**AMRUTHESH**

**241059041**

**CRYPTOLOGY**

**M.E – CYBER SECURITY**

**A Cybersecurity Incident:** **Equifax Data Breach (2017)**

At present, Equifax Data Breach is one of the biggest cybersecurity disasters where hackers exposed personal data of over 147 million Americans.

The root cause of the breach was Equifax’s failure to patch a known vulnerability in the Apache Struts framework. Despite receiving notifications from the U.S. Department of Homeland Security about the vulnerability and the need for urgent patching, Equifax’s IT staff failed to implement the fix.

Hackers were able to exploit this vulnerability, gain access to Equifax's network, and move laterally through its systems. Once inside, they extracted massive amounts of sensitive consumer data over the course of two months.

Equifax faced severe legal consequences, including a settlement of up to **$700 million**. The company’s reputation took a major hit, and it had to offer free credit monitoring to affected consumers. Several top executives resigned, and Equifax scrambled to overhaul its cybersecurity defenses.

The Equifax data leak shows that it’s crucial to quickly patch cracks especially when dealing with sensitive personnel information. This case demonstrates how inadequate Risk Management and unpatched vulnerabilities can have drastic and long reaching consequences.

**Terms explored during the Case Study:**

**1. Danger**  
 In the realm of cybersecurity, danger refers to any possible peril that can result in the loss or damage of data or a system. In the case of Equifax, it was hackers or cybercriminals trying to steal private customer information who posed the threat. The financial motivation behind this threat stemmed from possibilities like identity theft, fraudulent transactions, and even blackmailing using the data.  
  
**2. Succession** A threat actor could exploit a system’s weakness or flaw known as vulnerability. Equifax hack happened as a result of CVE-2017-5638 which was a known weakness in the Apache Struts web application frame work. Even though the patch for this problem had been available months before the hacking incident, they failed to apply it on time leaving their systems open to attack.  
  
**3. Attack** An attack is an intentional act to inflict injury on someone or something, gain access unlawfully to it, and violate it. The attack in Equifax case was initiated using Apache Struts vulnerability. The attackers had access to sensitive personal information stored by Equifax such as addresses, birth dates, and Social Security numbers.  
  
**4. Risk** Risk signifies the chance to incur loss or harm caused by a threat exploiting a weakness. This risk was indeed quite significant for Equifax because of the type of data they were safeguarding. The missed deadlines for patching and the irresponsible storage of sensitive information caused huge financial losses to the company, had legal implications on its standing and contributed towards damaging its reputation.  
  
**5. Application** An exploit can be described as the strategy or method through which an attacker exploits a vulnerability. In this case, attackers exploited the unpatched Apache Struts vulnerability through malicious code enabling them to steal Equifax’s data without authorization.  
  
**6. Asset** An asset refers to anything that has value for an organisation and requires protection. Equifax’s assets included its databases, computers and overall reputation, along with personal records of millions of customers.  
  
**7. Impact** The impact of a cyber breach refers to its result or damage. For instance, 147 million people’s sensitive information was exposed when hackers broke into Equifax’s system. Therefore, this resulted in losses for the company and negative consequences like legal suits and fines imposed by the government as well as serious harm done to the image of Equifax. Also, consumers faced possible long-term consequences such as financial thefts and identity impersonation.