Seminar 5 - Data Breach Case Study (Sony PlayStation Outage)

What types of data were affected?

Sony's PlayStation Network data leaks included people's names, addresses, email addresses, birth dates, usernames, passwords, logins, security questions and more from approximately seventy-seven million users (Baker and Finkle, 2011).

What happened?

In April 2011, the Sony PlayStation Network (PSN) was externally hacked, resulting in the leak of seventy-seven million user accounts. The data leaks included people's names, addresses, email addresses, birth dates, usernames, passwords, logins, security questions and more (Baker and Finkle, 2011). Following the attack on April 20th, Sony closed its PlayStation Network to investigate the incident. On May 14th, after twenty-four days since the closing of the PlayStation Network, Sony restored its network fully functionality (Williams, 2011). This attack cost Sony approximately one hundred seventy-one million American dollars (Schreier, 2011).

Who was responsible?

Sony's rapid innovation business model resulted in releasing software and services with insufficient security measurements (Baker and Finkle, 2011). This allowed hackers to penetrate Sony's system and eventually gain access to seventy-seven million users' private data.

Were any escalation(s) stopped - how?

In order to assess the attack and secure its systems from further attacks, Sony took down and updated all its systems for twenty-four days. This gave enough time for the cybersecurity professionals to assess what was externally accessed and further secure its systems from any future attacks (Baker and Finkle, 2011).

Was the Business Continuity Plan instigated?

Sony's business plan was to innovate first in lieu of a secure system. However, after this attack, Sony started releasing various firmware updates focusing on its security aspects and updated all its online services and software with new and more secure code (Baker and Finkle, 2011).

Was the ICO notified?

Sony was fined 250,000 pounds over its weak security systems implemented. According to the ICO, a company responsible for a large number of credit card transactions and log-in details should have strong security systems implemented. (BBC, 2013)

Were affected individuals notified?

On April 26, 2011, Sony made a detailed public announcement for the attack, including the exact data leaked and began e-mailing customers with information for the safety steps required (Williams, 2011).

What were the social, legal, and ethical implications of the decisions made?

The ICO fined Sony 250,000 pounds for its insufficient security measurements. However, Sony's biggest losses appeared from its customers' lost trust.

References:

Baker, B., L and Finkle, J. (2011) Sony PlayStation suffers massive data breach Available from: https://www.reuters.com/article/us-sony-stoldendata-idUSTRE73P6WB20110426 [Accessed 06 July 2021].

BBC (2013) Sony fined over 'preventable' PlayStation data hack Available from: https://www.bbc.com/news/technology-21160818 [Accessed 06 July 2021].

Schreier, J. (2011) Sony Estimates $171 Million Loss From PSN Hack Available from: https://www.wired.com/2011/05/sony-psn-hack-losses/ [Accessed 06 July 2021].

Williams, M. (2011) PlayStation Network hack timeline Available from: https://www.networkworld.com/article/2202583/playstation-network-hack-timeline.html [Accessed 06 July 2021].