# Securing Information Systems (Equifax Breach)

Brandon Pearson

# What happened?

Equifax is a major credit reporting agency that was breached in 2017. This breach exposed over 100 million users personal information and confidential data. This put customers at risk for their data being exploited by whomever was able to access it. The attack was able to be done due to Equifax failure to update software that had a known exploit. The attacks exploited the user support forum on Equifax website which allowed them to gain access.

The attack brought attention to user data/ big data and the social responsibilities of companies.

# Who was involved?

**Equifax** was target by unknown attackers or a unknown group of attackers.

It is believe that 4 chineses attackers committed the attack.

# Where did this occur?

Equifax is a United States company that was founded in 1899. The company has expanded over time reaching out across the U.S. and other countries.

Headquarters located in Atlanta, Georgia.

The companies web browser was exploited which allowed attackers access to Equifax's network.

# How did this happen? (lapse in security, mistake, etc.)

The incident occurred when Equifax failed to update a known security flaw. Equifax was made aware of this flaw by Apache Software Foundation the developer of the software that was used. Upon being notified about the update Equifax would fail in completing a accurate assessment of what needed to be updated. Which lead to attackers taking advantage of the security flaw.

The vulnerability was called CVE-2017-5638

# What were the consequences/impacts? (individuals, legal, ethical, social, society, environment)

Equifax is one of three major credit reporting companies. They hold millions of users private data and credit information.

The breach exposed millions of users private/confidential information. Individuals that were impacted are at risk of identity theft or other financial risk.

Equifax had to pay substantial fines due to the breach.

This breach brought attention to the concern of companies mishandling users data. This also impacted the companies public image.

# What was done to address or prevent this from happening again?

Equifax put substantial amount of effort in improving their cybersecurity and IT teams capabilities. Implementing detection systems in hopes to detect any breach in a faster manner if one take place.

After the breach Equifax hired more IT workers as well as put forth 1.2 billion dollars to better secure the company's assets.

# What are your suggestions to prevent this from happening again?

The company should have had a better tool to detect what piece of software or equipment needed to be updated. This would have been an effective way in ensuring all pieces of equipment were accounted for. Preventing the asset from being exploited due to the failure in updating it.

# Do you think this could happen again and why?

I think that this type of attack could easily happen again. The attack wasn’t the most sophisticated attack out there is was mainly the mistake that Equifax made that allows attackers to get in. The reason this could happen again is because the attack only was able to take place due to Equifax failing to update a piece of software. If it is as simple as one piece of software being exploited in order for attacker to gain access to a company then this could easily happen again.

# What are the potential impacts including intended and unintended of cyber security on individuals, society, or the environment?

One major concern with cyber security is the potential for it to overstep on citizens rights. Primarily their right to privacy being breached. For example: surveillance systems and government surveillance programs having access to things that people may deem private.

The government wants to create an overall safer cyberspace but it is tricky due to the concerns mentioned. With increased cyber security it can help protect financial systems as well as protect users from being targeted by attackers.