by S N

Submission date: 25-Jun-2021 12:15PM (UTC-0500)
Submission ID: 1612105362
File name: The_Problem_Equifax_Faced_in_2017.docx (16.98K)
Word count: 512
Character count: 2890

The Problem Equifax Faced in 2017

Name

Institution

Course

Instructor

Date

The Problem Equifax Faced in 2017

Equifax revealed in 2017 that hackers stole the personal details of 147.7 million Americans in its systems. Hackers broke into Equifax's system and obtained customer information, Social Security details, dates of birth, and addresses, impacting over half of the US citizenry. Then-CEO Rick Smith issued an apology in a video soon after discovering the hack (Wang & Johnson, 2018). After that, however, customers flocked to social platforms, especially on how bad Equifax's webpage was, as millions of individuals attempted to determine if the hack impacted them.

The firm was initially hacked through a consumer grievance portal. According to Wang and Johnson (2018), the perpetrators exploited a publicly known vulnerability in Equifax's information security protocols that ought to have been rectified but were not. Since its security structures were not sufficiently isolated from each other, the hackers could migrate the website to other hosts. They could pinpoint users and encoded information in plain text, granting them entry to even more platforms. As Equifax failed to update a private algorithm on one of its core security systems, hackers managed to steal data from the network without notice for months. Equifax did not explicitly reveal the attack until a month when it was discovered; stock purchases by top management around this period ignited suspicions of securities fraud. Subsequently, legislation introduced by Elizabeth Warren and several others that would have levied sanctions on credit-reporting companies that were hacked failed in the Upper house. It does not imply that the Equifax breach did not cost the firm anything. Two years after the attack, the firm reported spending $1.4 billion on cleaning expenses, including accelerated investments to change its information systems and strengthen software, internet, and information security. Subsequently, the company's credit rating was lowered, citing the vast amounts it will need to

invest in information security in the coming years. In July 2019, the business achieved a landmark deal with the Federal Trade Commission, marking the end of an ongoing civil lawsuit and requiring Equifax to spend nearly $1.38 billion to satisfy customer claims (Federal Trade Commission, 2020). There was much agony among millions of Americans who were unsure whether they were among the 40% affected by the data breach. Presently, things have calmed down in the years afterward, and there is now a new website where people can check to see whether they are impacted.

To sum it up, there is no such thing as an untouchable system. However, Equifax was compromised since it neglected to fix a simple flaw, despite having protocols to ensure such updates were implemented as soon as possible. Massive volumes of data were unknowingly stolen after someone failed to upgrade a digital signature. Equifax had invested millions of dollars on security equipment, but it had been inadequately deployed and monitored.

References

Federal Trade Commission. (2020, July 15). *Equifax data breach settlement*. https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement

Wang, P., & Johnson, C. (2018). Cybersecurity Incident Handling: A Case Study of the Equifax Data Breach. *Issues in Information Systems*, *19*(3).

I

ORIGINALITY REPORT

0%	0%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		