Unit 4 Seminar preparation - **Breach Analysis Case Study**

Case: Aadhaar (2018).

- What types of data were affected?
    - (KYC) - Aadhaar Has issued 12.2 Billion electronic **Know-Your-Customer** authentications (Unique Identification Authority of India, 2017) since it passed into Indian law as the Aadhaar Act 2016 (Ministry of Law and Justice, 2022).
    - Personal Identifier Data (PID)
        - Names
        - Thumb prints
        - Photos
        - Retina scans
        - Bank details
        - individual identity numbers

- What happened?
    - Aadhaar had been the victim of a biometric data leak in march 2018. The impact of this breach had been felt by 1.1 Billion people.
    - Adversaries gained access to the government database via a third party partner company API which had no access controls in place.
    - Data was then sold for as little as (Indian rupees) Rs 418 ($7) via a whatsapp group.

- Who was responsible?
    - For failure to implement API controls - Indane, a government owned subsidiary.
    - Some could argue Meta Platform, due to a whatsapp group selling stolen data (But complicated to argue due to encryption and privacy)
    - The hacker group remained anonymous but had asked for payments in Indian rupees.

- Were any escalation(s) stopped - how?
    - Delayed response to researchers advice.
    - Informed of the breach in january 2018 and action was taken against the exploit on march 23rd 2018 (Hill & Swinhoe, 2022)

- Was the Business Continuity Plan instigated?
    - Not instantly

- Was the ICO notified?
    - As far as i am aware, the answer is no. This may be because the ICO is part of UK GDPR. A further explanation about legal implications below.

- Were affected individuals notified?
    - It is not known how many European citizens have had their data compromised.
    - Due to Article 21 which is explained in more detail below, it is possible that every individual may not have been notified

- What were the social, legal and ethical implications of the decisions made?
    - Article 21 of the Constitution of India 1950, states, “No person shall be deprived of his life or personal liberty except according to procedure established by law” and that translates into meaning that those affected in the data breach may not be protected because the data falls under the Aadhaar Act 2016.
    - The Aadhaar Act means that non-citizens who spend more than 182 days in India within a 12 month period must also register their details and this is where it becomes complicated in compliance with the European General Data Protection Regulation (GDPR).
    - GDPR is the toughest privacy and security law in the world (GDPR.EU, 2020) but only applies to Aadhaar if the company encroaches into the EU and not on EU citizens in India
    - The UIDAI also applied to block journalists from exposing the leak under the Aadhaar Act 2016 (Nair 2018)

If you had been the ISM for the organisation you selected, what mitigations would you have put in place to stop any reoccurrences?

Carry Out a risk assessment (vulnerability scan and pentest) of all third party government departments who have access. Implement controls to reduce risk and ensure the Confidentiality of individual data via Identity and access management protocols with zero trust in mind.

References

Hill. M, & Swinhoe, D. (2022) The 15 biggest data breaches of the 21st century. Available from: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html [Accessed on 15th February 2023].

Ministry of Law and Justice (2022) Aadhaar Act 2016. Available from: https://www.indiacode.nic.in/ [Accessed 15th February 2023].

Nair. P, (2018) Aadhaar breach report: Reactions on freedom and privacy. Available from: https://www.csoonline.com/article/3448722/aadhaar-breach-report--reactions-on-freedom-and-privacy.html [Accessed on 16th February 2023].

Unique Identification Authority of India (2017) Aadhaar data. Available from: https://uidai.gov.in/aadhaar_dashboard/index.php) [Accessed 15th February 2023].