NAME: IQUEN L MARBA **YEAR & SECTION: BSIT-3C**
INSTRUCTOR:CHERRY BERTUFLO **DATE: 10/9/24**

Equifax Data Breach 2017

I. Summarize the information gathered from your readings. Cite sources accordingly

In March 2017, Equifax a major credit reporting agency, experienced a massive data breach in which attacker stole the personal data of hundreds of millions of individuals. The breach was caused by multiple security failure, including the use of an unpatched vulnerabilty in a web portal poor system segmentation, and storing passwords in plain text. Additionally, Equifax failed to renew an encryption certificate, allowing data to be exfiltrated unnoticed for months.

The breach was not publiczed until over a month after its discovery, and insider trading accusations arose when top executives sold stock during that period. The attack originated from a known vulnerability in Apache Struts that was not patched due to internal process failure. Despite warnings from a security firm about unpatched systems, these issues were not resolved, leading to significant data theft.

https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

II. Answer

How did the breach harm individuals and Equifax?

the information that was compromised and spirited away by the attackers, the attackers got hold of personal information like names, addresses, birthdays, Social Security numbers, and records, including credit card details and more.

Who was responsible for the breach and what were their actions?

Equifax was breached by Chinese state-sponsored hackers whose purpose was espionage, not theft.

Could the breach have been prevented with better security measures?

Yes

What were the long-term consequences of the breach?

Forty percent of American data has been hacked over the years. Even if things have been fixed, your information can still be used for stuff you wouldn't like, especially if you're part of that 40%.

What can be learned from this incident to prevent future data breaches?Which "commandment/s" were violated in this incident? Explain why these commandments were violated.

- **Thou shalt not use a computer to harm other people.**

  The attackers harmed millions of individuals by stealing their personal data, putting them at risk for identity theft.

- **Thou shalt not use a computer to steal.**

  The incident involve a theft of personal data

- **Thou shalt not use other people's computer resources without authorization or proper compensation.**

  The Chinese hackers exploited Equifax's systems without authorization.