Equifax 2017 Cybersecurity Breach

By Adam Haas

9/5/2023

CYSE 300 15767

A Cybersecurity breach of significant proportions affecting American consumers was announced by Equifax in September of 2017. Personal identifying information, personal financial information, and credit card numbers were compromised and affected over 146 million U.S. consumers. (Daswani & Moudy Elbayadi, 2021). This breach also led to a major loss in public confidence and 50 class action lawsuits were filed within the first 10 days (Pike, 2017). These kinds of breaches contribute to the public's lack of trust in companies' capacity to protect and secure their livelihoods.

This hack, perpetrated by members of the Chinese People's Liberation Army, exploited a software vulnerability CVE-2017-5638 that gave them extensive, continued access to highly sensitive consumer information. Over the course of several months, four individuals were able to continuously request access to and collect personal information affecting and potentially jeopardizing American's financial, professional, and political positions (Daswani & Moudy Elbayadi, 2021).

The key vulnerability that allowed attackers initial access to Equifax servers was through a third party server managed by Apache Struts which was out of date and needed to be patched. This vulnerability had the most critical rating of 10 in the Common Vulnerability Scoring System "because it let *anyone anywhere else in the world issue any command to the server that they wanted"* (Daswani & Moudy Elbayadi, 2021). There were several other breakdowns within Equifax's system that allowed hackers' continued and extensive penetration to go unnoticed with increasing access to consumer information for this extended period of time. If these additional vulnerabilities had been acted upon by Equifax, it could have mitigated or prevented the breach of sensitive private information. These additional vulnerabilities consisted of the use of the McAfee vulnerability scanner despite being end-of-life, not patching the software immediately

after the weakness was identified, using an email system to identify vulnerabilities versus a robust ticketing and tracking process, renewing security certificates in a timely manner, using the principle of least privilege, and using important countermeasures (Daswani & Moudy Elbayadi, 2021). The company's lack of action in these outlined areas contributed to the damage and scope of the breach and process breakdowns that made the intrusion so damaging to Equifax's security of private information.

The multifaceted breakdown of Equifax's security system led to this cybersecurity breach being one of the worst of our time. Consumers have greater confidence in companies' operations, processes, and procedures when information systems and a consumer's right to privacy are made a top priority via cybersecurity.

Works Cited

Daswani, N., & Moudy Elbayadi. (2021). *Big breaches : cybersecurity lessons for everyone*. Apress.

Pike, G. (2017, November). Equifax: Yet Another Data Breach. *Information Today*, 17. EBSCOhost.