**Equifax Data Breach: A Lesson in Human Error and Encryption Failure**

Rosemarie Kpaka

Bowie State University

CTEC111-101-Fall2024

Professor Henri' Cooper

October 2, 2024

**Introduction**

In an increasingly digital world, data breaches have become a major concern, affecting millions of individuals and companies worldwide. These incidents expose sensitive information, leading to financial losses, reputational damage, and legal consequences. Among the most infamous breaches is the 2017 Equifax data breach, which compromised the personal information of over 145 million Americans (McCoy, 2019). This paper examines the Equifax breach, focusing on the role of encryption and human error, and highlights key lessons for preventing such incidents in the future.

**Background on the Equifax Breach**

The Equifax breach occurred between mid-May and July 2017 but was not publicly disclosed until September of the same year (Bisson, 2022). The attackers exploited a vulnerability in Apache Struts, an open-source web application framework used by Equifax. Although the vulnerability had been disclosed and patched months earlier, Equifax failed to apply the necessary updates, leaving the system exposed to hackers. This breach resulted in the theft of sensitive information, including Social Security numbers, birth dates, addresses, and driver’s license numbers of millions of Americans (Nakashima, 2019). One of the critical failures in this breach was the improper use of encryption. Equifax had encryption mechanisms in place but failed to encrypt sensitive data such as Social Security numbers at key points of access. Additionally, the breach went undetected for months due to expired security certificates, preventing the company from identifying the intrusion in a timely manner (Bisson, 2022).

**The Role of Human Error and Encryption in the Breach**

While encryption is a fundamental security measure for protecting sensitive data, its effectiveness is often undermined by human error. In the Equifax case, human negligence played a significant role. The company failed to renew its security certificates, a basic task that could have triggered alerts about unauthorized access. Moreover, despite knowing about the Apache Struts vulnerability, the necessary patches were not applied in time (McCoy, 2019). Research shows that human error is a significant factor in data breaches. According to a 2022 report by Verizon, 82% of data breaches involve some element of human error, whether due to poor decision-making, misconfiguration, or negligence (Verizon, 2022). In the case of Equifax, this human oversight created an environment where encryption could not perform its protective role, ultimately allowing the attackers prolonged access to sensitive information.

**Consequences of the Breach**

The Equifax breach had severe financial, legal, and reputational consequences. U.S. regulators fined the company approximately $700 million to settle investigations and lawsuits related to the breach (McCoy, 2019). In the United Kingdom, the Information Commissioner’s Office imposed a £500,000 fine on Equifax for its failure to protect the personal data of British citizens (Nakashima, 2019). In addition to financial penalties, the company’s reputation took a major hit. Equifax became a cautionary tale for how not to handle cybersecurity. The company’s failure to act on known vulnerabilities and its mismanagement of encryption protocols eroded consumer trust, leading to significant business challenges. The breach also spurred regulatory reforms, including the General Data Protection Regulation (GDPR) in Europe, which now requires companies to implement stronger data protection measures and face higher fines for non-compliance (Bisson, 2022).

**Lessons Learned and Prevention Strategies**

The Equifax breach provides several critical lessons for companies seeking to protect sensitive data. First, organizations must ensure that security patches and updates are applied promptly to avoid known vulnerabilities being exploited. This can be achieved through automated patch management systems that reduce reliance on human intervention. Second, businesses need to make their security stronger. Encryption can keep data safe, but only if it is used properly. For private data, businesses should use end-to-end encryption and check their encryption methods often to make sure they are working right (Bisson, 2022). Also, using automatic certificate management can help stop problems like the one Equifax had, where outdated certificates let the breach go unnoticed. Lastly, companies need to spend money on cybersecurity training to lower the chance of mistakes made by people. Regular training can help workers spot possible security risks and make sure that basic security chores are done on time, like updating certificates and installing patches.

**Conclusion**

The security breach at Equifax in 2017 is a stark warning of how important it is to use encryption correctly and the dangers that come from making mistakes. Cyberattacks can be stopped by technology like encryption, but it only works if people are also carefully watching over it. After the Equifax hack, companies can better protect themselves from future data breaches by using stronger security, setting up automatic systems, and training their employees.

**References:**

Bisson, D. (2022). 7 data breach examples involving human error: Did encryption play a role? *Digital Guardian*. https://digitalguardian.com/blog/7-data-breach-examples-involving-human-error

McCoy, K. (2019). Equifax data breach: The biggest in history? *USA Today*. https://www.usatoday.com/story/news/nation/2019/09/08/equifax-breach-biggest-history-heres-what-you-need-know/2235188001/

Nakashima, E. (2019). Equifax fined $700 million over massive data breach. *The Washington Post*. https://www.washingtonpost.com/equifax-fined-over-massive-data-breach

Verizon. (2022). 2022 data breach investigations report. *Verizon Business*. https://www.verizon.com/business/resources/reports/dbir/