**NAME: SOURABH PANDYA**

**ENROLLMENT NO : 0827CY221061**

**TOPIC: Equifax Data Breach**

**The case discusses the events leading up to the massive data breach at Equifax, one of the three U.S. credit reporting companies, the organizational and governance issues that contributed to the breach, and the consequences of the breach. The case supplement provides details of how Equifax recovered from the breach and changes the company made. On September 7, 2017, Equifax announced that the personal information of over 140 million consumers had been stolen from its network in a catastrophic data breach, including people’s Social Security numbers, driver's license numbers, email addresses, and credit card information. The announcement sparked a massive backlash, as consumers and public officials questioned how a company that managed sensitive personal information about over 800 million individuals could have such insufficient security measures. It came to light that Equifax had been aware of critical faults in its cybersecurity infrastructure, policies, and procedures for years but had failed to address them. Equifax’s public response also received criticism. CEO Richard Smith and numerous other executives resigned, and Equifax was left facing dozens of lawsuits, government investigations, and the potential for new regulation.**

**The vulnerability that caused the breach was vulnerability Apache Struts CVE-2017-5638. Apache Struts is a popular framework for creating Java Web applications maintained by the Apache Software Foundation. The Foundation issued a**[**statement**](https://blogs.apache.org/foundation/entry/media-alert-the-apache-software)**announcing the vulnerability and released a**[**patch**](https://cwiki.apache.org/confluence/display/WW/S2-045)**on March 7, 2017.**

**Equifax breach by the numbers**

**76 days: Amount of time during which the attackers were active within Equifax’s networks without being discovered**

**143 million: Number of consumers whose data was potentially affected by the breach**

**$125: The most you can expect to get in compensation if your data was exfiltrated from Equifax’s systems**

**$1.4 billion: Amount Equifax has spent on upgrading its security in the wake of the incident**

**0: Number of fraud or identity theft cases that can be traced back to this incident**

**Ramsomware:-**

**Ransomware is a type of malware that locks and encrypts a victim's data, files, devices or systems, rendering them inaccessible and unusable until the attacker receives a ransom payment. The first iterations of ransomware used only encryption to prevent victims from accessing their files and systems**.

**Wannacry Ransomware Attack**

**Wannacry Ransomware Attack**

**WannaCry is an example of crypto ransomware, a type of malicious software (malware) used by cybercriminals to extort money.**

**Ransomware does this by either encrypting valuable files, so you are unable to read them, or by locking you out of your computer, so you are not able to use it.**

**Ransomware that uses encryption is called crypto ransomware. The type that locks you out of your computer is called locker ransomware.**

**Like other types of crypto-ransomware, WannaCry takes your data hostage, promising to return it if you pay a ransom.**

**WannaCry targets computers using Microsoft Windows as an operating system. It encrypts data and demands payment of a ransom in the cryptocurrency Bitcoin for its return**.

## How does a WannaCry attack work?

**The cybercriminals responsible for the attack took advantage of a weakness in the Microsoft Windows operating system using a hack that was allegedly developed by the United States National Security Agency.**

**Known as EternalBlue, this hack was made public by a group of hackers called the Shadow Brokers before the WannaCry attack.**

**Microsoft released a security patch which protected user’s systems against this exploit almost two months before the WannaCry ransomware attack began. Unfortunately, many individuals and organizations do not regularly update their operating systems and so were left exposed to the attack.**

**The attackers demanded $300 worth of bitcoins and then later increased the ransom demand to $600 worth of bitcoins. If victims did not pay the ransom within three days, victims of the WannaCry ransomware attack were told that their files would be permanently deleted**.

## What impact did the WannaCry attack have?

**The WannaCry ransomware attack hit around 230,000 computers globally.**

**One of the first companies affected was the Spanish mobile company, Telefónica. By May 12th, thousands of NHS hospitals and surgeries across the UK were affected.**

**A third of NHS hospital trusts were affected by the attack. Terrifyingly ambulances were reportedly rerouted, leaving people in need of urgent care in need. It was estimated to cost the NHS a whopping £92 million after 19,000 appointments were canceled as a result of the attack.**

**As the ransomware spread beyond Europe, computer systems in 150 countries were crippled. The WannaCry ransomware attack had a substantial financial impact worldwide. It is estimated this cybercrime caused $4 billion in losses across the globe.**

**Submitted To: Prof. Satyam Shrivastava**