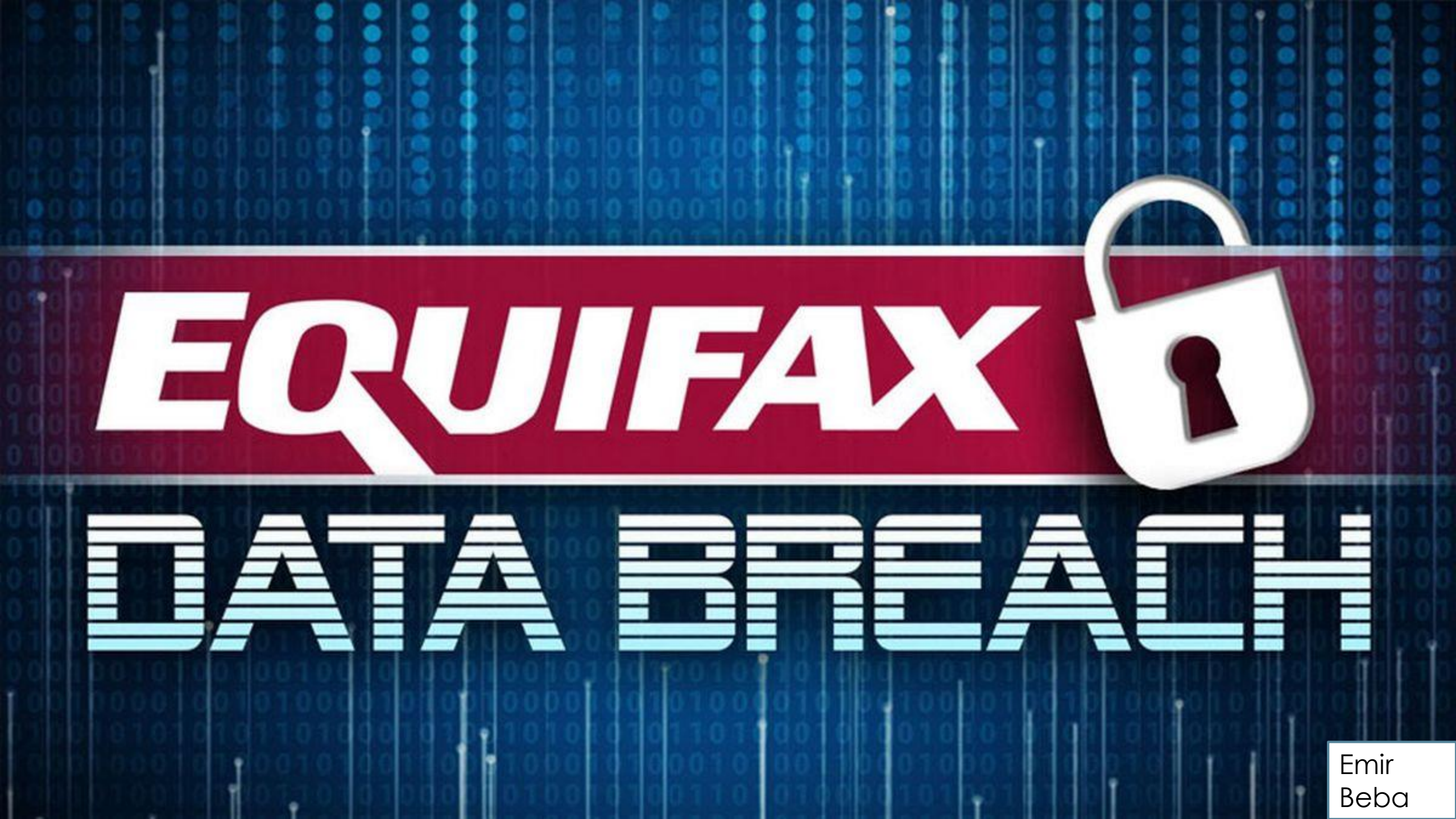

Emir
Beba

ABOUT EQUIFAX

Equifax

- Equifax is an American multinational consumer credit reporting agency and is one of the three largest consumer credit reporting agencies, along with Experian and TransUnion.
- Equifax collects and aggregates information on over 800 million individual consumers and more than 88 million businesses worldwide. In addition to credit and demographic data and services to business, Equifax sells credit monitoring and fraud prevention services directly to consumers.

BACKGROUND INFORMATIONS ABOUT THE BREACH

Background informations about the breach

- In September 2017, Equifax announced a cyber-security breach, which it claims to have occurred between mid-May and July 2017, where cybercriminals accessed approximately 145.5 million Equifax consumers' personal data.
- Like plane crashes, major infosec disasters are typically the result of multiple failures. The Equifax breach investigation highlighted a number of security lapses that allowed attackers to enter supposedly secure systems and exfiltrate terabytes of data.

- The company was initially hacked via a consumer complaint web portal, with the attackers using a widely known vulnerability that should have been patched but, due to failures in Equifax's internal processes, wasn't.
- Equifax did not publicize the breach until more than a month after they discovered it had happened; stock sales by top executives around this time gave rise to accusations of insider trading.

- HOW LARGE THE EXPOSURE WAS?
- WHAT WAS AFFECTED?

- Equifax announced a data breach that exposed the personal information of 147 million Americans (about 44 per cent of the population)
- Residents in the United Kingdom (15.2 million) and Canada (about 19,000) were also impacted.
- Equifax also confirmed at least 209,000 consumers' credit card credentials were taken in the attack.

What was affected?

- Cybercriminals accessed Equifax consumers' personal data, including:
- Their full names
- Social Security Numbers
- Birthdates
- Addresses
- Credit cards
- Driver‘s license numbers

- FOR HOW LONG THE BREACH WAS ACTIVE?

- Forensics analyzed after the fact revealed that the initial Equifax data breach date was March 10, 2017: that was when the web portal was first breached via the Struts vulnerability. However, the attackers don't seem to have done much of anything immediately.
- It wasn't until May 13, 2017 — in what Equifax referred to in the GAO report as a "separate incident" — that attackers began moving from the compromised server into other parts of the network and exfiltrating data in earnest.

- From May through July of 2017, the attackers were able to gain access to multiple Equifax databases containing information on hundreds of millions of people; as noted, a number of poor data governance practices made their romp through Equifax's systems possible.
- On September 7. 2017, Equifax, discovered the application vulnerability on one of their websites led to a data breach that exposed

- How it has been attacked?

- The vulnerability that caused the breach was vulnerability Apache Struts. Apache Struts is a popular framework for creating Java Web applications maintained by the Apache Software Foundation.
- The company was initially hacked via a consumer complaint web portal, with the attackers using a widely known vulnerability that should have been patched but, due to failures in Equifax's internal processes, wasn't.

- The attackers were able to move from the web portal to other servers because the systems weren't adequately segmented from one another.
- The attackers pulled data out of the network in encrypted form undetected for months because Equifax had crucially failed to renew an encryption certificate on one of their internal security tools.

- WHAT SHOULD HAVE BEEN DONE TO PREVENT THE BREACH?

There are many lessons to learn here:

- Ensuring application and cyber security are essential to our hyper-connected world.
- A thorough penetration test or code review could have found the security risk early on.
- Introducing powerful automation into the company's security testing would have also helped. They would have been able to identify the risk long before it became a serious problem.

- Complex and outdated IT systems:

Equifax's aggressive growth strategy and accumulation of data resulted in a complex IT environment. Both the complexity and antiquated nature of Equifax's custom-built legacy systems made IT security especially challenging.

- Failure to implement responsible security measurements:

Equifax allowed over 300 security certificates to expire, including 79 certificates for monitoring business critical domains.

- Unprepared to support affected consumers:

After Equifax told the public of the data breach, it was unprepared to identify, alert and support affected consumers. The breach website and call centers were immediately overwhelmed, and affected consumers couldn't access information needed to protect their identity.

- WHAT ARE THE CONSEQUENCES?

Impact on customers:

- 147 million US customers:

-Social Security Numbers

-Driver‘s License Numbers

-Addresses

-Birthdates

-Credit Card Numbers

- **Financial Loss**:

-After insurance, costs tied to dealing with crisis could run between 200 and 300 million dollars.

According to attorneys in Chicago:

-Equifax will pay more than 1 billion dollar.

-Offering 12 months free Trusted ID Premier credit monitoring

- **Investors:**

Wall Street has rendered an estimate 4 billion lost stock market value

Also, all of this has made a big loss of reputation.

References

- https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
- https://slideplayer.com/slide/15007809/
- https://epic.org/privacy/data-breach/equifax/
- https://securityboulevard.com/2018/12/how-to-avoid-becoming-the-next-equifax-investigation-reveals-breach-was-entirely-preventable/
- https://www.atlanticbt.com/insights/what-could-have-prevented-equifax-breach/