Week 10: Data Breach Case Study

Read Swinhoe, D., 2020. The 15 Biggest Data Breaches of The 21St Century. [online] CSO Online.

Select one of the cases by completing Data Breach choice. Once you have made your selection, you will be able to see the links to the case. Then complete a breach checklist as discussed in the lecturecast (reproduced below):

- What types of data were affected?

  According to the Data Protection Commission (2020), the adobe system compromise led to the exposure of customers' encrypted payment data, email addresses and encrypted passwords. The source code for Acrobat pdf document editing software and picture editing software Photoshop was illegally accessed (BBC News, 2013)

- What happened?

  The breach occurred via an intrusion into a public web facing server and used this compromised server to access other servers on the network (Office of the Australian Information Commissioner, 2015).

- Who was responsible?

  An unknown attacker from outside the organisation

- Were any escalation(s) stopped - how?

  The following steps were taken by Adobe to prevent escalation according to the Data Protection Commission (2020):

  - The impacted database server was disconnected from the network
  - Blacklisted IP addresses from which the attacker accessed their systems
  - All affected users had their password reset
  - Relevant administrator accounts passwords were changed.
  - The banks processing customer payments for Adobe were also notified of the breach, so they could take necessary measures to protect their customers' accounts.
  - Employed a third-party company to conduct an investigation of the cause of the security breach of its systems and to identify what data may have been compromised
  - Took actions to reduce the risks related to the theft of certain source-code elements
  - The breach was reported to law-enforcement authorities and notifications were issued to affected individuals alerting them of the security breach

- Was the Business Continuity Plan instigated? Yes, as explained above.

- Was the ICO notified?

  Yes. The breach happened between 30 August 2013 and 17 September 2013 and the ICO was notified in October 2013 (Office of the Australian Information Commissioner, 2015).

- Were affected individuals notified?

  Yes, also in October 2013.

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

  Adobe faced a lawsuit fined by 15 attorney general of participating states and had to pay $1m in settlement (Krebsonsecurity, 2016).

  Adobe's notification process could have been improved on as the news was first released by a security blogger, Brian Krebs before Adobe came public with the information (BBC News, 2013).

  For a company like Adobe, they could have also implemented basic security steps like hashing and salting to protect customers' passwords in their backup systems (Office of the Australian Information Commissioner, 2015). They failed to take adequate steps to protect customer information.

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

As recommended by the Office of the Australian Information Commissioner (2015), I would ensure the following:

- Strengthen the information security systems with multiple levels of protection.
- Ensure that sufficiently robust security measures are applied consistently across all systems.
- Regular review of data security processes.
- Engaging a suitable qualified external auditor to check that the implemented measures are adequate to strengthen the system.

References

BBC News (2013) Adobe hack: At least 38 million accounts breached. Available from: **https://www.bbc.com/news/technology-24740873** [Accessed 17 October 2021]

Data Protection Commission (2020) CaseStudies|DataProtection Commission. Available from: **https://dataprotection.ie/en/pre-gdpr/case-studies** [Accessed 04 October 2010]

Krebsonsecurity (2016) Adobe Fined $1M in Multistate Suit Over 2013 Breach; No Jail for Spamhaus Attacker Available from: https://krebsonsecurity.com/2016/11/adobe-fined-1m-in-multistate-suit-over-2013-breach-no-jail-for-spamhaus-attacker/ [Accessed 17 October 2021]

Office of the Australian Information Commissioner (2015) Adobe Systems Software Ireland Ltd: Own motion investigation report. Available from: https://www.oaic.gov.au/privacy/privacy-decisions/investigation-reports/adobe-systems-software-ireland-ltd-own-motion-investigation-report [Accessed 17 October 2021]