A Care Ethics Analysis of the Equifax Data Breach

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Kaitlin Phan

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor
Benjamin Laugelli, Department of Engineering and Society

Introduction

The Equifax data breach was one of the most significant cyberattacks of 2017. The attack's effects were significant, affecting millions of people and multiple businesses and agencies. The breach occurred after Equifax security officials failed to install a software upgrade that had been recommended to seal off digital intruders from obtaining access to information for over 140 million American consumers. The information accessed includes names, Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers; credit card information for approximately 209,000 consumers was also stolen, as well as certain dispute documents with personally identifying information for approximately 182,000 consumers (Primoff & Kess, 2017).

Previous case studies of the Equifax data breach focus on the technical shortcomings of the security team and the subsequent mishandling of public relations by leadership. However, by viewing the factors as individual faults rather than understanding it to be a related, collective issue, we pose the risk of continuing to embody these issues in our engineering teams and practices.

I believe that examining the Equifax data breach case using care ethics will provide a better analysis of how the social dynamics of the employers and employees of Equifax were unacceptable, leading to the failure. Specifically, I will show that the employers have a relationship with the employees and this relationship has three certain obligations of care not met on either sides: competency, service orientation, and project management skills. In this analysis, I will utilize evidence from the Congressional reports about the data breach and news articles about the investigation following the breach.

Background

The Equifax data breach resulted from a known vulnerability in the Apache Struts server software that had been announced in early March 2017. According to former Equifax CEO Richard Smith's congressional testimony on October 3rd, 2017, the company was notified of the available patch on March 8th, with an internal email being sent out instructing the IT staff to apply the patch within 48 hours the following day (Committee on Energy and Commerce, 2017). Equifax apparently didn't apply the patch until its online dispute portal had been compromised three months later, after which there was a five-week delay in reporting the data loss to the public. At this point, it had been approximately six months since the announcement of the vulnerability and availability of the patch. Then Equifax upset people even further by requiring consumers that in order to sign up for their free one-year credit monitoring service—which was necessitated by a data breach resulting from their own incompetence—you had to agree to a forced arbitration clause, forfeiting your rights to sue the company for any harm you might suffer (Berghel, 2017).

Literature Review

Many investigative articles and research have been released analyzing Equifax's data breach. Several scholarly sources have investigated how human error and technological failures led to Equifax's data breach and its subsequent ramifications among the political and technical communities. However, scholars have not adequately considered how Equifax's design team and their social dynamics played a role in the failed design and execution of Equifax's site.

In *Apache Struts 2: how technical and development gaps caused the Equifax Breach*, the causes to the data breach are analyzed, including discussion about the Apache Struts vulnerability (Luszcz, 2018). Luszcz even went as far as saying that Equifax and other companies should re-examine their development processes for openings that let vulnerabilities in. These development gaps, he proposes, can be closed by implementing better security practices and instituting security policies into engineering planning and processes. While there is a proposal on what can be improved on in the future, this is generalized to all companies (specifically geared towards tech teams) and fails to note the social integrity of the company behind the design.

Similarly to Luszcz, in *Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform*, Smith & Mulrain (2018) examined factors that contributed to the breach, and political implications of the breach in terms of company law and policies. Smith & Mulrain noted Equifax's lack of patch management diligence and lackluster response to multiple sources recommending them to apply the patch to address a known vulnerability was specifically responsible for the attack, agreeing with Luszcz's analysis. However, they additionally looks into national security implications and the impacts on the current legal regime, recognizing the dangers to society and the government liability as well (Smith & Mulrain, 2018). Again, while this article considers factors beyond the technical, it focuses more on the government implications of the data breach and future policy action, rather than delving into the social arrangements made by Equifax as a company specifically.

Both sources made a point to analyze what technical issues caused the data breach to happen with the Apache vulnerability and the Equifax security team, how it was handled by Equifax leadership, and what the consequences were among the public and government. While it is important to understand what happened to learn from past mistakes, I will further investigate how Equifax's design team and their social collective configuration created a site that allowed hackers to exploit its vulnerabilities. This design, made from a team that did not meet expected social norms in the engineering workplace, allowed for a flawed system to be deployed.

Conceptual Framework

My analysis of the social dynamics of the Equifax company draws on the care ethics framework of social norms of engineering which allows me to focus on the organizational norms and group processes at Equifax rather than the individual values of each engineer. Care ethics is the ethical theory that emphasizes the importance of relationships, which are coupled to special responsibilities and moral obligations (van de Poel & Royakkers, 2011). People are connected to each other and feel responsible for each other, resulting in care. Good care is one that involves compassion and attention. While most approaches to engineering ethics focuses on the individual, these neglect the relationships with others that engineers enter in through their work and are morally relevant.

Devon (1999) argues that “the more appropriate units of analysis in engineering ethics are collective configurations such as the engineer’s workgroup”. Instead of viewing ethics as a tension between the morality of the individual and the practices of society, from a care ethics view it is suggested that the focus should be shifted to the tension between the ideal and the actual norms and structures that characterize group processes and social institutions. In this case, I am focusing on a form of care ethics known as social ethics of engineering, which is an approach that focuses on the social arrangements rather than individual decisions, so long as they meet certain procedural norms (van de Poel & Royakkers, 2011).

I will use Devon's norms of engagement for the participation of engineers in group processes (involving both engineers and non-engineers) as a standard for creating an ideal design team. The norms are listed below:

1. Competency
2. Cognizance
3. Democratic information flows
4. Democratic teams
5. Service orientation
6. Diversity
7. Cooperativeness
8. Creativity
9. Project management skills

Figure 1: Devon's Norms of Engagement

As noticed by van de Poel and Royakkers, these norms are similar to the virtues for morally responsible engineers, with the key difference being that these norms are more geared towards group level standards. Like the virtues, it is only deemed "acceptable" if the social arrangements of the group meet certain procedural norms (van de Poel & Royakkers, 2011).

For the purposes of the paper, I will assume that the Equifax design team demonstrates meeting the norms of engagement based on their past actions and traits that align with that norm. Through a social ethics analysis, I will compare instances of Equifax's social arrangements with respect to those of the ideal design team outlined by Devon: competency, service orientation, and project management skills.

Analysis

Equifax's lack of following the norms of engagement for how engineers and non-engineers should participate in group processes lead to the numerous data breaches the company faced. The failure to meet the norms for competency, service orientation, and project management skills ultimately led to the biggest data breach in 2017. This is shown by actions and descriptions of the Equifax team. Since all norms need to be met for a team's arrangements to be deemed acceptable, it logically follows that a group cannot be missing any of these norms. Equifax fails to meet three of these. Within this analysis, I will show how the Equifax company failed to meet each of the three norms, meaning their social arrangements are not acceptable for making moral engineering decisions.

Competency

In order to understand why Equifax's team failed to meet the competency norm, it is necessary to provide more history of security issues for Equifax. The major data breach in 2017 was not the first time Equifax faced hacking. Warnings prior to the data breach were issued well in advanced of that, as early as March 8th, 2017, when Cisco Systems and the US Department of Homeland Security's Computer Emergency Readiness Team following the Apache Foundation announced the vulnerability (Srinivasan et al., 2019). Earlier that month, Equifax faced a separate breach, in which the company notified a small number of banking customers and brought in a security firm to assist its investigation into the breach (University of Texas McCombs School of Business, n.d.). Even earlier, in December 2016, a security researcher had examined Equifax's servers and warned the company that its system was vulnerable to the kind of hack that would later occur in 2017. Equifax eventually patched this vulnerability, but only after the mid-2017 breach had taken place. Upon investigation by an independent cybersecurity team after the mid-2017 breach, other security flaws were also found (University of Texas McCombs School of Business, n.d.). All of these separate instances come together to present a collective larger issue of incompetency.

As Devon defines competency, it means an engineer must be able to realize an effective product, and there must be ways to assess the competency (degrees, licenses, and references), and of checking the work of any engineer for errors. As mentioned above, several researchers with qualifications called out Equifax to fix a problem that had been discovered, which they never got around to patching despite these warnings. Based on this series of inaction by Equifax, the team is remiss in their work and duty towards a safe, secure product, and is thus not demonstrating competence by not listening to licensed professionals' advice about errors that had been made that had the potential to be dangerous, especially for a product of that scale.

However, it is important to acknowledge that the security team at Equifax did conduct a scan to see if the vulnerability existed in the system (Committee on Energy and Commerce, 2017). The scan failed to detect the Apache Struts vulnerability within Equifax's environment where they were running the application on. Some might think that the software used for scanning was simply ineffective or out of date so it was unable to detect certain new vulnerabilities, despite Equifax's due diligence in conducting the necessary scan. However, I would argue this further proves the lack of competence of the Equifax team. If the scanning software wasn't updated or properly patched to detect the vulnerability, that would suggest that the IT and security teams behind the software lacked knowledge about the software that they should have possessed and was negligent. As Devon (1999) mentioned, engineers are responsible for "the appearance of new competencies for engineers such as life-cycle analysis and design". The engineering process does not end at creation, nor does it stop innovating. As time passes and technology evolves, it requires engineers to adapt their technology and make sure their design continues to be effective and without error.

Service Orientation

Service orientation means that the organization should anticipate and prioritize the needs of their customers. This design typically is user-centered and includes direct client participation and indirect client participation (the general public) through conferencing, technology assessment, market research, and hearings whereby the tradeoffs in design options are carefully laid out and evaluated (Devon, 1999).

Following the discovery of the data breach, Equifax failed to provide ongoing communication and information regarding the attack. During the first week after the news broke publicly, Equifax was completely silent. While corporate leadership and security teams attempted technical damage control, journalists covered the story, as well as the perceived absence of corporate communication, using terms such as “scandal”, “epic failure” and “catastrophe” (Novak & Vilceanu, 2019). By not allowing consumers to participate and ask them for their opinion on the situation and proposed new designs to fix the data breach, Equifax broke the norm of servicing their clients. Equifax even failed to address the concern of clients, instead choosing not to say anything at all while the situation was being remedied, leaving clients with no sense of security and no idea of what was going on. Even worse, it was found that three Equifax former executives, John Gamble (Chief Financial Officer), Joseph Loughran (President of US Information Solutions), and Rodolfo Ploder (President of workforce solutions) had sold about $1.8 million worth of company stock on August 2nd, more than a month before the company disclosed the data breach to the general public (Berghel, 2017). This lack of external communication while Equifax executives were doing things under the table makes it seem like Equifax put their financial needs before those of the consumers affected by the data breach. I would argue these actions, or lack thereof, demonstrate a poor service oriented company that did not think about their customer's needs.

One could argue that Equifax did all they could to provide support and communicate with their consumers after the fact, through the set-up of a new website and call centers. In mid-August 2017, Equifax initiated a response-related effort called Project Sparta, through which they created a consumer-facing website (equifaxsecurity2017.com) for individuals to find out whether they were affected by the breach and, if so, to register for credit monitoring and identity theft services (Committee on Oversight and Government Reform, 2018). Equifax also set up a call center staffed by 1,500 temporary employees (Committee on Oversight and Government Reform, 2018). However, upon Equifax's public announcement of the data breach on September 7th, the website and call centers were overwhelmed with requests for information and left consumers without answers as to whether they were affected by the breach. Despite Equimax's significant effort to aid victims of the security breach following the announcement, the company failed to adequately prepare to respond to a data breach that large. This left many consumers frustrated and unassisted.

The communication issues with the consumers were further mishandled by members of the team. Security experts thought directing consumers from equifax.com to equifaxsecurity2017.com for data breach information was not secure because the link looked suspicious and confusing (Committee on Oversight and Government Reform, 2018). The long website link even seemed to be confusing to Equifax employees. For example, Equifax's Twitter account directed customers to a phishing website for nearly two weeks because an employee accidentally reversed the order of the words (Novak & Vilceanu, 2019). I argue that these miscommunications between the consumer and Equifax signify a corporate culture consisting of poor service orientation.

Project Management Skills

Good project management skills entails knowing what expertise and duties are required in order to assign and manage them in a fail-safe way. This includes displaying good decision making and conflict resolution practices to prevent failures from happening. Project management is not typically taught in engineering schools or in companies, which leads to many problems (Devon, 1999). However, companies should still engrain good management practices into group behavior. In this case, Equifax lacks a good organizational management structure to facilitate good communication and coordination necessary for an effective product.

Typically, the Chief Security Officer (CSO) reports to the Chief Information Officer (CIO). However, an internal restructuring change made it so that the the CSO reported to the Chief Legal Officer instead of the CIO (Committee on Oversight and Government Reform, 2018).

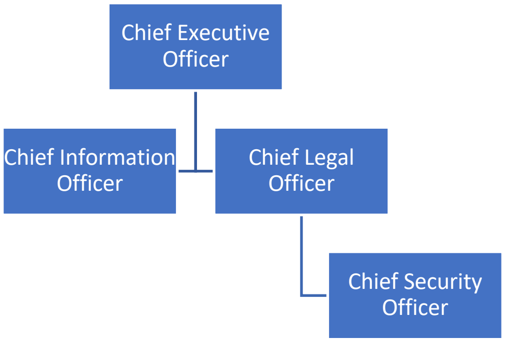

Figure 2: Equifax IT Organizational Structure

The functional result of the CIO/CSO structure (pictured in Figure 2) meant IT operational and security responsibilities were split, creating a disconnect between the two teams, leading to an accountability gap. This organizational structure allowed for ineffective IT coordination. One example of the lack of IT-Security coordination was that multiple and incomplete software inventory lists were kept separately by each group. Both IT and Security rely on accurate inventory lists to operate, patch, and monitor the company's IT systems (Committee on Oversight and Government Reform, 2018). In a well-organized environment, lists would be merged into a single master document with both teams working together to complete the inventory. This demonstrates that Equifax did not have an optimal IT management environment.

Conclusion

By viewing the Equifax company as a collective instead of holding one person accountable, I have argued the social arrangements of the Equifax team were unacceptable based on past analyses and actions. These actions show that the three norms of engagement for the participation of engineers in group processes (involving both engineers and non-engineers) were not met with respect to competency, service orientation, and project management skills. Examining this moral problem from a group process rather than an individual view is relevant as engineers are often involved in complex projects with many stakeholders who rely on them, and in this case, Equifax failed to express due care to their consumers.

Engineers in a company must be aware of an increasingly large number of interconnected issues, responsibilities, and responses to engineering issues. Thinking as a collective is increasingly important, as blaming one part of a whole does little to resolve the issue at hand. A moral problem is solved by having a team that meets all obligations of care and responsibility in the relationships within that team.

References

Berghel, H. (2017) "Equifax and the Latest Round of Identity Theft Roulette," in Computer, vol. 50, no. 12, 72-76. https://doi.org/10.1109/MC.2017.4451227

Committee on Energy and Commerce. [Report], Oversight of the equifax data breach: Answers for consumers: Hearing before the Subcommittee on Digital Commerce and consumer protection of the Committee on Energy and Commerce, House of Representatives, one hundred fifteenth congress, First Session, October 3, 2017 (2017). Retrieved from https://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf.

Committee on Oversight and Government Reform. [Report], The equifax data breach: Majority staff report, 115th Congress (2018). Retrieved from https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf.

Devon, R. (1999). Towards a social ethics of engineering: The norms of Engagement. *Journal of Engineering Education*, *88*(1), 87–92. https://doi.org/10.1002/j.2168-9830.1999.tb00416.x

Luszcz, J. (2018). Apache struts 2: How technical and development gaps caused the Equifax breach. *Network Security*, *2018*(1), 5–8. https://doi.org/10.1016/s1353-4858(18)30005-9

Novak, A. N., & Vilceanu, M. O. (2019). “the internet is not pleased”: Twitter and the 2017 equifax data breach. *The Communication Review*, *22*(3), 196–221. https://doi.org/10.1080/10714421.2019.1651595

Primoff, W., & Kess, S. (2017). The Equifax Data Breach: What CPAs and Firms Need to Know Now. *The CPA Journal; New York*, *Vol. 87* (Iss. 12), 14–17. Retrieved from https://www.proquest.com/docview/2185469906.

Smith, M., & Mulrain, G. (2018, September). *Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform* . Journal of National Security Law & Policy. https://jnslp.com/wp-content/uploads/2018/09/Equi-failure_The_National_Security_Implications_2.pdf

Srinivasan, S., Pitcher, P. and Goldberg, J.S. (2019), Data Breach at Equifax, HBS No. 9-119-031, Harvard Business School Publishing, Boston, MA.

University of Texas McCombs School of Business. (n.d.). *Equifax's breach of trust*. Ethics Unwrapped. Retrieved February 26, 2023, from https://ethicsunwrapped.utexas.edu/video/equifaxs-breach-of-trust

van de Poel, I., & Royakkers, L. (2011). Ethics, technology, and engineering: An Introduction. Blackwell Publishing.