The Equifax 2017 Data Breach:

Vulnerabilities, Repercussions, and Potential Mitigations

Samantha Riggs

Old Dominion University

CYSE 300: Introduction to Cybersecurity

Dr. Joseph Kovacic

September 7, 2024

Equifax is one of largest consumer reporting agencies (CRAs), currently supporting 87 million consumers with credit card related services only. On September 7th, 2017, Equifax announced that a data breach incident had occurred. This breach affected 143 million consumers based in the U.S. alone, which after further investigation, rose to 148 million, making it one of the largest cybersecurity incidents related to identity theft to date.

In March of 2017, a vulnerability present in the Apache Struts software (software Equifax used to run certain applications on legacy systems), was publicly disclosed. Equifax was alerted by the Department of Homeland Security and two days later, Equifax's Global Threat and Vulnerability Management team emailed an alert, instructing the application of a necessary patch. Equifax was found to have not fully patched its systems however, and in May of 2017, an attack on Equifax's systems was initiated.

This attack lasted for an estimated 76 days. Attackers were able to obtain control and access to Equifax's network, where the unencrypted credentials of which were further used to access 48 unrelated databases outside of Equifax's Automatic Consumer Interview System. Over 9,000 queries were performed on these databases. The attack lasted this long due to an outdated certificate, which left the infiltration undetected. Once the certificate was updated, Equifax was immediately notified of the suspicious web traffic caused by the movement of data.

The U.S. House of Representatives Committee on Oversight and Government Reform stated that Equifax had at least two points of failure to mitigate or prevent the breach. First due to a lack of accountability and the existence of an unclear line of authority in Equifax's IT management structure. Secondly, there was a growth strategy implemented by Equifax in 2005 which resulted in a large accumulation of data. This acquisition resulted in a complex and antiquated IT environment, making security difficult.

After the breach was disclosed, many different lawsuits were filed in search of compensation for actual damages, future damages, and monitoring fees among other things. In 2019, Equifax settled with the Federal Trade Commission along with the Consumer Financial Protection Bureau, 48 U.S. states, Washington D.C., and Puerto Rico, having to pay $575 million dollars in fines and victim compensation.

References:

Liu, H., & FTC, S. at the. (2024, July 24). *Equifax Data Breach Settlement*. Federal Trade Commission. https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

U.S. House of Representatives Committee of Oversight and Government Reform. (2018). *The Equifax Data Breach* https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf