



Module Code & Module Title

CS5071NT – Professional and Ethical Issues

Assessment Type

Milestone 2

Semester

2025 Spring

Student Name: Ayan Shrestha

London Met ID: 23049210

College ID: np05cp4a230075

Assignment Submission Date: Tuesday, April 29, 2025


Assignment Due Date: Tuesday, April 29, 2025

Submitted To: Ms. Enjina Ghimire

Word Count:2099

I confirm that I understand my coursework needs to be submitted online via Google Classroom 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 mark of zero will be award

23049210 Ayan Shrestha

 Islington College, Nepal

Document Details

Submission ID

trn:old::3618:93448222

Submission Date

Apr 29, 2025, 12:46 PM GMT+5:45

Download Date

Apr 29, 2025, 12:47 PM GMT+5:45

File Name

23049210 Ayan Shrestha

File Size

11.3 KB

8 Pages

1,823 Words

9,696 Characters







Page 2 of 11 - Integrity Overview

Submission ID trn:old::3618:93448222

4% Overall Similarity

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

Match Groups

-  **6 Not Cited or Quoted 2%**
Matches with neither in-text citation nor quotation marks
-  **3 Missing Quotations 2%**
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

- 0%  Internet sources
- 1%  Publications
- 3%  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.	Legal Issue	1
2	Professional Issue.....	4
3	Conclusion	7
4	References.....	8

1. Legal Issue

Legal Issue refers to the matter of taking place within the framework of law which requires resolution through legal process. This issue is a situation which involves and covers all of the legal principles rights or obligations that require the interpretation or application of the law.

A serious legal concern was triggered by the Capital One data breach of July 2019, which exposed sensitive information of over 106 million individuals. The compromised data (including credit applications, Social Security numbers, bank account details) enabled immediate risks from regulatory and litigation. Specifically, under the legal lens, the adequacy of Capital One's cybersecurity measures, the responsibility shared with Amazon Web Services (AWS), and the responsibilities to consumers and shareholders also came under public scrutiny. This situation set the stage for such investigations under consumer protection, financial or securities laws, and would subject Capital One to lawsuits and substantial financial penalties. (Lu, 2019)

- Negligence of data protection law

Capital One was cursed for failing with the proper use of security to protect the customer information which breaks the US. Federal Trade commission (FTC) rules requiring companies to protect consumer data. A criminal attacker gained unauthorized access to personal information stored at Capital One due to the bank's failure to adequately protect consumer personal information. The exposed sensitive data from the breach included names, addresses, Social Security numbers, and linked bank account numbers as well as credit scores of approximately 98 million U.S. residents. The class action lawsuit alleged that Capital One did not do enough to ensure that its personal information was safe, plaintiffs argued. (Capital One Settlement Administrator, 2022)

- Class-Action Lawsuit

Class action lawsuits filed by customers who were affected by the 2019 Capital One data breach were major civil legal issues. Capital One was careless and did not effectively protect people's private and financial information that put millions at risk of identity theft, they said. For that reason, Capital One agreed to pay \$190 million in 2021

to cover the customers' financial losses and other costs. Such lawsuits revealed that breaches of rules to keep customer data safe mean not only breaking the rules but also ending up on the hook for hefty civil penalties and legal actions. (The Seattle Times, 2021)

- **Obligation of Federal trade commissions (FTC) Act**

The 2019 Capital One data breach investigated Capital One under the Federal Trade Commission (FTC) Act because it apparently did not take basic security measures like requiring several factors for logins in orders from cyber security warnings of vulnerabilities in its cloud systems. Although the FTC didn't force a fine, the breach shows that a lack of cybersecurity doesn't necessarily lead to criminal punishment under consumer protection laws if companies exaggerate their services' security. For that reason, Capital One agreed in 2021 to pay \$190 million to settle with customers for financial losses and any related costs. The case also raises legal risks for companies under the FTC Act when security failures result in consumer harm (Capital One Financial Corporation , 2022)

- **Security Law Violations**

Capital One is a public company, so in theory anything serious would have to be brought to the attention of investors. It is required by the Securities Exchange Act of 1934. A company can get drawn into legal trouble with the U.S. Securities and Exchange Commission (SEC) if it ignores a potential problem such as a big data breach and fails to report to investors on time. In Capital One's case, Capital One was asked whether it shared the news with investors quickly and clearly enough after the data breach. That's a similar case that Yahoo had before it too where they were fined \$35 million for delaying investors on thinking about a large cybersecurity attack. Thus, reporting of such problems should be honest and fast. They could also be fined or subject to other legal actions if Capital One is found guilty of withholding or delaying the breach information. (Lu, 2019)

- Loss of work product privilege

Capital One hired a cybersecurity company called Mandiant to look into why the data breach occurred. Normally, under a rule called the Work Product Doctrine, reports like this would be kept secret because work done to prepare for lawsuits is protected. But the court did find that the report was not protected in the Capital One Consumer Data Security Breach Litigation (2020). Mandiant had already been doing the same sort of work for Capital One before the breach, part of their regular business. For this reason, the court directed Capital One to deliver the report to the ones suing it. Then this is a big legal problem for Capital One, because it tended to make their defence less strong and the other side more strong. (Heuer, 2020)

1 Professional Issue

A profession is generally understood to be a disciplined group of people with a special knowledge, skills which are acquired through extensive education and training, following a body of learning, generally recognized as a professional discipline, and which such profession follows ethical standards.. (Millett & Tapper, 2015), A professional is someone who uses his knowledge and skills in order to serve people, maintain high ethical standards, remains responsible, and acts for the growth of the society. Being a professional also involves honesty, keeping skills updated and gaining the public's trust. (Bowman, 2012).

The professional issue presented in 2019 by the Capital One data breach were about cyber security, confidentiality, accountability, and how ethical standards were being handled in employees, contractors, and management. As the professionals who deal with the protection of sensitive information they are supposed to follow the strict codes of ethics like ACME, BCS, IEEE. But that breach underlined that some security misconfigurations, some poor risk management and some poor professional responsibilities lead to a serious breach. (Lu, 2019)

- Failure in cloud security

Company face a lot of professional issue during the data breach. One of the professional issue in the capital one data breach was the improper configuration of firewall setting in the Amazon Web services (AWS). Due the misconfigurations, there was an unauthorized access to sensitive information which affected more than 100 million individuals. Even the professional for cloud security were not following the best and practices and did not properly test the access control. This is a serious failure in terms of professional competence and duty of care as evidenced by the ACM Code of Ethics (Principle 2.9) that states systems should be designed to be secure and robust, and the IEEE Code of Ethics (Clause 1) which stresses the importance of protecting the privacy and safety of the public. (Paula et al., 2020)

- Overdependence on compliance

Capital One's security strategy involved making security compliance checklists rather than making practical real world protection for customer data. Although, they followed the regulatory standards, they failed to deal with well known risks, such as SSRF vulnerabilities, implying a very big professional gap. However, if the critical are not addressed the policy of compliance will not be enough. It shows a lack of ethical responsibility to protect users from harm, according to the ACM Code of Ethics (Principle 1.2), the BCS Code of Conduct (Section 1), in which professionals are required to avoid actions that may harm (Paula et al., 2020)

- Fail to prioritize public safety

The professionals of the Capital One data breach did not do what they should do according to the IEEE Code of Ethics, which requires them to prioritize the welfare, health and safety of the public. Over 100 millions people personal information was exposed during the data breach including their social security and bank details. If proper cloud security configurations were in place and thorough risk management was performed then this huge exposure might not have occurred. Capital One set millions of people at risk by focusing its efforts to do more with business speed and cloud adoption, rather than fully securing the systems. (IEEE, 2024)

- Lack of effective incident response

lack of effective response to handle incidents was another large professional issue in the Capital One breach. In particular, the Capital One breach occurred in March 2019, but was not detected until months later — and Capital One waited to notify the public. When a breach occurs, professionals are ethically obligated to have strong system of detection and quick response actions as well as transparent communication. According to the IEEE Code of Ethics states that engineers shall acknowledge and correct errors promptly as far that error affects public interest. Capital One's slow and weak response actually allowed the attacker to access sensitive information and potentially misuse and causing more harm to the individuals that were affected.

- Insufficient Staff training and development

The Capital One breach brought to light one professional problem: a lack of continuous staff training and development. In accordance with the BCS Code of Conduct, IT professionals should commit to keeping their knowledge and skills up to date so that they are aware of new technologies, risks, and security practice. In Capital One's case, it did not understand or defend against important security threats such as Server-Side Request Forgery (SSRF) attacks. That suggests that professionals who were tasked with securing cloud systems weren't adequately trained in the latest cybersecurity threats. Mistakes such as misconfiguring and delayed breach detection are more likely to occur without regular training. This indicates they did not fulfill the professional duties to keep up with competency and safeguard data for the public. (BCS, 2024)

2 Conclusion

The Capital One breach shows how important it is for companies to follow both the law and strong ethical values when handling a crisis. People who work with computers have a responsibility to use their skills to help society, not just their company. As Help Net Security (2018) explains, the **ACM Code of Ethics** reminds tech professionals that they must always think about the public good when making decisions. Companies should act early by setting strong cybersecurity rules and quickly informing people if something goes wrong. Doing this not only protects customers but also saves the company from big fines and loss of trust. If businesses ignore either the technical or ethical side of a problem, they could face serious financial and reputation damage.

If I were in that position, I would focus on being **open and honest** to reduce harm and keep data safe. Following the ACM Code, I would report any risks or system weaknesses as soon as I find them. As a leader, I would make sure the company's cloud security is properly set up and train employees to avoid mistakes that could cause breaches. I would also make sure that both the management team and customers are told clearly and quickly if a breach happens, explaining what it means for them. Every step I take would match legal rules and aim to protect society. In the end, I believe that mixing good technical work with strong ethics is the best way to protect people's trust and make the digital world safer.

3 References

- BCS. (2024) *BCS Code of Conduct* [Online]. Available from: <https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct>.
- Bowman, R. (2012) *Understanding What it Means to Be a Professional*. *Taylor & Francis*, Available at: <https://www.tandfonline.com/doi/abs/10.1080/00098655.2012.723641>.
- Capital One Financial Corporation. (2022) [Online]. Available from: <https://www.capitalonesettlement.com/Content/Documents/Amazon%20Answer.pdf>.
- Capital One Settlement Administrator. (2022) *Notice of Capital One Data Breach Class Action Settlement*. [Online]. Available from: <https://www.capitalonesettlement.com/Content/Documents/Notice.pdf>.
- Heuer, J. (2020) *Breach Report in Capital One Litigation Not Privileged*.
- IEEE. (2024) *IEEE Code of Ethics*. [Online]. Available from: <https://www.ieee.org/about/corporate/governance/p7-8.html>.
- Lu, J.J. (2019) *Assessing The Cost, Legal Fallout Of Capital One Data Breac*. *ResearchGate*, Available at: https://www.researchgate.net/publication/335210159_Assessing_The_Cost_Legal_Fallout_Of_Capital_One_Data_Breach.
- Millett, S. & Tapper, A. (2015) *Revisiting the Concept of a Profession*. *ResearchGate*, Available at: https://www.researchgate.net/publication/283112028_Revisiting_the_Concept_of_a_Profession [Accessed 28 April 2025].
- Paula, A.M.G.d., Neto, N.N. & Madnick, S. (2020) *A Case Study of the Capital One Data Breach* [Online]. Available from: <https://web.mit.edu/smadnick/www/wp/2020-07.pdf>.
- The Seatles Times. (2021) *Capital One to Pay \$190M Settlement in Data Breach* [Online]. Available from: <https://www.seattletimes.com/business/capital-one-to-pay-190m-settlement-in-data-breach-linked-to-seattle-woman/>.

