

4-2 Group Discussion

MBA-635

Olaide OGUNMEFUN

David PEKALA

Mikendra PORTER

Christopher PRATT

19 July 2020

**Table of Contents**

[4-2 Discussion-Module Four 3](#_Toc45906164)

[Company Response to Compliance Gaps 3](#_Toc45906165)

[Stakeholder and Corporate Brand Impacts 4](#_Toc45906166)

[Short- and Long-Term Effects 5](#_Toc45906167)

[References 6](#_Toc45906168)

# 4-2 Discussion-Module Four

# Company Response to Compliance Gaps

Equifax, one of the three largest credit reporting agencies that assess the financial health of Americans in the country, was breached in 2017 causing millions of customer records to be exfiltrated by the attackers who breached the agency. “The multistate investigation found Equifax failed to take basic measures to secure its network that led to a September 2017 data breach that impacted approximately 147 million people. Breached information included names, Social Security numbers, birth dates, addresses, credit card numbers, and, in some cases, driver’s license numbers” (Jaeger 2019). Equifax did not respond well to the compliance issues involved in the data breach. The breach happened in September of 2017; however, Equifax was alerted to ‘patch’ its network in March of 2017. After being alerted to “a critical security vulnerability affecting its ACIS database, which handles inquiries from consumers about their personal credit data”, Equifax’s security team did follow up the alert with an order, but did not follow up to make sure the order was carried out (Jaeger 2019).

Equifax’s data breach of 2017 could have been prevented. “Basic security measures Equifax failed to implement include a policy to ensure security vulnerabilities were patched; failing to segment its database servers to block access to other parts of the network once one database was breached; and failing to install robust intrusion detection protections for its legacy databases” (Jaeger 2019). Had Equifax implemented consistent regulations, the breach could have been stopped in its tracks long ago. Designating an employee to oversee the information-security program, understanding that “Companies that profit from personal information have an extra responsibility to protect and secure the data” by minimizing its collection of sensitive data, as well as conducting annual assessments of their technology as well as internal and external security risks are some compliance lessons Equifax should implement after something like this.  The fine for what happened was large. Not just with money, but with the executive board and company as well as the rules they now must adhere to, to make sure this does not happen again.

# Stakeholder and Corporate Brand Impacts

The timing of Equifax response to the March 2017 data breach was poor at best and affected the stakeholder’s and the company brand negatively. Several errors and bad judgement on behalf of Equifax were discovered after the fact that seemingly could have been prevented. Equifax used an open source software program called Apache Struts which is used to build web applications in Java. In March of 2017, a cybersecurity researcher discovered a security flaw in the program. The vulnerability was so serious that the Department of Homeland Security Computer Emergency Readiness Team (CERT) issued a warning on March 8 to vulnerable parties, Equifax being one of them (Srinivasan, Pitcher, Goldberg, 2019). On March 9, 430 Equifax employees received notification. Unfortunately, the Apache Strut vulnerability was not identified or patched in response to the notification. On March 16, the vulnerability was discussed in depth at Equifax, however, most of their senior managers with cybersecurity responsibilities did not generally attend the meeting. It took until March 14 for Equifax to install the countermeasures, but the damage was already done. Hackers created multiple back doors into Equifax’s system that they were able to steal consumers personal information until mid-summer (Srinivasan, Pitcher, Goldberg, 2019). Equifax’s number one stakeholder are its customers. If they truly had the best interest of their customers at heart, the patch would not have been missed by 430 employees, including senior cybersecurity managers.

On September 7, Equifax announced that 143 million Americans personal information was exposed. The value of Equifax stock dropped from $143 to $93/share in a week (Srinivasan, Pitcher, Goldberg, 2019), negatively affecting their stockholders. Coincidentally, three senior officials at Equifax sold a combined $1.8 million in shares in the beginning of August that year. Poor timing that negatively affected the trust stakeholders had with Equifax. Equifax did take steps to protect consumers from the breach: credit monitoring, credit lock, free credit reports, and identity theft insurance all free for one year. This response was necessary, and it was the first step in rebuilding their brand and stakeholder confidence. Unfortunately, the website Equifax set up to provide information about the breach was confusing and easily faked. It was difficult for consumers to contact Equifax directly, the Consumer Financial Protection Bureau received over 7,500 complaints due to dropped calls and Equifax agents not returning calls. This negatively affects stakeholder confidence in the company and further frustrates an already negative situation.

The company did not prioritize the needs of their stakeholders in the decision-making process of the case. Change to Win (CtW) Investment Groups advisors' letter to Equifax Chairman, Mark Feidler, criticizing the board exposes the lack of priority to their stakeholder’s. The letter stated that the haphazard response to the data breach indicated that the board did not anticipate a concern with the company’s operations, and they gave little thought to Equifax’s most important asset, its reputation as a credit reporting agency. It also asserted that the board neglected to grasp the materiality of the breach to its consumers and shareholders (Srinivasan, Pitcher, Goldberg, 2019).

# Short- and Long-Term Effects

MIKENDRA TO INSERT

Describe the **short- and long-term effects** of the case on the business sustainability of the company.

# References

Goldberg, J., Pitcher, Q., Srinivasan, S. (2019). Harvard Business School. Data Breach at

Equifax. Retrieved from <https://services.hbsp.harvard.edu/lti/links/content-launch>

Jaeger, J. (2019, July 22). Lesson from Equifax penalty (at least $575M): Breach 'entirely preventable'. Retrieved July 15, 2020, from <https://www.complianceweek.com/regulatory-enforcement/lesson-from-equifax-penalty-at-least-575m-breach-entirely-preventable/27445.article>

Paine, L. (2014, August 01). Managing for Organizational Integrity. Retrieved July 15, 2020, from <https://hbr.org/1994/03/managing-for-organizational-integrity>