Assessment Task 1B: Ethics & Professional Conduct

Author's Name: XXX XXXX
Swinburne University of Technology
Melbourne, Australia
????????@student.swin.edu.au

This document aims to present and analyse ethics and professional conduct in the IT professional field trough the examination of a practical example from real life where the Australian Computer Society Code of Ethics is applied.

The analysis will begin with the description of one of the major cyber-attacks in the history of internet to a private IT company and then the document will address more specific areas in regards of which core ethical values were violated.

Early in 2014, Yahoo suffered a major cyber-attack which ended in the steal of one of its' databases that contained personal information of 500 million people [1], according to the FBI that played an important role during the investigation, the incident was originated due to a phishing attack performed towards a specific group of Yahoo employees, after installing a malware contained in the phishing emails sent, the hackers got access to Yahoo infrastructure and created a backdoor in a web server from where all the information was stolen [2]. The data base stolen contained relevant personal information such as: names, phone numbers, encrypted passwords, password challenge questions and answers [3]. Moreover, records related to 200 million users were published in the dark web available to anybody that would like to buy that information. Additionally, what makes this incident even more critical is the fact that the data stolen is usually used in different websites to create users or modify passwords, therefore not only the information that is stored in Yahoo email accounts could have been accessed but also accounts in different systems or websites could have been compromised. Almost two years after the incident took place, in December 2016, Yahoo made this publicly known to all users and investors. This cyber-attack and the release of the news long after brought many difficulties to the company, including legal actions that had a profound reputational and economic impact.

After understanding the incident and its' consequences, several ethical issues can be addressed on hacker's and victim's side, but the following lines will be focused in the actions performed by Yahoo. In that regards, the main ethical issue identified is that Yahoo knew about the incident since December 2014 but since the company was being purchased by Verizon at that time, they decided to not make the public announcement until December 2016, just 5 months after that both companies reached an agreement for the acquisition of Yahoo [4].

Since this is an IT Company, the main profession involved was IT and some specific fields can also be mentioned in regards of the ethical issue such as Information Security, Risks and IT Management, because of the lack of security controls and monitoring implemented in the IT infrastructure that allowed the attack to happened and then the poor risk evaluation performed in regards of the IT vulnerabilities and the decision to avoid making the announcement of the cyber-attack to investors and users.

In the last section of this document, a complete analysis of the case is performed to clearly understand the principles that were violated, for this purpose the ACS code of conduct presented in [5] and [6] was used as a reference.

1. The Primacy of the Public Interest: Since the company was in a purchasing process by Verizon, the public announcement should have been made before settling an economic agreement in July 2016 between both companies, but Yahoos' private interests took precedence and that action had consequences such as the fine imposed by the U. S. Securities and Exchange Commission [7].
   The values that were violated from the ACS Code of Conduct are the following.
   a. advise your stakeholders as soon as possible of any conflicts of interest or conscientious objections that you have
   b. endeavour to preserve the integrity, security, continuity and utility of ICT;
   c. endeavour to preserve the confidentiality and privacy of the information of others [6].
2. Honesty: Due to the breach of public trust of stakeholders known as users and investors known as Verizon that was purchasing Yahoo. In this regards, the values violated were the following:
   a. Not knowingly mislead a client or potential client as to the suitability of a product or service [6].
3. Competence: This principle is strictly related to the limitations and deficiencies found in the information security controls implemented in IT Yahoo services that allowed the attack to happened. The values violated were the following:
   a. endeavour to provide products and services which match the operational and financial needs of your stakeholders
   b. respect and protect your stakeholders' proprietary interests
   c. advise your stakeholders when you believe a proposed project, product or service is not in their best interest [6].
4. Professionalism: This is addressed for the lack of professional standards provided by the company that affected the integrity and privacy of users that were affected by the steal of personal information, additionally the lack of respect and dignity from this company to their users and investors. The values violated were the following:
   a. Refrain from any conduct or action in your professional role which may tarnish the image of the profession or detract from the good name of the ACS [6].

References

[1] S. Burke, "Yahoo's data breach explained" CNNMoney, September 23, 2016. [Online]. Available: https://www.youtube.com/watch?v=zRQTTQpCbUo [Accessed April 5, 2019].

[2] S. Gallagher, D Kravets, "How did Yahoo get breached? Employee got spear phished, FBI suggests", arsTechnica: https://arstechnica.com/tech-policy/2017/03/fbi-hints-that-hack-of-semi-privileged-yahoo-employee-led-to-massive-breach/, March 16, 2017, [Accessed April 6, 2019].

[3] S. Kovach, "FBI: Russian hackers likely used a simple phishing email on a Yahoo employee to hack 500 million user accounts", Tech Insider: https://www.businessinsider.com.au/fbi-yahoo-hackers-used-spear-phishing-email-gain-access-500-million-accounts-2017-3?r=US&IR=T, March 17, 2017, [Accessed April 6, 2019].

[4] J. Kastrenakes, "SEC issues $35 million fine over Yahoo failing to disclose data breach", The Verge: https://www.theverge.com/2018/4/24/17275994/yahoo-sec-fine-2014-data-breach-35-million, April 24, 2018, [Accessed April 7, 2019].

[5] Australian Computer Society, "ACS Code of Ethics", ACS: https://www.acs.org.au/content/dam/acs/acs-documents/Code-of-Ethics.pdf, April 6, 2014. [Accessed April 3, 2019].

[6] Professional Standard Board - Australian Computer Society, "ACS Code of Professional Conduct", ACS: https://www.acs.org.au/content/dam/acs/acs-documents/ACS%20Code-of-Professional-Conduct_v2.1.pdf, April 6, 2014. [Accessed April 3, 2019].

[7] U. S. Securities and Exchange Comission, "Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million" https://www.sec.gov/news/press-release/2018-71, April 2018. [Accessed April 7, 2019].