CIST 3381- Information Assurance & Security
Spring 2022
Case Study 2: Data Breach at Equifax

Group Name:
L1

Group members' names:

1. Michael Chillemi
2. Vivian Yin
3. Amanda Quach
   John Raven

CIST 3381- Information Assurance & Security
Spring 2022
Case Study 2: Data Breach at Equifax

Group Name: L1 **Your Name:** John Raven

Ques 1) How does Equifax's business model work? What is the role played by consumers' in Equifax's product offerings?

Answer:

- Collects customer PII from bank accounts
- Consumer's offer personal info to Equifax and Equifax then compiles all accounts matching their info into a score and report
- Equifax offered fraud ~~protect~~ detection services and identity theft detection services
- Consumer's could sign up for these products and review reports to ensure everything reported was accurate
- Not just American consumers were effected, Canada and U.K. Residents were effected as well

CIST 3381- Information Assurance & Security
Spring 2022
Case Study 2: Data Breach at Equifax

Group Name: L1 **Your Name:** Michael Williams

Ques 2) Was Equifax lax or unlucky to be cyber-breached in this way?

Answer:

- Equifax was lazy,
- not a lot of security
- did not update vulnerabilities
- lack of communication
- late on patches
- only it can install software (unit on them)
- cyber security configure
- low security audits
- team correlation = poor
- Servers not segmented
- changing position - not inform new person
- unlucky they got hacked
- sold stocks / unknown about data breach
- certificates not up to date

CIST 3381- Information Assurance & Security
Spring 2022
Case Study 2: Data Breach at Equifax

Group Name: L1 **Your Name:** Vivian Hin

Ques 3) How well did Equifax responded to the breach? What do you think accounts for the delay in informing the Board?

Answer:

- Equifax knew abot the new patch but took a few months before patching Apache struts.
- emails were sent out but it wasn't sent out to the right people since the company security team was split into two branches
- Banned an IP address that was entering their network. More IP addresses came through and that's when they shutdown their system
- Hired outside sources to look into the vulnerabilities
- Informed the public months after & there was a lack of transparency
- ~~financial~~ seniors officers sold his stock the day of his breach (2 mil)
- Equifax set up a poor website but that website also has its own vulnerabilities
- bad url of the website they created which allows hackers to phish individuals.

CIST 3381- Information Assurance & Security
Spring 2022
Case Study 2: Data Breach at Equifax

Group Name: L1 **Your Name:** Amanda Quach

Ques 4) To what extent would you hold Equifax's board accountable for the company's lack of cybersecurity preparedness? Assuming you are serving on the company's board, what questions you'd ask to know about the security preparedness of the company

Answer:

Very accountable for the company's lack of cybersecurity preparedness.

Allowing the hiring of CFS with no knowledge of security.

~~Not asking enough~~

Irresponsible

No actions taken against past breaches. (Red flags)

Board not ~~upda~~ up to date.

Lack of ~~respon~~ response to exodus of cybersecurity talent.

Questions

- Pen test (Intrusion) Frequency?
- ~~Th~~ What is the plan for during a breach?
- ~~Tim~~ Progress of integrating acquired companies systems (or security) to be compatiable to company's system.
- Is 1% percent ~~spending target~~ towards security enough?
- Are employees trained/~~updat~~ up to date with cybersecurity
- ~~Preparedness for~~ Prevention Plans
- ~~Is~~ Are the security tools up to date.
- Severity/liklihood of hack?

Quantifying cyber-risk?

updates to response plan & process?