



CS5071NI - Professional and Ethical Issues

100% Individual Coursework

2024-25 Autumn

Credit: 15 Semester Long Module

Student Name: Aaliya Singh Bhandari

London Met ID: 23047627

College ID: NP01CP4A230364

Assignment Due Date: Monday, May 19, 2025

Assignment Submission Date: Sunday, May 18, 2025

Word Count: 3065

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.

23047627 Aaliya Singh Bhandari2.docx

 Islington College, Nepal

Document Details

Submission ID

trn:oid:::3618:96606146

Submission Date

May 19, 2025, 9:23 AM GMT+5:45

Download Date

May 19, 2025, 9:25 AM GMT+5:45

File Name

23047627 Aaliya Singh Bhandari2.docx

File Size

20.6 KB

15 Pages

3,035 Words

17,828 Characters



Page 1 of 20 - Cover Page

Submission ID trn:oid:::3618:96606146







Page 2 of 20 - Integrity Overview

Submission ID trn:oid:::3618:96606146




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
-  **9 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

- 6%  Internet sources
- 1%  Publications
- 10%  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. PART 1: INTRODUCTION AND BACKGROUND OF THE SCANDAL.....	1
1.1. Introduction	1
1.1.1. Introduction to the Company	1
1.1.2. Introduction To Cyber Threats and Data Breaches	2
1.2. Background of the Scandal	2
1.2.1. Past Breaches	2
1.2.2. Overview Of the Scandal	2
1.2.3. Evolution Of Breach	3
1.2.4. Intention of breach	3
1.2.5. Impact Of the Breach	3
2. PART 2: SOCIAL ISSUES.....	4
2.1. Identity Theft and Financial Fraud	4
2.2. Erosion of Public Trust in Financial Institutions	4
2.3. Psychological Distress and Fear of Data Misuse	4
2.4. Digital Inequality and Vulnerability of Marginalized Groups.....	5
2.5. Increased Demand for Regulatory Reform	5
3. PART 3: ETHICAL ISSUES.....	6
3.1. Corporate Responsibility and Negligence:	6
3.2. Abuse Of Insider Knowledge and Skills:	6
3.3. Privacy and Consumer Rights:	6
3.4. Failure to Communicate Transparently with Affected Customers:.....	6
3.5. Lack Of Proactive Ethical Risk Management.....	7
4. PART 4: LEGAL ISSUES.....	8
4.1. Violation of the Gramm-Leach-Bliley Act (GLBA)	8
4.2. Breach of Consumer Protection Laws.....	8
4.3. Criminal Charges under the Computer Fraud and Abuse Act (CFAA).....	8
4.4. Data Breach Notification Law Violations.....	9
4.5. Regulatory Settlements and Financial Penalties	9
5. PART 5: PROFESSIONAL ISSUES.....	10
5.1. Failure to Implement Security Best Practices (BCS Code of Conduct)	10
5.2. Misuse of Privileged Access and Insider Threats (ACM Code of Ethics)	10
5.3. Lack of Accountability and Transparency (IEEE Code of Ethics)	10

5.4. Inadequate Risk Assessment and Management (ACM Code of Ethics).....	11
5.5. Failure to Uphold Public Interest and Welfare (BCS Code of Conduct)	11
6. PART 6: CONCLUSION AND PERSONAL REFLECTION	12
6.1. Conclusion	12
6.2. Personal Reflection and Ethical Recommendations.....	13
<i>REFERENCE</i>	<i>14</i>

1. PART 1: INTRODUCTION AND BACKGROUND OF THE SCANDAL

1.1. Introduction

1.1.1. Introduction to the Company

Capital One Financial Corporation (COF) is a leading American bank holding company that specializes in a broad range of financial services, including credit card issuance, retail banking, auto loans, and savings products. Established in 1994, the company has a strong market presence primarily across the United States, with growing operations in Canada and the United Kingdom. As of 2024, Capital One ranks among the largest banks in the United States based on assets and is a Fortune 500 company (BBC, 2019)

Unlike traditional banks, Capital One heavily invests in technology and cloud-based solutions to improve service delivery and customer experience. It was one of the first major banks to commit to a full migration of its IT infrastructure to Amazon Web Services (AWS) cloud, aiming to enhance scalability, cost efficiency, and technological innovation. However, while cloud technologies bring benefits, they also expose organizations to new cybersecurity risks if not properly managed (Newman, 2020).



Figure 1: Capital One

1.1.2. Introduction To Cyber Threats and Data Breaches

In this digital era, organisations that are related to financial faces huge amounts of customer data which are sensitive, which makes it the top concern of cybersecurity. But still till this date, breaches occur every now and then. Out of many, one incident that is still talked heavy is Capital One Data Breach in 2019. It exposed personal information of over 100 million U.S. customers and 6 million Canadian Customers (McMillan, 2019) The breach developed from a WAF (web application firewall) which allowed an unauthorized individual called Paige Thompson, a former Amazon Web Services (AWS) employee. This was the talk to the town for a very long time which highlights the risk that comes with cloud computing, the responsibilities of the institutions which are involved in securing consumer data and the severe outcome of cybersecurity failures.

1.2. Background of the Scandal

1.2.1. Past Breaches

Before Capital One's breach, data breaches in the financial industry were high-profile and highlighted data security weaknesses. In 2017 alone, more than 147 million people's sensitive information - Social Security numbers, credit reports, and birthdays - were pilfered in the Equifax hacking breach. It is one of the most severe and highest-profile breaches on record in the U. S (Federal Trade Commission , 2024). Another high-profile breach in 2014 involved JPMorgan Chase being a target for a cyber breach that affected more than 76 million households and 7 million small businesses. Hackers compromised customer names, addresses, and contact information through a server vulnerability. (Jessica Silver-Greenberg, 2014)

1.2.2. Overview Of the Scandal

The Capital One data breach took place in March 2019, but it wasn't found until July 2019, during an external security researcher found the leaked information in GitHub. Paige Thompson utilized the misconfiguration in Capital One's AWS S3 storage, which allowed her to access and remove the data. The breach showed the Social Security Numbers, Bank account details and personal information, which was leading to huge amount of privacy breach. (BBC, 2019)

Capital One only became aware of the violation only after a white hat hacker informed them of all the exposed data which lead to an internal investigation, the company found out all the breach and

they reported it to the FBI which later resulted in Paige Thompson arrest. Capital One faced major financial and legal battles, that includes 80 million fines from the Office of the Comptroller of the Currency (OCC) and a 190 million to the affected customers who were affected. (Newman, 2020)

1.2.3. Evolution Of Breach

The data breach was carried out by Paige Thompson who is a past software engineer at Amazon Web Services (AWS). She exploited a misconfigured firewall in Capital One's AWS cloud storage that provided unauthorized access to data in S3 buckets. She used scanning tools to identify the vulnerability and extract confidential data. Although it occurred in March, it wasn't discovered until July when it was reported by a white-hat hacker after discovering leaked data on GitHub (Ma, 2019)

1.2.4. Intention of breach

Unlike most financially motivated cyber aggressors, it appeared that Thompson's actions were motivated by political or personal reasons. She is not shown to have attempted to sell the data and cash in on it financially. She discussed the breach publicly on forums and even posted the information publicly for all to see, and that is how she got caught. Those who study her actions feel she was more interested in exposing vulnerabilities than making profits. (Former Seattle Tech Worker Indicted on Federal Charges for Wire Fraud and Computer Data Theft, 2019)

1.2.5. Impact Of the Breach

The consequences of the breach were wide-reaching. American banking regulators fined Capital One \$80 million due to risk management and data security practice inadequacies. Capital One also settled with affected customers in a class-action lawsuit to pay \$190 million (CNBC, 2020). Beyond monetary losses, the breach damaged Capital One's reputation and raised serious concerns about cloud services' security, especially in connection with financial establishments using third-party services like AWS. (Waldman, 2022)

2. PART 2: SOCIAL ISSUES

This kind of breach is far-reaching in its implications for millions upon millions of its consumers and raises concerns for privacy violation, trust, and identity theft. Its concerns at present encompass one major concern being financial fraud using personal banking information, its victims becoming victims of identity theft, unauthorized transactions and financial losses. Its stolen data, according to its cybersecurity agency, is likely to end up in the dark web, its criminals exchanging personal information. (Smith, 2020)

2.1. Identity Theft and Financial Fraud

One of its direct societal implications was a greater threat of identity theft and financial fraud, customer information that contained Social Security numbers, bank account numbers, and credit reports were compromised. Such information is generally used by cyber thieves to allow them to create unauthorized bank accounts, apply for loans, or even make false purchases in their victims' names. Victims of identity thieves may take years and even months to settle their losses as they incur financial loss and lost opportunities in the meantime. (BCC News, 2019)

2.2. Erosion of Public Trust in Financial Institutions

Public trust is the foundation of the financial services sector. The Capital One incident significantly damaged consumer confidence not only in Capital One but in banks and financial technology services more broadly. Customers questioned whether institutions claiming technological advancement truly had the competence to protect their personal data. The breach fueled negative feedback about online banking security and cloud computing models, leading some customers to revert to more traditional, less technology-reliant methods (Smith, 2020)

2.3. Psychological Distress and Fear of Data Misuse

Beyond financial impacts, the breach inflicted psychological distress on millions of individuals. Fear of their personal information being misused for identity theft, blackmail, or even targeted scams created anxiety and insecurity among customers. Psychological studies have shown that

data breach victims often suffer long-term stress, trust issues, and feelings of helplessness (CNN, 2019). Such emotional consequences extend far beyond the direct financial costs.

2.4. Digital Inequality and Vulnerability of Marginalized Groups

Not all individuals affected by the breach had equal access to resources to protect themselves. Low-income populations and digitally marginalized groups often lack cybersecurity awareness or financial resources to implement protective measures like credit monitoring services. As a result, breaches like Capital One's disproportionately harm the most vulnerable members of society, exacerbating digital and economic inequality (Forbes , 2021)

2.5. Increased Demand for Regulatory Reform

The scale of the Capital One breach led to an intensified call for stronger consumer data protection laws. Although regulations like the General Data Protection Regulation (GDPR) exist in Europe, the United States lacked comprehensive federal data protection legislation at the time. Citizens, advocacy groups, and policymakers demanded stricter regulations to hold corporations accountable and empower consumers to protect their data rights (The Verge, 2019)

3. PART 3: ETHICAL ISSUES

The breach also brought very serious ethical failure to the limelight and highlighted where both company and corporate conduct fell short of professional expectations. From an ethical point of view, Capital One has multiple concerns:

3.1. Corporate Responsibility and Negligence:

Capital One had a major duty which was to protect customer information and make sure that the cloud infrastructure was secure, but the misconfiguration of WAF encouraged negligence while implementing the security measures. In ethical frameworks Consequentialism, organizations should anticipate the potential consequences of their actions. (Brown, 2020)

3.2. Abuse Of Insider Knowledge and Skills:

Paige Thompson's former AWS software Engineer made us raise the ethical question about the responsibility of an IT engineer. She misuses the knowledge of AWS security flaws and violated the principles of honesty in IT professionals. As an IT professional it is a duty to not misuse their technical knowledge to harm others. (Johnson, Ethics in IT security: The role of professionals in preventing data breaches, 2019)

3.3. Privacy and Consumer Rights:

When customers provide their personal information to the organization, they put trust in the cloud computing system to protect it in any case or scenario but breach like this causes them to fear and not trust the organization completely. Under Virtue Ethics, the way the company takes responsibility for data management and proactive security measures reflects the ethical character of a company. (Westin, 2020)

3.4. Failure to Communicate Transparently with Affected Customers:

After the discovery of the breach, Capital One didn't inform the public immediately, which affected the individuals, some had a minor loss while some had major loss. The ethical

standards like honesty, transparency, and integrity. But the delayed disclosure took the time from customers to take any action to protect their accounts.

3.5. Lack Of Proactive Ethical Risk Management

Ethical practice demands that companies not only react to the problem but also consistently work to prevent foreseeable harm and problems. Capital One's failure to conduct risk assessments before moving to AWS shows ethical shortsightedness.

4. PART 4: LEGAL ISSUES

Capital One breach resulted in not only economic loss but also triggered heightened legal examination of data privacy, compliance, and business accountability in handling personal consumer information. The following are five of the key concerns of law in the wake of the hack:

4.1. Violation of the Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to safeguard sensitive customer data and disclose their information-sharing practices. Capital One's failure to secure customer data violated its obligations under GLBA's Safeguards Rule, which mandates companies to implement strong security protocols (Federal Trade Commission, 2021). By misconfiguring their cloud security, they exposed personal information without sufficient protection, leading to potential enforcement actions by regulators.

4.2. Breach of Consumer Protection Laws

Multiple lawsuits alleged that Capital One's inadequate cybersecurity measures constituted unfair and deceptive practices under various state consumer protection laws, such as the Virginia Consumer Protection Act (CNN, 2019). These laws exist to ensure that companies act reasonably to protect consumers from harm. By neglecting to secure their systems properly, Capital One opened itself to consumer litigation and regulatory penalties.

4.3. Criminal Charges under the Computer Fraud and Abuse Act (CFAA)

Paige Thompson was indicted under the U.S. Computer Fraud and Abuse Act (CFAA) for unauthorized access to Capital One's computer systems. CFAA criminalizes hacking activities that involve accessing protected systems without permission. Thompson's actions, although not intended for direct financial gain, still constituted unauthorized access, resulting in multiple charges including wire fraud and computer-related offenses (United States Department of Justice, 2020)

4.4. Data Breach Notification Law Violations

Most U.S. states require companies to notify affected customers "without unreasonable delay" following a data breach. Although Capital One eventually disclosed the breach, questions were raised about whether they violated notification timelines. Delays in informing consumers can lead to further legal exposure under data breach notification statutes (BBC, 2019)

4.5. Regulatory Settlements and Financial Penalties

Capital One agreed to pay \$80 million in fines imposed by the U.S. Office of the Comptroller of the Currency (OCC) for failing to establish effective risk management processes before migrating to the cloud (Forbes , 2021). In addition, a class-action lawsuit settlement of \$190 million was reached with customers. These settlements serve as legal acknowledgment of Capital One's inadequate cybersecurity practices and the legal obligations companies have toward consumer protection.

5. PART 5: PROFESSIONAL ISSUES

The breach highlighted severe professional failings, particularly regarding the responsibilities of IT professionals and corporations to protect sensitive information. These failures can be evaluated using established professional codes such as those from ACM (Association for Computing Machinery), BCS (The Chartered Institute for IT), and IEEE.

5.1. Failure to Implement Security Best Practices (BCS Code of Conduct)

According to the BCS Code of Conduct, IT professionals are expected to adhere to best practices in security and system management. Capital One's failure to configure its web application firewall properly reflects a serious breach of professional diligence standards. Proper audits, testing, and validation procedures were neglected, demonstrating a lack of professional responsibility (BCS Code of Conduct, 2021)

5.2. Misuse of Privileged Access and Insider Threats (ACM Code of Ethics)

Paige Thompson's case exemplifies insider threats, where an IT professional uses insider knowledge maliciously. The ACM Code of Ethics emphasizes that professionals must "honor confidentiality" and avoid using technical knowledge to harm others. Thompson's unauthorized activities breached core professional standards (ACM Code of Ethics, 2018)

5.3. Lack of Accountability and Transparency (IEEE Code of Ethics)

The IEEE Code of Ethics mandates accountability, honesty, and disclosure of potential dangers in their entirety. Capital One's delayed and incomprehensive public disclosure of the attack amounts to a flagrant default of ethical requirement. Non-compliance with such ethical standards can lead to loss of trust among the public, juridical penalties, loss of reputation, as well as erosion of the stakeholder relationship. Violation of these standards harms not only parties but also affects the ethical reputation of the profession in general. (IEEE Code of Ethics, 2020).

5.4. Inadequate Risk Assessment and Management (ACM Code of Ethics)

Professional practice mandates rigorous risk analysis, especially in new technology adoption. Capital One's transition to AWS in disregard of identified vulnerabilities in security was in contravention of the ACM Code of Ethics, which holds computer professionals to "avoid harm" as well as to perform rigorous risk analysis before a shift in systems. Not conducting ethical risk management undermines systems stability as well as security, apart from violating professional duty to protect users and parties involved. (ACM Code of Ethics, 2018)

5.5. Failure to Uphold Public Interest and Welfare (BCS Code of Conduct)

The BCS Code of Conduct outlines that computer professionals have a moral duty to serve in public interest and as guardians of society's wellbeing. For Capital One, that millions of people's sensitive personal information was hacked suggests a deep concern over a duty to safeguard the public. When public interest is not safeguarded by professionals, it can prompt a devastating loss of trust, legal penalties, reputation loss, as well as damage to vulnerable parties. Such moral failures tarnish professional reputations as well as erode public confidence in digital systems (BCS Code of Conduct, 2021)

6. PART 6: CONCLUSION AND PERSONAL REFLECTION

6.1. Conclusion

The case of 2019's Capital One data breach is significant as it is a case study of the relationship between technology, ethics, law, and standards of conduct in the modern economy. Although Capital One had the image of being an innovative company and an early adopter of infrastructure in the cloud, the company did not put in place the appropriate cybersecurity controls in protecting sensitive customer information. The resultant breach of personal details of over 100 million people resulted in significant financial, social, and psychological harm. The event raised fundamental issues of company accountability, insider risk, transparency, rights of consumers in privacy, and regulation of data protection. Regulators such as the Office of the Comptroller of the Currency (OCC) levied significant fines, while class action suits highlighted the extent of the failures of Capital One.

On a larger scale, Capital One hack unveiled structural weaknesses in how organizations embark on digital transformations. Plunging headfirst into cloud-hosted platforms with insufficient risk assessment and ethical considerations is dangerous. The hack taught the entire sector in general an invaluable lesson: security should never be an afterthought but an integral part of technological innovation. The code of ethics adopted by ACM, IEEE, and BCS requires openness, honesty, accountability, and the duty not to do harm. These concepts were violated both by Paige Thompson as well as by the organization itself, Capital One.

6.2. Personal Reflection and Ethical Recommendations

The case study involving Capital One highlighted the need to infuse ethics into all stages in the technology system life cycle. The breach served to highlight that technical proficiency is insufficient to prevent breakdowns in cybersecurity. Ethical awareness must be infused in all aspects of system design and management so that stakeholders' interests comprising customers, employees, investors, and members of the public can be protected. The case also served as an illustration of how trust, transparency, and accountability must form cornerstones in any tech-based organization, particularly one handling sensitive personal data. (Shaharyar Khan, 2022)

The violation further emphasized organizational responsibility not to harm and to ensure information privacy. Utilizing ethical principles such as utilitarianism and deontological ethics allows actions to be judged on the grounds that they result in the least harm, respect for human rights and organizational reputation. Ethical reasoning indicates that being proactive such as regular security scans, timely breach notifications, and insider-threat tracking is extremely effective in reducing harm risk and stakeholders' trust. (Sprintzeal, 2024)

First, regular third-party cybersecurity audit processes must be conducted by organizations to identify and fix vulnerabilities in cloud infrastructure. Secondly, consumer transparency must take center stage so that affected stakeholders are informed in a timely manner in case a data breach occurs. Thirdly, stringent insider threat programs must be mandatory, whereby alerting mechanisms identifying irregular activity by authorized personnel. These practices show ethical norms by averting harm, upholding customer rights, and organizational accountability. (Shaharyar Khan, 2022)

Lastly, this case highlights the need to map organizational practice onto professional codes of ethics, as issued by Association for Computing Machinery (ACM) and British Computer Society (BCS). These and not mere recommendations but mandatory requirements that maintain ethical practice and protect public interest. Ethical responsibility and success through regulations must go together with innovation to foster organizational resilience. In years ahead, conformity with ethical decision structures will be crucial in defining accountable practice and minimizing data breaches to an absolute minimum. (Shaharyar Khan, 2022)

REFERENCE

- McMillan, J., 2019. In: *Capital One and the risks of cloud computing: A security analysis. Journal of Digital Security*, . s.l.:s.n.
- Newman, A., 2020. [Online]
Available at: <https://www.wired.com/story/wired-awake-300719/>
- Smith, P., 2020. *Identity theft risks and cybersecurity best practices.*, s.l.: s.n.
- Johnson, R., 2019. *The social impact of financial data breaches: A case study of Capital One*, s.l.: Financial Security Review.
- Brown, K., 2020. Corporate negligence in cybersecurity: Lessons from major breaches. *Cybersecurity Journal*, pp. 45-60.
- Johnson, R., 2019. Ethics in IT security: The role of professionals in preventing data breaches. *Journal of Information Ethics*, pp. 78-92.
- Westin, A., 2020. Privacy and data protection in financial institutions. *Privacy Journal*, pp. 89-101.
- Anon., 2021. [Online]
Available at: <https://www.forbes.com/sites/zakdoffman/2021/12/24/capital-one-will-pay-190-million-to-settle-data-breach-lawsuit/>
- Anon., 2019. *The Verge*. [Online]
Available at: <https://www.theverge.com/2019/7/29/8934697/capital-one-data-breach-aws-cloud-server-hack>
- Anon., 2020. *United States Department of Justice*. [Online]
Available at: <https://www.justice.gov/usao-wdwa/pr/former-seattle-tech-worker-indicted-wire-fraud-and-computer-data-theft-connection>
- Anon., 2021. *BCS Code of Conduct*. [Online]
Available at: <https://www.bcs.org/membership/become-a-member/bcs-code-of-conduct/>
- Anon., 2018. *ACM Code of Ethics*. [Online]
Available at: <https://www.acm.org/code-of-ethics>
- Anon., 2024. [Online]
Available at: <https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement>
- Jessica Silver-Greenberg, M. G. a. N. P., 2014. [Online]
Available at: <https://archive.nytimes.com/dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/>
- Ma, A., 2019. [Online]
Available at: <https://www.businessinsider.com/capital-one-hack-data-breach-email-tip-off-2019-7>

Anon., 2019. *Former Seattle Tech Worker Indicted on Federal Charges for Wire Fraud and Computer Data Theft*. [Online]

Available at: <https://www.justice.gov/usao-wdwa/pr/former-seattle-tech-worker-indicted-federal-charges-wire-fraud-and-computer-data-theft>

Waldman, A., 2022. [Online]

Available at: <https://www.techtarget.com/searchsecurity/news/252521775/Paige-Thompson-found-guilty-in-2019-Capital-One-data-breach>

Shaharyar Khan, I. K. Y. H. S. M., 2022. *A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned*. [Online]

Available at: <https://dl.acm.org/doi/10.1145/3546068>

Sprintzeal, 2024. [Online]

Available at: <https://www.sprintzeal.com/blog/capital-one-cyber-incident>

Anon., 2019. [Online]

Available at: <https://www.bbc.com/news/world-us-canada-49177267>

Anon., 2019. [Online]

Available at: <https://www.bbc.com/news/technology-49175964>

Anon., 2019. [Online]

Available at: <https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html>

Anon., 2021. [Online]

Available at: <https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act>