Activity: Equifax Breach, A Company’s Duty to Others

Background

* **Incident**: The Equifax data breach in 2017 exposed the personal information of about 148 million U.S. citizens, including Social Security numbers and driver's license details.
* **Issue**: The breach was caused by a vulnerability in Apache Struts, a software framework used by Equifax.

Contributing Factors

* **Delayed Response**: Equifax was notified about the vulnerability but failed to install the necessary patches in time.
* **System Management Issues**: Inadequate IT practices and management contributed to the breach.

Ethical Challenges

* **Corporate Responsibility**: The breach raises questions about the ethical obligations of corporations in protecting consumer data.
* **Transparency and Accountability**: Equifax's delayed response and handling of the incident prompt discussions on ethical communication during crises.
* **Privacy vs. Business Interests**: The case illustrates the tension between collecting data for business and safeguarding personal information.
* **Magnitude Breach**: With a company like Equifax and it’s role in the economy, arguments have been made that Equifax was not given it’s fair punishment due to it’s size and “importance” this has lead to conversations about the level of “forgiveness” companies can get depending on size and what they are involved in.

Summary

The Equifax Data Breach of 2017 is a significant event in cybersecurity history. Between May and July 2017, Equifax, one of the largest credit bureaus in the U.S., suffered a massive data breach. On September 8, 2017, they announced the breach. This breach exposed sensitive personal information of approximately 147 million individuals. The exposed data included names, Social Security numbers, birth dates, addresses, and in some cases, driver's license numbers and credit card information. Rick Smith, the Chairman and CEO made a video announcing the breach as well as a dedicated site to help determine if one’s data had been compromised. The Public was not happy and raged about the breach as well as the response on social media.

The breach was attributed to a vulnerability in the Apache Struts web framework used by Equifax. The company was made aware of the vulnerability when a security patch was released a couple months prior to the breach. Despite being aware of the vulnerability, Equifax failed to implement the necessary security updates in time.

This breach raised significant concerns about data security practices, corporate responsibility, and the protection of consumer data. It led to investigations, legal actions, and a reevaluation of data security protocols across various industries. After January 22, 2020, users were given a site to make claims for any fees incurred as a result of the breach. In February of 2020, the U.S. Department of Justice charged 4 Chinese military-backed hackers in connection with the attack.

Sources:

[How the Equifax hack happened, and what still needs to be done - CNET](https://www.cnet.com/news/privacy/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/)

[Equifax Data Breach Settlement | Federal Trade Commission (ftc.gov)](https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement)

[(PDF) A Case Study Analysis of the Equifax Data Breach 1 A Case Study Analysis of the Equifax Data Breach (researchgate.net)](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)

[Chinese Hackers Charged in Equifax Breach — FBI](https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020#:~:text=Four%20Chinese%20military-backed%20hackers%20were%20indicted%20in%20connection,identifiable%20information%20ever%20carried%20out%20by%20state-sponsored%20actors.)

[(163) Rick Smith, Chairman and CEO of Equifax, on Cybersecurity Incident Involving Consumer Data. - YouTube](https://www.youtube.com/watch?v=bh1gzJFVFLc)