Analysis of the Equifax Data Breach ethical impact

Tangina Parvez

Master of Business Analytics, Hult International Business School

Data Management & SQL - DAT-5486 - FMBAN1

Instructor: Professor. Chase Kusterer

Submission: 12-26-2022

"Companies that profit from personal information have an extra responsibility to protect and secure that data," said FTC Chairman Joe Simons. And "Equifax failed to take basic steps that may have prevented the breach that affected approximately 147 million consumers with approximately 209,000 consumers' credit card numbers breached."

Analysis of the Equifax Data Breach ethical impact

Introduction – Ethical dilemma and cybersecurity

This paper aims to analyse the cybersecurity incidents concerning Equifax and consider incident management processes that may help to prevent cyber threats. Information Technology (IT) assets are critical assets of the company that comprises operational IT assets, IT systems, or repositories used to collect and store valuable business data and customer data. The revolutionized IT system and information-sharing capabilities have changed how we work and communicate, including internal communication, and created various risks and ethical dilemmas. The main ethical issues created by the advancement revolve around privacy, accuracy, and accessibility of data (Reynolds, 2012, p. 38). On the other hand, Mason added another to the list of ethical issues, namely, property, i.e., who has the ownership of the information? The dilemma of privacy concerns how much information is necessary for businesses and how much they should be allowed to retain. Whereas the accuracy of information needs to be verified, who is responsible for the authenticity, and who is responsible if the information is not accurate? Accessibility is related to privacy but from the perspective of the organization, i.e., what are the rights of the organization to collect and store information, and what standards would apply to them to safeguard the information (Mason, R. O., 1986). The purpose of outlining the dilemmas relates to providing an impromptu reference of the complexity around data collection and data safety. On the other hand, it is vital to look at information security models to assess the level of safeguards necessary. For instance, the CIA triad is a theory that IT assets may be compromised in three ways: confidentiality (compromising the information), integrity (compromising the system), and availability (compromising the system by denying others access). Chai, W. (2022).

Cause and effect of Equifax Breach

Equifax, a credit reporting agency that collects personal and financial information of individuals to generate financial credit reports, was subject system breach. The breach resulted in 147 million individuals' personal and financial information being stolen (Thomas, Jason. 2019). The failure of implementing a security patch to a vulnerability, CVE-2017-5638, that affected a component of Struts called the Jakarta Multipart parser gave hackers access to the Equifax website, particularly the online dispute portal. The hackers opened a simple backdoor known as a web shell because the systems were not adequately segmented from one another. They could access different machines, databases, files, etc. The hackers had access to the system for four months, which allowed them to amass data of 147 million individuals and take the information of specific individuals (Kara. 2021). On September 8, 2017, Equifax released a statement that it had been a victim of a cyberattack resulting in a massive data breach (Rajna, 2018) and later settled to pay compensation to its consumer (Leonhardt, M. 2019). The consequences of the data breach will affect the customers whose sensitive information is stolen, and identity thieves may use this information to commit crimes and fraud, such as applying to open bank accounts, applying for credit, or getting driver's license, and destroy one's financial standing and reputation.

The seriousness of the Equifax breach relates to a credit bureau that has access to billions of personal and financially sensitive information and failed to affectedly address the vulnerability by failing to install necessary patches, renew an encryption certificate on one of their internal security tools, segregate critical IT assets, and failed to notice the presence for four months. Further, the breach is one of the largest in the world that comprises the personal and financial information of nearly half the population of the United States. Lastly, the failure of company had to properly and responsibly deal with the crisis because it delayed its response and poorly managed the crisis, including setting up a separate domain that was flagged by various browsers as a phishing threat, and its top executives

were accused of insider trading. Though it is important to mention here that forensic investigations suggested the stolen information has not been found that points towards state-sponsored cyberattack.

The credit reporting agencies, as a bureau with the responsibility to collect, store and analyse the financial and personal information of the individuals had higher ethical responsibility to protect the individual's information, such as, financial products available to any individual would depend on the reports and this information would not be available to any other businesses. Therefore, from the ethical implication, the company has failed to protect the privacy of the individuals, whereas they held the most sensitive information of an individual. Consequently, affected individuals have less access to financial products and lost access to their personal proprietary information without any fault of their own.

Current assessment and recommendations

After the Equifax breach, the government has taken some steps to protect the consumers, including creating regulations, requiring data holders to inform consumers of data breaches, and passing the Economic Growth, Regulatory Relief, and Consumer Protection Act (Thomas, J. 2019). However, further responses were due to address the concerns of the consumers, such as empowering Federal Trade Commission with more powers to deal with national security concerns and having provisions recognizing the fiduciary duty of the credit reporting agencies (Kalia, A. 2017). Moreover, there is no federal data protection legislation in the United States, in contrast to the General Data Protection Regulation (GDPR) in the European Union that stipulates specific rules, norms, and compliance regarding dealing with personal information. Nonetheless, the most important aspect of data protection is internal rules and policies to avoid or reduce the risks of attacks. At the time of more work-from-home/remote working policies, the management of cyber-attack risk becomes more imminent. It is suggested that critical information infrastructure must adopt the National Institute for Standards and Technology (NIST) framework to identify critical assets, apply techniques for protection, adopt recovery plan in times of crisis and investigation of the incident, and based on

outcome of investigation adopt measure to prevent future incidents. Other measures may include following the principle of least privilege, i.e., users and computer systems should be given only the access they need to do the job, and defensive control such as encryption, firewall, and antivirus protection. Endpoint detection and response (EDR) and security operation centres.

Tables

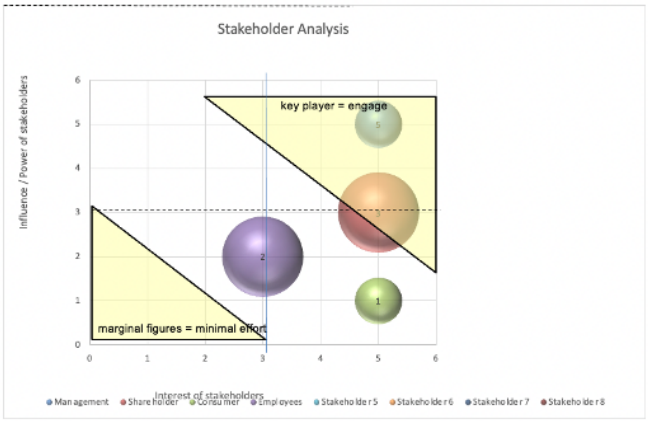
Student Name: Tangina Parvez

Stakeholder Analysis 1

Adapted from www.freepmtools.com

"The stakeholder analysis is an instrument to illustrate and to discover different needs of different stakeholders of particular companies"

	Stakeholder	Interest of stakeholders [0;5] - [0=small; 5=big]	Influence/Power of stakeholders [0;5] - [0=small; 5=big]	Preferences (possitive / negative) [1;3;5] - [1=pos; 3= neutral; 5= neg]
1.	Management	5	5	1
2.	Shareholder	5	3	3
3.	Consumer	5	1	1
4.	Employees	3	2	3
5.	Stakeholder 5			
6.	Stakeholder 6			
7.	Stakeholder 7			
8.	Stakeholder 8			



References

Ethics in information technology : Reynolds, George Walter, 2012 - : Free Download, Borrow, and Streaming : (n.d.-b). Internet Archive. https://archive.org/details/ethicsininformat0000reyn/page/n9/mode/2up

Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach. (2021, September 18). Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach

Mason, R. O. (1986). Four Ethical Issues of the Information Age. MIS Quarterly, 10, 5-12. http://dx.doi.org/10.2307/248873

Chai, W. (2022, June 28). confidentiality, integrity, and availability (CIA triad). WhatIs.com. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Thomas, Jason. (2019). A Case Study Analysis of the Equifax Data Breach 1 A Case Study Analysis of the Equifax Data Breach. 10.13140/RG.2.2.16468.76161.

https://www.researchgate.net/publication/337916068_A_Case_Study_Analysis_of_the_Equifax_Data_Breach_1_A_Case_Study_Analysis_of_the_Equifax_Data_Breach

Hearing on "Oversight of Equifax Data Breach: Answers for Consumers" Before the Subcomm. On Digital Commerce and Consumer Protection of the H. Comm. on Energy and Commerce, 115th Cong. (October 3, 2017). https://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf (prepared testimony of Richard F. Smith, former Chairman, and CEO, Equifax).

Kara. (2021, April 30). Case study: Equifax data breach. Seven Pillars Institute. https://sevenpillarsinstitute.org/case-study-equifax-data-breach/

Rajna, G. (2018). *Equifax Data Breach. viXra. Retrieved*. Vixra. http://vixra.org/pdf/1808.0215v1.pdf

Leonhardt, M. (2019, July 23). *Equifax to pay $700 million for massive data breach. Here's what you need to know about getting a cut*. CNBC. https://www.cnbc.com/2019/07/22/what-you-need-to-know-equifax-data-breach-700-million-settlement.html

Leonhardt, M. (2019b, July 23). *Equifax to pay $700 million for massive data breach. Here's what you need to know about getting a cut*. CNBC. https://www.cnbc.com/2019/07/22/what-you-need-to-know-equifax-data-breach-700-million-settlement.html

Bloomberg - Are you a robot? (n.d.-b). https://www.bloomberg.com/tosv2.html?vid=&uuid=70fdd132-8560-11ed-bbc2-574c58597172&url=L25ld3MvYXJ0aWNsZXMvMjAxNy0wOS0wNy90aHJlZS1lcXVpZmF4LWV4ZWN1dGl2ZXMtc29sZC1zdG9jay1iZWZvcmUtcmV2ZWFsaW5nLWN5YmVyLWhhY2s=

Thomas, J. (2019, December 13). *A case study analysis of the equifax data breach 1 A case study analysis of the equifax data breach*. Unknown. https://www.researchgate.net/publication/337916068_A_Case_Study_Analysis_of_the_Equifax_Data_Breach_1_A_Case_Study_Analysis_of_the_Equifax_Data_Breach

Kalia, A. (2017, November 7). *Here's how Congress should respond to the equifax breach*. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2017/11/heres-how-congress-should-respond-equifax-breach

Cybersecurity framework. (2013, November 12). NIST. https://www.nist.gov/cyberframework

Choosing the best cyber security solution for your organization - ITSM.10.023. (n.d.). Canadian Centre for Cyber Security. Retrieved December 26, 2022, from https://cyber.gc.ca/en/guidance/choosing-best-cyber-security-solution-your-organization-itsm10023