In-class Exercise-3

THE CASE OF EQUIFAX (2019)

- **What Happened?**

Equifax failed to take basic steps to secure personal information stored on its network—resulting in the 2017 data breach that jeopardized the personal data of a staggering 147 million people. Specifically, Equifax failed to address unpatched critical and high-risk vulnerabilities across systems that persisted for months at a time.

- **How was it discovered?**

The breach was discovered on July 29, 2017, when Equifax's security team noticed suspicious traffic on the ACIS Dispute Portal after replacing expired security certificates. Although the team blocked the traffic, additional suspicious activity was detected the next day, prompting them to take the portal offline. A forensic investigation later revealed that, between May 13 and July 30, 2017, multiple attackers had exploited an unpatched vulnerability to gain unauthorized access to Equifax's network, leading to the exposure of extensive consumer data. By August 11, Equifax confirmed the breach had compromised a significant amount of personal information.

- **How many people were affected?**

During the months attackers went undetected on Equifax's network, they executed nearly 10,000 queries targeting sensitive personal information, including Social Security numbers (SSNs) and dates of birth. According to forensic analysis, the attackers stole around 147 million names and dates of birth, 145.5 million SSNs, 99 million physical addresses, 20.3 million phone numbers, 17.6 million email addresses, and 209,000 payment card numbers. The compromised data included information from consumers who had used Equifax's services, such as credit scores, credit monitoring, and identity theft prevention, as well as those who had requested free credit reports.

- **Provide Breach Details:**

In September 2017, Equifax disclosed a data breach that exposed sensitive personal information of over 147 million consumers. The breach stemmed from Equifax's failure to implement basic security measures on its Automated Consumer Interview System (ACIS) Dispute Portal. In March 2017, the U.S. Computer Emergency Readiness Team (US-CERT) warned Equifax of a critical vulnerability in Apache Struts, a software used in the ACIS Dispute Portal. Despite this warning, Equifax failed to apply a security patch to the portal for months due to miscommunication and ineffective security scans.

Between May and July 2017, attackers exploited this vulnerability to gain unauthorized access to Equifax's network. Once inside, they moved laterally across multiple databases due to a lack of network segmentation and obtained further access through unsecured credentials stored in plain text. Equifax discovered the breach in late July and, by August 2017, confirmed that a large amount of consumer data had been compromised.

Equifax failed to address a critical vulnerability (2017-CVE-5638) due to over-reliance on an automated vulnerability scanner without implementing additional safeguards to ensure the issue was resolved. This oversight, along with inadequate segmentation of database servers linked to the Automated Consumer Interview System (ACIS), allowed attackers to easily access a wide range of consumer data. Equifax also left a file share accessible to attackers and stored over 145 million Social Security numbers and other sensitive data in plain text, violating its own encryption policies. The lack of security controls on legacy systems like ACIS led to months of undetected intrusion.

- **List of consequences (was Equifax required to do as per the FTC?)**

- Equifax must establish a system to solicit and address employee security concerns.
- Required to implement and maintain a comprehensive information security program for 20 years.
- Must undergo independent, third-party assessments every two years to evaluate and improve the security program.

- Assessments will review the implementation of the program, identify gaps, and provide recommendations.
- Equifax must fully disclose all relevant network and IT information to the assessor.
- Annual certification must be provided for 20 years confirming:
- 1. Compliance with the FTC order.
- 2. No material noncompliance has gone unreported.
- 3. Cooperation with third-party assessors.
- 4. Any security incidents (covered incidents) are reported.
- Concealing or misrepresenting facts during the assessment process is prohibited.