Ethical Dilemma at Equifax

Piyush Kumar

Hult International Business School

Data Management & SQL - DAT - 5486 - FMBAN1

Chase Kusterer

October 23,2022

Ethical Dilemma at Equifax

Equifax experienced an ethical dilemma that placed the company at stake when hackers stole data from 144.5 million consumers (Novak & Vilceanu, 2019). The company could either report the data breach and lose its customers or can hide the incident and put the customers' data in jeopardy and risk legal sanctions when identified. This shows that the company lacked ethical standards because it did not show any concern about the situation. The systems used by Equifax were found to be old, and the security systems were also out of date. Equifax realized the breach but did not report it to its consumers for almost two months. Equifax inflicted harm to the consumers by not protecting their data and jeopardizing their financial security (Novak & Vilceanu, 2019).

The consumers were just walking around, not knowing that their data was stolen or any issues occurred with their data. This may have led to some of the customers facing identity theft, and Equifax failed to give them a chance to get prepared or even prevent the loss from happening. This shows that Equifax did not ethically handle the crisis. The ethics in this situation focus on integrity and honesty because Equifax was not honest to their consumers that their data was stolen but instead decided to hide the situation. This shows that Equifax failed to own its mistakes which led to problems in the company. Equifax would have shown the best ethical value by admitting that there was an issue with customers' data. Consumers expect financial institutions such as Equifax that keep sensitive data to have business ethics of having security measures that are up to date and make sure the data is kept safe (Novak & Vilceanu, 2019).

Solutions to the Ethical Dilemma

A data breach can be one of the most stressful situations that a business can face, and this call for action to resolve it. Equifax can develop regulation actions that can help solve the ethical dilemma of a data breach. If the company suspects a data breach, it can prevent it by repairing its systems by executing an incident response plan to minimize the impact of the breach (Ahmad et al., 2020). A data breach is an issue that should be managed through teamwork. The company can also contain the breach by isolating the affected systems to prevent further damage until the systems are repaired.

Considering public communication may be a critical way of managing the data breach, where the main function of the incident response team would be to determine how the notifications will be made and when. One should be aware of the particular laws in the state and have instructions on the response team plan that outlines how the mandated notifications can be made (Zou et al., 2019). The notifications should be made timely to prevent major problems from occurring. Equifax would have made notifications earlier to prevent further company problems. Providing information may be better than saying nothing at all.

If the media marks a brand as untrustworthy for withholding information, the company can end up being hurt even worse than the effects of the data breach itself. Equifax could have provided information on the data breach issue to its consumers to prevent further harm from happening. The company can also ensure that the systems are fixed before returning them. This ensures that no further incidence of the breach can occur. The incident response team should also be prepared if an incident similar to that may occur by mitigating the damage from the cyber attack and restoring the digital services (Ahmad et al., 2020). To protect the customers' privacy, one must store the data in a secure database to prevent it from ending up in the wrong hands.

Stakeholder Analysis

The recommended solution would impact each group in different ways. The main stakeholders at Equifax include the consumers, government, employees, and investors. Communicating the data breach to the users would impact them by making them aware of the breach and pausing using the systems to prevent further harm (Zou et al., 2019). This helps them to consider not using the system to relay information about them before the company deals with the issue of the systems. Also, repairing the systems impacts the users because they may feel relieved that their data may be secured to prevent further damage. This helps the company safeguard its users and gain back their loyalty. The solution would impact the incident response team by being the main people dealing with the situation. The team will help the company to update its systems and have the user's data protected.

Better solutions may bring profit to the company, encouraging the investors to continue investing in the company. If a company fails to take action on the main problem at hand, the investors may be discouraged from investing because investors always want to see that their money is put to good use and also build their name. Data breaches affect the government by disrupting the services they offer, which helps them improve the data quality of the data breach and increase its global visibility landscape (Neto et al., 2021). The solution may impact the government by creating laws and actions that may help prevent such data breaches. To influence the stakeholders to adopt the solution, transparently communicating with them and making them understand the situation would be best to build their trust again. Also, the company can show them that it is possible to secure their data again by developing a secure database.

References

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How the integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939–953. https://doi.org/10.1002/asi.24311

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

Neto, N. N., Madnick, S., Paula, A. M. G. D., & Borges, N. M. (2021). Developing a global data breach database and the challenges encountered. *Journal of Data and Information Quality (JDIQ)*, *13*(1), 1-33.https://doi.org/10.1145/3439873

Zou, Y., Danino, S., Sun, K., & Schaub, F. (2019, May). YouMight'Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-14).https://doi.org/10.1145/3290605.3300424