics.docx

Islington College,Nepal

Document Details

Submission ID
trn:oid:::3618:96635285

Submission Date
May 19, 2025, 12:21 PM GMT+5:45

Download Date
May 19, 2025, 12:22 PM GMT+5:45

File Name
23049013 Shuva Shree Adhikari CW Ethics.docx

File Size
20.0 KB

18 Pages

2,962 Words

17,059 Characters

23% Overall Similarity

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

Match Groups

37 Not Cited or Quoted 16%
Matches with neither in-text citation nor quotation marks

13 Missing Quotations 6%
Matches that are still very similar to source material

2 Missing Citation 1%
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

10% Internet sources
4% Publications
21% 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.

Table of Contents

1. Introduction and Background of the Scandal

1.1. Introduction

1.1.1. Introduction to the Company:

Capital one is a banking company that offers both commercial and retail banking services along with credit card products through its subsidiaries. The company's products and services cover children savings account, car loans, capital market solutions, refinancing services, commercial and small business lending, investment services, and credit and debit cards.(GlobalData, 2025)

1.1.2. Introduction to Cyber Threats and Risks:

Cyber threat is an attack to steal information or harm digital life in general. It also causes the possibility of a successful cyber-attack aimed at attaining unauthorised access, damage, disruption or theft of an information technology asset, computer system, intellectual property or other sensitive data. This threat could be from a known source within the organisation or by unidentified individuals from distant locations. Computer viruses, loss of data, Denial of Service (DoS) attacks, and other attack vectors are part of cyberattacks. (Tunggal, 2025)

1.1.3. Types of Cyber Breaches:

1.1.3.1. Data Breaches

1. Unauthorized Access:

   Ill invasion into computer systems, networks, or databases is breach. These breaches mostly involve hackers entering into the system to steal, alter or delete information. Not only an outside hacker's attack but also an employee having authorization to access files and information beyond his or her level of authorization are the causes of unauthorized access. (Bakharev, 2024)

2. Data Theft:

   Data Theft is the theft of all sorts of digital information which includes gaining access to private information or violating privacy. It is done mainly through computers, servers, or any electronic devices. A person, who has not been authorized and is accessing financial or private data, can delete, modify, or deny access without permission from the owner. Data theft usually occurs whenever the attackers want to sell the data or use it to commit identity theft. (Kaspersky, 2025)

3. Phishing:

   Phishing is an crime where an individual pretend to be an existing organisation and attempts to reach victims through contacts, email, phone or mobile text with the single motive of

tricking them into giving confidential details such as personally identifying information, banking and credit card numbers, and passwords. (PhishingOrg, 2025)

4. Denial-of-Service(DoS):

   A denial-of-service attack is a type of cyber-attack where an attacker makes an effort to render a computer or some other device out of use to its clients by interrupting its functioning. It typically involves overwhelming a target system with requests making it unable to process regular traffic, causing denial-of-service to other consumers. (Cloudflare, 2025)

1.2. Background

The Capital One attack was among the largest data breaches. On July 29, Capital One announced that a data security incident led to the exposure of approximately 100 million individuals' personal data in the United States and nearly 6 million in Canada. The official report stated that the breach was done by Paige A. Thompson, a former software engineer at Amazon Web Services (AWS) and main suspect in the investigation, who breached illegally a Capital One data server. The attacker had access to personal data gathered by the bank from applicants for credit cards, such as names, addresses, zip codes, phone numbers, email addresses, birth dates, and income reported. Apart from credit card application information, the intruder got fragments of customers' information like customers' status details, fragments of transactions records, Social Security numbers, and parts of their associated bank account numbers of the credit card owners. (Shaharyar Khan, 2022)

2. Social Issues

Social issues are behaviours or conditions that has a negative effect on members of society and must be addressed. These social issues affect not only individuals but also cause disturbance or misery for huge groups of people. The problem is that a social issue has a negative impact on a big percentage of the population, contradicts their values or ideals and is recognised as a significant problem that must be resolved. These concerns can be addressed through social action, distribution of resources, or regulation. (Stewart, 2023)

The social issues with the case are:

1. Impact on Individuals:

   The capital data breach that affected more than 100 million people in the US and 6 million in Canada by exposing their data led to the rise of many social issues. The incident affected sensitive data, such as Social Security numbers and bank account information, which reduced the trust in financial organizations and its ability to protect personal information. (Capital One, 2022)

2. Risk of Identity Theft:

   Personal data breaches increased the risk of identity theft and fraud, making individuals to take precautions like credit monitoring and freezing. It showed weaknesses related to using Social Security numbers as primary identities, causing experts to push for more secure identification processes. (Aguilera, 2019)

3. Data Privacy Concerns:

   The breach revealed the need for stronger consumer privacy laws, raising advocacy organizations to seek for comprehensive federal legislation that would hold firms accountable for data security. This data breaches caused many privacy issues for consumers. Due to data breach, sensitive customer information found its way into the darkest regions of the digital market. This data can then be utilized, without user awareness or agreement, for a number of criminal purposes. (Stella, 2019)

4. Delayed Data Exposure:

   Equifax, a NCRAs took two months to reveal a cybersecurity incident had happened in July but that was hidden from the public until September. During that time, 147 million consumers were unaware that their personal information, including federal income tax records and employee records for government employees, was at risk. Neither did users of significant government programs realize that they were harmed too. (Crowell, 2019)

5. Corporate Trust Failure:

   The leak damaged public trust in financial institutions, as people became anxious about the security of their financial information and the institutions' ability to protect it. As a result, there was an increase in public demand for company to be held accountable for data breaches, showing the importance of open communication and settlements for those harmed. (Crowell, 2019)

3. Ethical Issues

Ethical issues emerge when a specific choice, situation, or action conflicts with the moral standards of a society. Both individuals and companies can be part of these disputes, as any of their actions may be viewed from an ethical perspective. These disputes can occasionally pose legal risks, as certain resolutions to the issue might infringe upon a particular law. In some instances, the issue might not have legal implications, yet it could provoke an unfavourable reaction from third parties. (MyAccountingCourse, 2025)

The ethical issues with the case are:

1. Weak Security and Prevention Failure :

   The incident highlighted the issue of the weak security in the handling of the information and data by the company. Similar accidents took place before in 2017 where a former employee accessed the personal information of costumers for four months. There also happened a similar breach in 2014 and in 2015 at Amazon Web Services' annual conference, a Capital One official spoke about the company's efforts to migrate critical portions of its technology to Amazon's cloud infrastructure, allowing it to focus on developing consumer applications and other needs but still the data was breached. (Emily Flitter, 2019)

2. Inadequate Risk Management:

   Capital One failed to develop proper risk management in 2015 when it changed information technology operations to a cloud-based service. The

company's internal audit failed to discover several weaknesses in its cloud environment management, as well as risky or poor actions that were part of a pattern of misconduct. (Technology, 2020)

3. Executive Decision Failure:

   Many Capital One policies and decisions were made by senior leadership, who were primarily responsible for providing an effective cybersecurity strategy and allocating sufficient resources to achieve their security goals in their cloud transition. However, the leadership failed to create adequate risk management processes for its cloud strategy. This raised ethical concerns about the board's responsibility towards its customers. (Shaharyar Khan, 2022)

4. Violation of Trust:

   Capital One had a clear duty to protect its client's sensitive data as Social Security numbers and account information. The breach violated the responsibility of trust by exposing clients to threats such as identity theft and economic fraud. Ethically, the corporation failed in its function of data security, indicating major dereliction of duty and loss of consumer trust. (Shaharyar Khan, 2022)

5. Accountability and Responsibility:

   The breach led in a $190 million settlement to impacted customers but the compensation may not be sufficient to cover the long-term damage. The case raises ethical concerns about Capital One's accountability and whether the settlement offered was adequate and reasonable for the victims. (Gema, 2023)

4. Legal Issues:

A legal issue is something that has legal implications and can need the services of an attorney for its solution. Legal issues can emerge in a variety of ways, like from deliberate events of your life, like buying a home or creating a will. They may also emerge abruptly, like family issues, disagreements at work, or being accused of committing a crime. The other dominant legal problems are immigration and asylum, consumer rights, housing issues, and debt and money management problems. (SRA, 2021)

The legal issues with the case are:

1. Class One Lawsuit:

   Capital One was sued less than 24 hours after the event, accusing it of major security failures. The proposed class action was filed in the United States District Court for the District of Columbia, accusing the firm of negligence for failing to protect personal information. (HewardMills, HewardMills, 2019)

2. Lawsuit Settlement:

   Capital One had to pay a $190 million lawsuit settlement and also allocated funds for the affected customers. The settlement covered the 98 million customers who were harmed by the breach. (Ennis, 2023)

3. Consent Order:

   The OCC issued a consent order against Capital One, ordering them to pay $80 million fine and form an independent compliance committee to review cybersecurity issues. The order additionally asked Capital One to provide improvements within 60 days. (Gandel, 2020)

4. Mitigate Damage:

   Capital One was legally required to mitigate the damage caused by the breach, which included informing affected customers and providing credit monitoring services. The Federal Reserve's ruling asked Capital One's board of directors to submit a written plan describing how it expected to improve risk management and internal controls for client data protection. (Ennis, 2023)

5. Investigation by The Federal Trade Commission (FTC):

   The Federal Trade Commission (FTC) investigated Capital One's data security and found that the company failed to do sufficient risk assessments and consider security flaws before the breach occurred. This resulted in mandatory improvement in data security program for Capital One. (HewardMills, 2019)

5. Professional Issues

5.1. Profession and Professionals

Profession:

A profession is a type of occupation that requires higher learning and training. The traditional studied professions include law, medicine, and ministry. Learnt professions are marked by the requirement of unconventional learning, the presence of close relationships and commitment to a higher plane of ethics than the marketplace. (LSD, 2025)

Professionals:

Professionals are highly educated individuals who have received extensive education and training. A professional is someone who earns a living by performing specialised work that they learnt through significant education and training, and who feels obligated to follow particular rules defined by their profession's organisation. A professional can pursue a wide range of jobs where most pay well. (Team, 2025)

5.2. Professional Issues

Professional ethics are the rules that observe the conduct of any group of individuals or individual within the business world. Professional ethics sets standards on how people are supposed to deal with others and institutions. Professional ethics tend to be codified as a set of rules that are followed by a specific group of people. This implies that all the members in a specific group

will adhere to the same professional ethics regardless of their different beliefs. (Immigration Advisers Authority, 2025)

The professional issues with the case are:

1. Misconfigured Firewall:

   The WAF, which is designed to protect against web-based attacks, was not properly configured, allowing the attacker to bypass its intended purpose. The threat actor gained network access via a misconfigured open-source web application firewall (WAF). The multi-stage attack enabled the offender to extract data from an AWS S3 storage bucket. (Jones, 2022)

   This issue is associated to ACM Code of Ethics – 1.2 Avoid Harm which states that negative impacts, particularly one that are significant and unjust. Unjustified bodily or mental injury, the destruction or revelation of information, and damage to property, reputation, and the environment are also harm. (Association for Computing Machinery, 2018)

2. Ineffective Encryption:

   The role, ISRM-WAF-Role, attached to the instance appears to have excessive rights, permitting the listing and access of S3 buckets containing sensitive data. The attacker utilised this privilege to list and download the buckets locally. The data was encrypted, but the intruder was able to decrypt it as well. (Shaharyar Khan, 2022)

   This issue is associated to IEEE Code of Ethics - Maintain confidentiality and respect privacy and it shows that extensive

permissions broke the idea of least privilege, which increased risk and affected the condition of data security. (IEEE, 2025)

3. Weak Cloud Infrastructure:

   Issues in the cloud architecture allowed attackers to acquire access to sensitive data by accessing the metadata service and using temporary credentials. (Shaharyar Khan, 2022)
   This issue violated ACM Code of Ethics – 1.2 Avoid Harm, 1.6 Respect Privacy, 2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks. Improper cloud infrastructure security led to data breaches caused by weak configuration that affected users and stakeholders. Insufficient data security led to unauthorised access to confidential information. The principle failed due to insufficient evaluation of cloud security problems before execution. (Association for Computing Machinery, 2018)

4. Server-Side Request Forgery (SSRF):

   The Capital One hacker took use of a server-side request forgery (SSRF) weakness in the company's web application firewall. The attacker exploited the SSRF vulnerability and the WAF privileges on Capital One's AWS server to steal important information. (Poston, 2019)
   This issue mainly addressed BCS Code of Conduct – Public Interest: “You shall have due regard for public health, privacy, security and well-being of others.” where The SSRF vulnerability allowed data theft, risking user privacy and security and Professional Competence and Integrity: “You shall work competently and diligently for your clients and

employers.” inability to implement secure code and configuration showed a lack of diligence and skill. (BCS, 2025)

5. Regular Security Audits:

Regular security audits and vulnerability scans are crucial for detecting misconfigurations before they are exploited. Capital One failed to frequently monitor and audit system configurations, resulting in WAF misconfiguration and other vulnerabilities which caused the incident. (Sprintzeal, 2024)

This issue fall under the Software Engineering Code of Ethics (ACM/IEEE SECEPP) - 1.03 Approve software only if they have a well-founded belief it is safe, 3.10 Ensure adequate testing, debugging, and review of software and related documents, 6.08 Take responsibility for detecting, correcting, and reporting errors in software and associated documents. Without audits there is no guarantee for safety of system for long period of time. Security audits are major component of review and quality assurance. Regular audits helps to identify problems before any harm to the system. Irregular or audit failure can also be seen as lack in professional accountability. (Association for Computing Machinery, 1999)

6. Conclusion and Personal Reflection:

6.1. Conclusion:

The Capital One 2019 data breach serves as an important example of how critical it is for organisations today to invest heavily in strong cybersecurity measures, particularly when operating in cloud settings. As infrastructure becomes more complex digitally and as data becomes more valuable, the effect of one misconfiguration such as that of Capital One's web application firewall can be very harmful. Institutions must effectively configure firewalls, conduct regular and thorough security audits, and aggressively control vulnerabilities before they may be exploited. Beyond technical improvements, any organization's approach must include ethical governance and a strong commitment to consumer data security. In today's digital environment, cybersecurity must be viewed as an integral component of corporate social responsibility, rather than as an afterthought.

The responsibility of safeguarding sensitive data is not based on technical measures alone. It must be connected with an organisation's ethical governance framework, where leadership is fully accountable for maintaining strong data protection and stakeholders are involved in every part of it. Ethical governance requires prioritising user privacy, ensuring informed consent, and designing systems that reflect fairness, respect, and accountability.

Finally, the Capital One breach serves as a wake-up call for all organisations to make cybersecurity an ethical and moral priority.

6.2. Personal Reflection:

Doing this report I got to know about capital one and what it serves as. A financial organization offering financial and banking services to millions of people in the US and Canada, it is the largest commercial service.

The Capital One 2019 data breach affected over 100 million individuals. This incident greatly influenced my knowledge of the actual consequences of failing to meet appropriate ethical, professional, and technological standards. Based on the issue, I believe Capital One's failure was largely due to its disregard for core cybersecurity principles and ethical commitments.

If I were in a position of authority, I would advise creating a zero-trust security method, requires continuous verification of individuals, devices, and network activities, independent of whether they are inside or outside of the organization investing more significantly in cloud security certifications, and cultivating a workplace where security is everyone's duty. I would also invest in cloud security personnel certifications to enhance technical expertise. I would also create a culture where cybersecurity is everyone's responsibility, not just an IT problem. I would make sure that every personnel working in or out of the organization has a better and vast understanding of cybersecurity which includes regular awareness campaigns, clearly defined security procedures, and responsibility at all levels. Organisations must recognise that ethical cybersecurity practices are required to retain confidence and uphold social contracts with stakeholders.

Finally, the Capital One breach shows how one neglected vulnerability can result in such huge damage. It has impacted me to approach technology with a stronger sense of moral responsibility, recognising that professional decisions have long-term ramifications for people's lives.

7. References

Aguilera, J. (2019, 07 30). *Time*. Retrieved from Time: https://time.com/5638896/capital-one-data-breach-4-things-secure/

Association for Computing Machinery. (1999). Retrieved from Association for Computing Machinery: https://www.acm.org/code-of-ethics/software-engineering-code

Association for Computing Machinery. (2018). Retrieved from Association for Computing Machinery: https://www.acm.org/code-of-ethics

Bakharev, N. (2024, 01 10). *Brightse*. Retrieved from Bright: https://www.brightsec.com/blog/unauthorized-access-risks-examples-and-6-defensive-measures/

BCS. (2025). Retrieved from BCS: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/

Capital One. (2022, 04 22). Retrieved from capitalone.com: https://www.capitalone.com/digital/facts2019/

CapitalOne. (2025). Retrieved from CapitalOne: https://www.capitalone.com/

Cloudflare. (2025). Retrieved from Cloudflare: https://www.cloudflare.com/en-gb/learning/ddos/glossary/denial-of-service/

Crowell, C. (2019, 08 11). *New Pittsburgh Courier* . Retrieved from New Pittsburgh Courier : https://newpittsburghcourier.com/2019/08/11/capital-one-data-breach-put-another-100-million-consumers-at-risk/

Emily Flitter, K. W. (2019, 07 29). *The New York Times*. Retrieved from The New York Times: https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html

Ennis, D. (2023, 07 13). *CyberSecurityDive*. Retrieved from CyberSecurityDive: https://www.cybersecuritydive.com/news/fed-ends-capital-one-breach-

action/686970/#:~:text=The%20Fed's%20order%20required%20Capital,her%20to%20access%20the%20data.

Gandel, S. (2020, 08 06). *CBS News*. Retrieved from CBS News: https://www.cbsnews.com/news/capital-one-hack-credit-card-applications-settlement/

Gema, S. (2023, 10 31). *Medium*. Retrieved from Medium: https://medium.com/@sweetgema383/an-ethical-lapse-equifax-data-breach-case-study-033c76cf28ef

GlobalData. (2025). *GlobalData*. Retrieved from GlobalData: https://www.globaldata.com/company-profile/capital-one-financial-corp/#

HewardMills. (2019, 09 07). Retrieved from https://www.hewardmills.com/the-legal-fallout-of-the-capital-one-data-breach/#:~:text=The%20UK%20Information%20Commissioner%2C%20Elizabeth,in%20the%20EU%20and%20beyond.

HewardMills. (2019, 09 07). *HewardMills*. Retrieved from HewardMills: https://www.hewardmills.com/the-legal-fallout-of-the-capital-one-data-breach/#:~:text=Less%20than%2024%20hours%20after%20this%20event%2C,negligence%20for%20failing%20to%20safeguard%20personal%20data.

IEEE. (2025). Retrieved from IEEE: https://www.ieee.org/about/corporate/governance/p7-8

Immigration Advisers Authority. (2025). Retrieved from Immigration Advisers Authority: https://www.iaa.govt.nz/for-advisers/adviser-tools/ethics-toolkit/professional-ethics-and-codes-of-conduct/#:~:text=Professional%20ethics%20are%20principles%20that,institutions%20in%20such%20an%20environment.

Jones, T. (2022, 12 04). *Medium*. Retrieved from Medium: https://medium.com/nerd-for-tech/capital-one-data-breach-2019-f85a259eaa60

Kaspersky. (2025). Retrieved from Kaspersky: https://www.kaspersky.com/resource-center/threats/data-theft

LSD. (2025). Retrieved from LSData: https://www.lsd.law/define/profession

MyAccountingCourse. (2025). Retrieved from MyAccountingCourse: https://www.myaccountingcourse.com/accounting-dictionary/ethical-issues#What_Does_Ethical_Issues_Mean

PhishingOrg. (2025). Retrieved from PhishingOrg: https://www.phishing.org/what-is-phishing#:~:text=Phishing%20is%20a%20cybercrime%20in,credit%20card%20details%2C%20and%20passwords.

Poston, H. (2019, 10 21). *Infosec*. Retrieved from Infosec: https://www.infosecinstitute.com/resources/news/lessons-learned-the-capital-one-breach/#:~:text=Principle%20of%20least%20privilege%20One%20of%20the,permissions%20necessary%20to%20perform%20their%20job%20role.

Shaharyar Khan, I. K. (2022, 11 07). *ACM Digital Library*. Retrieved from ACM Digital Library: https://dl.acm.org/doi/10.1145/3546068

Sprintzeal. (2024, 12 17). Retrieved from Sprintzeal: https://www.sprintzeal.com/blog/capital-one-cyber-incident#:~:text=You%20see%2C%20from%20the%20experience,which%20resulted%20in%20unauthorized%20access.

SRA. (2021, 08 21). Retrieved from Solicitors Regulation Authority: https://www.sra.org.uk/consumers/choosing/legal-issue/

Stella, S. (2019, 07 30). *Public Knowlwdege*. Retrieved from Public Knowledge: https://publicknowledge.org/capital-one-data-breach-reinforces-need-for-strong-consumer-privacy-protections/

Stewart, R. (2023, 11 21). *Study.com*. Retrieved from Study.com: https://study.com/academy/lesson/social-issues-definition-

examples.html#:~:text=Social%20Issues%20are%20any%20behavior,health%20consequences%20for%20teenagers%20themselves).

Team, I. E. (2025, 03 05). *Indeed.* Retrieved from Indeed: https://ie.indeed.com/career-advice/career-development/what-is-professional

Technology. (2020, 08 06). *The Washington Post*. Retrieved from The Washington Post: https://www.washingtonpost.com/business/technology/capital-one-fined-80-million-in-data-breach/2020/08/06/bde1a106-d844-11ea-a788-2ce86ce81129_story.html

Tunggal, A. T. (2025, 03 11). *UpGuard*. Retrieved from UpGuard: https://www.upguard.com/blog/cyber-threat#:~:text=A%20cyber%20or%20cybersecurity%20threat,attacks%2C%20and%20other%20attack%20vectors.