CYBERSECURITY AND MANAGEMENT'S ETHICAL RESPONSIBILITIES: THE CASE OF EQUIFAX AND UBER

James Rasalam, Valdosta State University
Raymond J. Elson, Valdosta State University

CASE DESCRIPTION

The primary subject matter of this case concerns ethical decision making. The case has a difficulty level of four, appropriate for senior level. The case is designed to be taught in one class period of approximately 50 -75 minutes and is expected to require 2-3 hours of outside preparation by students.

CASE SYNOPSIS

Protecting sensitive customer data and company information has proven to be problematic for some companies. As a result, companies across all industries must be alert to security vulnerabilities that leave them exposed to hackers. This is best illustrated by Equifax, a credit reporting bureau, and Uber, a ride-sharing company, that disclosed data breaches to the public in 2017. These cyber-attacks were far-reaching, with the Equifax breach affecting approximately 145 million customers and the Uber attack affecting 57 million customers and drivers. Management of both companies delayed notifying the public of the data breach on a timely basis and corporate executives may have benefited financially from this inaction. This raises the question as to management's ethical responsibility after experiencing a cyber-attack.

The case study focuses on the actions taken by company management to address the respective data breaches. It does not address steps that could be taken by the companies to reduce cybersecurity risk. Students are asked to use the normative, deontological, and consequentialism ethical theories to assess managements' responses to the cyber-attacks.

INTRODUCTION

When an organizational crisis occurs, management must navigate the tumultuous times by making appropriate business and ethical decisions while often only having a limited amount of information. However, there are examples of when these decisions are questioned by the public, especially when there is a lack of transparency or accountability. Companies are now facing new and evolving risks and those charged with governance are challenged to manage them effectively.

Equifax, the credit reporting company, and Uber, the ride-sharing company, were criticized for the way in which management responded to data breaches that resulted in the exposure of millions of customers' records to hackers. Although those charged with governance may have fulfilled their legal responsibilities, this may not be true from an ethical perspective. A look at each data breach and managements' actions might help to shed some light on whether the ethical responsibilities were satisfied.

EQUIFAX

Credit Reporting Regulations

Credit reporting companies are those that gather credit information from numerous sources, which is then sold to customers. These companies must follow the regulations provided in the Fair Credit Reporting Act (FCRA), the goal of which is to promote the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FCRA also includes provisions that allow consumers to seek damages from violators, even if it is a credit reporting bureau.

Company Information

The Retail Credit Company (RCC) was founded in 1899 and was renamed Equifax in 1976. RCC began its operations by gathering customers' information, such as recording the length of time a customer took to make a payment after a purchase had been made. This information is helpful to businesses in determining the creditworthiness of customers and in estimating the allowance for doubtful accounts within the balance sheet. RCC received this information from individual merchants for free, but after compiling the data, could sell the information back to all the merchants for a profit. However, over time, RCC increased the scope and amount of data collected per customer to include customers' personal information, even if it was a rumor and inaccurate, within its publications. This caused the Federal Trade Commission to investigate the RCC.

Equifax is now a publicly traded, global information solutions company that uses unique data, innovative analytics, technology and industry expertise to power organizations and individuals around the world by transforming knowledge into insights that help make more informed business and personal decisions.

The company employs approximately 10,400 employees worldwide and collects and maintains data on more than 820 million consumers and 91 million businesses.

The Data Breach and Management's Response

Equifax's management discovered a data breach had occurred in its system on July 29, 2017 that affected approximately 145.5 million Americans citizens, 700,000 United Kingdom residents, and 8,000 Canadian citizens. The company disclosed the breach to the public on September 7, 2017. In its disclosure, the company noted that the breach was caused by hackers who exploited a vulnerability within its software. The public disclosure resulted in the stock price plummeting by 34.85% to $92.98 by September 15, 2017.

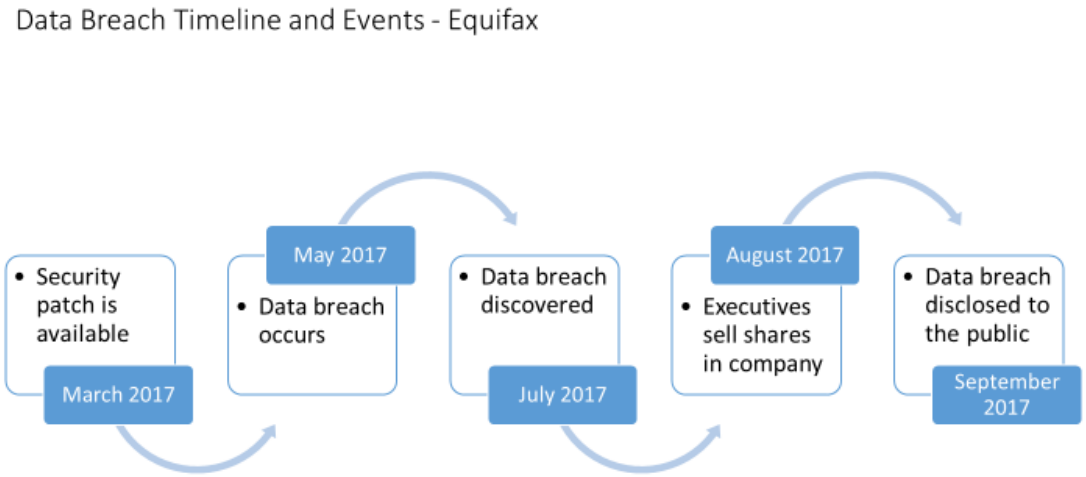
The data breach occurred over a two-month period beginning on May 13, 2017 until its discovery on July 29, 2017. The hackers were able to access consumer information such as names, social security numbers, birth dates, addresses, driver's license numbers, and credit card information. Two months prior to the breach, on March 8, 2017, Equifax's management and the management of other companies were informed by the Computer Emergency Readiness Team of the Department of Homeland Security that there was a need to patch a data storage software vulnerability. This was extremely important since the failure to address this specific vulnerability was analogous to leaving the backdoor to one's house wide open for thieves to easily enter.

Equifax management sent the notice to the information technology department, but the patch was never implemented. From the moment this patch was made available in March, until the breach was discovered in July, Equifax's information security department had been periodically

inspecting the system using prescribed protocols, such as running scans. Bottom line, however, Equifax failed to detect the vulnerability that had not been fixed by the information technology department and failed (for six weeks) to detect the unauthorized access by the hackers.

The Chief Executive Officer (CEO) noted that the reason for the forty-day delay in notifying the public was to determine the scope of the attack, which required time. This was accomplished through an independent investigation conducted by cybersecurity forensic consulting firms. After the scope had been determined, the firms advised that once the knowledge of the breach was made public, other hackers would also be notified of the possibility of gaining access to the system and may attempt to do so. To prevent this situation, Equifax took additional time to reinforce the system. Also, Equifax's management notified the Federal Bureau of Investigation of the breach.

The following diagram provides a timeline of the data breach and subsequent actions:



After the breach was discovered, but before it was disclosed to the public, four senior executives, including the Chief Financial Officer, cumulatively sold company shares valued at $1.8 million. These executives were allegedly not aware of the existing data breach at the time of the sale transactions. A special committee of independent directors supported by independent counsel was created to determine the legitimacy of these transactions. The committee reviewed supporting documents and conducted interviews to gather corroborative evidence. It exonerated the executives from any wrongdoings and concluded that the transactions were properly approved, followed company policy, and were not insider trading.

However, in a separate action, the chief information officer sold shares valued at approximately $1 million prior to Equifax notifying the public about the data breach. Executive management and the board of directors deemed this transaction as inappropriate and notified the Securities and Exchange Commission and the United States Justice Department.

UBER

Company Background

The company presently known as Uber was originally called UberCab when it was founded in San Francisco, California in 2009. The premise behind the company's business model is to allow a customer to request a car using a smartphone app, which uses the phone's GPS to send the closest driver to the customer's location. The idea for this service came about from the need to quickly find a ride given the limited number of taxi cabs in the area. The San Francisco Municipal Transit Authority (SFMTA) had a maximum limit to the total number of taxi drivers allowed in the city. Even if demand exceeded supply, no more than 1,500 licenses to operate taxis within the city would be awarded.

Due to the nature of the ride-hailing service, UberCab caused turmoil with the taxi industry, government regulators, and its own drivers. The taxi drivers and regulators were concerned that UberCab did not pay the same license fees as similar companies. SFMTA and the California Public Utilities Commission sent "a cease-and-desist letter" to UberCab's CEO, who subsequently changed the company's name to Uber by removing the word Cab. Thereafter, Uber continued to provide services in San Francisco and then began a global expansion.

Uber operates on a simple mission: to bring transportation to everyone, everywhere. It does so through an organization that spans approximately 78 countries and 600+ cities worldwide. All of this is achieved with over 16,000 employees as of 2017. The company reported having 75 million riders and 3 million drivers with 4 billion trips completed worldwide in 2017. It averages approximately 15 million trips completed each day.

Uber, a private company, is currently governed by an 11-person board of directors. They are supported by a 16-person executive management team, each delegated with the authority to manage various aspects of the organization.

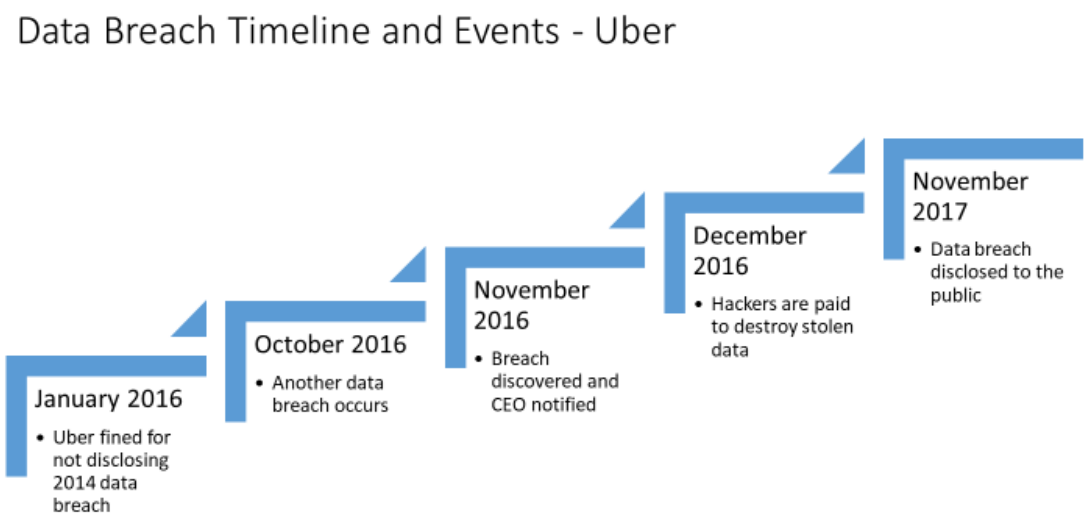
The Data Breach and Management's Response

Uber's management discovered a data breach had occurred in its system that affected approximately 57 million customers and 600,000 Uber drivers. The breach was caused when two hackers identified codes that included Uber employees' usernames and passwords within a database owned and secured by a third-party organization. Uber personnel had erroneously entered this security information that could then be used to access the company's database.

Uber utilized a program called "bug bounty," which is a common practice in the technology industry, to detect and correct vulnerabilities in its information system. This program works by allowing hackers, external to the company, to attempt finding vulnerabilities within the entity's system. Then, after showing the system weaknesses to the company's management, hackers can be paid up to $10,000 for their findings. However, in this case, one of the hackers demanded a $100,000 payment after gaining access to the system and retrieving over 57 million records. The hacker also threatened to publicly disclose the stolen information if the payment was not received. Uber's management paid the hacker $100,000 and decided to have the hacker sign a non-disclosure agreement, which stated that the hacker would keep the information private and destroy the data. It is worth noting that the payment was made despite the Federal Bureau of Investigation's 2016 warning to companies not to make such payments to hackers.

This breach occurred in October 2016 and was disclosed to the public in November 2017, which is over a year later. However, the company's CEO was notified of the data breach in November 2016. Information obtained in the breach included phone numbers, email addresses, and names of Uber customers, and the license numbers for many of the company's drivers. After realizing the breach had occurred, Uber's CEO and management chose not to disclose the data breach to the public, regulators, nor to its own board of directors. Prior to this, the company had experienced a data breach in 2014 and was fined $20,000 by the State of New York in January 2016 for failing to disclose the matter in a timely manner.

The following diagram provides a timeline of the data breach and its aftermath:



The board was not aware of the data breach until it began to lose confidence in the chief security officer's (CSO) performance. It hired a law firm to investigate the CSO; the breach was discovered during this process and subsequently disclosed to the public. The CSO and legal director of security and law enforcement were both fired, while the CEO resigned and became a member of the board of directors.

DISCUSSION QUESTIONS

Students should be able to:

1. Use the normative, deontological, and consequentialism ethical theories to evaluate managements' responses to the respective cyberattacks.
   [**Note to Students**: The table provided in Appendix A should be used to formulate responses Information on ethical theories can be found in the ethics chapter of an auditing textbook or on the Internet. One suggestion is https://owlcation.com]

2. Comment on which organization responded to the cyber-attacks in a more ethical manner (based on Appendix A).

		Evaluation of Management's Ethical Response	
Ethical Theories	**Brief Summary of the Theory**	**Equifax**	**Uber**
(a) Normative or virtue-based (Aristotle)	Emphasizes the importance of developing good habits of mind and character. These are often formed when young and includes wisdom, courage, honesty, temperance, and justice.		
(b) Deontological or duty-based (Kant)	The morality of an action should be based on whether the action itself is right or wrong under a series of rules For instance, we should always treat people with dignity.		
(c) Consequentialism	Moral conduct is determined solely by a cost-benefit analysis of an action's consequences. Therefore, an action is morally right if the consequences of that action are more favorable than unfavorable.		

Appendix A

REFERENCES

A summary of your rights under the Fair Credit Reporting Act. Retrieved from https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf

Anonymous, (2018, April 12). Uber agrees to 20 years of cybersecurity audits after FTC raises concerns. Retrieved December 22, 2018 from https://lifars.com/2018/04/uber-agrees-20-years-cybersecurity

Auchard, E. (2017, October 11). *British MP asks why Equifax delayed notifying UK data hack victims*. Retrieved February 22, 2018 from https://finance.yahoo.com/news/british-mp-asks-why-equifax-164424428.html

Blystone, D. (2018, February 16). *The Story of Uber*. Retrieved April 3, 2018 from https://www.investopedia.com/articles/personal-finance/111015/story-uber.asp

Bosa, D., & A. Balakrishnan (2017, December 1). *3 top Uber managers resign amid backlash from data breach and Waymo lawsuit revelations*. Retrieved April 3, 2018 from https://www.cnbc.com/2017/12/01/3-top-uber-mangers-resign-after-data-breach-lawsuit-hearing.html.

Cowley, S. (2018, March 14). *Ex-Equifax Executive Charged with Insider trading tied to '17 breach*. Retrieved April 10, 2018 from https://www.nytimes.com/2018/03/14/business/equifax-executive-insider-trading.html

2017, November 3. *Equifax Board Releases Findings of Special Committee Regarding Stock Sale by Executives*. Retrieved February 27, 2018 from https://investor.equifax.com/news-and-events/news/2017/11-03-2017-124511096

Equifax. Retrieved February 22, 2018 from https://www.equifax.com/about-equifax/*Fair Credit Reporting Act*. 15 U.S.C. § 1681 et seq.

Federal Trade Commission. (2017, January 19). *Uber Agrees to Pay $20 Million to Settle FTC Charges That It Recruited Prospective Drivers with Exaggerated Earnings Claims*. Retrieved March 31, 2018 from https://www.ftc.gov/news-events/press-releases/2017/01/uber-agrees-pay-20-million-settle-ftc-charges-it-recruited

Hartmans, A. (2018, January 18). *Travis Kalanick's final months as Uber CEO reportedly included squirming on the floor 'on his hands and knees' and offering the driver he yelled at $200,000*. Retrieved March 31, 2018 from http://www.businessinsider.com/how-travis-kalanick-behaved-in-final-months-as-uber-ceo-report-2018-1

Hendry, E. (2017, October 3). *How the Equifax hack happened, according to its CEO*. Retrieved February 22, 2018 from https://www.pbs.org/newshour/nation/equifax-hack-happened-according-ceo

Isaac, M., Benner, K., & S. Frenkel (November 21, 2017). *Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data*. Retrieved April 3, 2018 from https://www.nytimes.com/2017/11/21/technology/uber-hack.html

Kolhatkar, S. (2018, April 9). At Uber, a new C.E.O. Shifts Gears. Retrieved April 27, 2018. https://www.newyorker.com/magazine/2018/04/09/at-uber-a-new-ceo-shifts-gears

Larson, S. (2017, November 17). *Uber's massive hack: What we know*. Retrieved April 1, 2018 from http://money.cnn.com/2017/11/22/technology/uber-hack-consequences-cover-up/index.html

Larson, S. (2017, November 22). *Uber paid hackers $100,000 after they stole data on 57 million users*. Retrieved February 22, 2018 from http://money.cnn.com/2017/11/21/technology/uber-hacked-2016/index.html?iid=EL

McCrank, J. (2017, October 10). *Equifax says 15.2 million UK records exposed in cyber breach*. Retrieved February 22, 2018 from https://www.reuters.com/article/us-equifax-cyber/equifax-says-15-2-million-uk-records-exposed-in-cyber-breach-idUSKBN1CF2JU.

Moyer, L. (2017, November 3). *Equifax special committee says executive stock sales were in the clear*. Retrieved April 27, 2018 from https://www.cnbc.com/2017/11/03/equifax-special-committee-says-executive-stock-sales-were-in-the-clear.html.

Newcomer, E. (2017, November 21). *Uber Paid Hackers to Delete Stolen Data on 57 Million People*. Retrieved April 1, 2018 from https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data

Osborne, C. (2016, January 7). *Uber fined $20K in data breach, 'god view' probe*. Retrieved April 3, 2018 from https://www.cnet.com/news/uber-fined-20k-in-surveillance-data-breach-probe

Perlroth, N. & M. Isaac (2018, January 12). *Inside Uber's $100,000 Payment to a Hacker and the Fallout*. Retrieved April 3, 2018 from https://www.nytimes.com/2018/01/12/technology/uber-hacker-payment-100000.html

Popken, B. (2017, September 15). *Equifax Execs Resign; Security Head, Mauldin, Was Music Major*. Retrieved February 27, 2018 from https://www.nbcnews.com/business/consumer/requifax-executives-step-down-scrutiny-intensifies-credit-bureaus-n801706

Puzzanghera, J. (2017, September 26). *Equifax CEO steps down after data breach; he'll still get $18-million pension*. Retrieved April 27, 2018 from http://www.latimes.com/business/la-fi-equifax-ceo-20170926-story.html.

Rainone, C. (2014, July 9). *Uber: What you need to know about the car service app*. Retrieved March 31, 2018 from https://www.nbclosangeles.com/news/tech/Uber-Ride-Sharing-Taxi-surge-pricing-cab-booking-266414691.html.

Reese, K. (2006, March 11). *Equifax*. Retrieved February 5, 2018 from http://www.georgiaencyclopedia.org/articles/business-economy/equifax.

Roberts, C. (2018, March 28). *Lawsuit: SF let Uber and Lyft kill taxi cabs, and stuck credit union with the bill*. Retrieved March 31, 2018 from https://sf.curbed.com/2018/3/28/17174108/san-francisco-sfmta-taxis-cabs-uber-lyfe-industry-credit-union

Tysiac, K. (2018, February 21). *SEC publishes new requirements for cybersecurity disclosures*. Retrieved April 1, 2018 from https://www.aicpa.org/content/jofa-home/news/2018/feb/sec-cybersecurity-disclosures-201818424.html

What is a credit reporting company? (2017, May 25). Retrieved February 5, 2018 from https://www.consumerfinance.gov/ask-cfpb/what-is-a-credit-reporting-company-en-1251/