**Seminar 5 – Preparation - 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?

What happened?

Who was responsible?

Were any escalation(s) stopped - how?

Was the Business Continuity Plan instigated?

Was the ICO notified?

Were affected individuals notified?

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

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

**Case Study: Marriott International**

**What types of data were affected?**

PII (Personally Identifiable Information), including credit cards and passport numbers

According to Hill & Swinhoe (2021) “The data copied included guests’ names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, dates of birth, gender, arrival and departure information, reservation dates, and communication preferences. For some, the information also included payment card numbers and expiration dates, though these were apparently encrypted.”

**What happened?**

In November 2018 Marriott International (a US-based hospitality company) announced a data breach in their network affecting approximately 500 million guests. Marriot acquired Starwood in the year 2016 however according to Marriott’s investigation led by cyber security experts’; hackers gained unauthorized access to the Starwood network in 2014 (Starwood hotels, 2018). This is a typical example of an Advance Persistent Threat (APT) attack where hackers gain access to the network and remain hidden for a long period of time to gather information.

**Who was responsible?**

According to an article written by the New York Times (The New York Times Company, 2021) the attack was attributed “to a Chinese intelligence group seeking to gather data on US citizens”.

**Were any escalation(s) stopped - how?**

Yes, according to Hill and Swinhoe (2021) “On September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database. Marriott quickly engaged leading security experts to help determine what occurred”. It was discovered that two tools were used by hackers to take control of the administrator account i.e. Remote Access Trojan (RAT) and MimiKatz – a tool for sniffing out username/password combos in system memory (Fruhlinger, 2020). Furthermore Sorenson (2019) mentions that containment and access control measures were implemented. In addition the system was retired as of 18 December 2018.

**Was the Business Continuity Plan instigated?**

From the articles read, this is unclear as the data breach did not bring down the Marriott network. The immediate response to the security breach was to bring in security experts and consultants to conduct an investigation.

**Was the ICO notified?**

Yes, consequently ICO has fined Marriott International £18.4million for failing to keep millions of customers’ personal data secure (ICO, 2020).

**Were affected individuals notified?**

Yes, furthermore according to Sorenson (2019) a website was setup to determine if a specific client’s information was breached

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

According to Fruhlinger (2020) the data breach affected more than 500 million customers. Legally Marriott was fined £18.4million by the Information Commissioners Office (ICO, 2020).

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

* Keep encrypted data and the keys used to encrypt it separated from each other
* Phase out Starwood systems and accelerate security enhancements to its network.
* Implement access control together with an Identity and Access Management (IAM) system with MFA to any network devices.
* Implement endpoint security tools such as anti-virus and anti-malware.
* create a security monitoring team that constantly monitors the network. This includes unusual/suspicious access to database systems.

**References**

Starwood hotels (2018). *Original notice from November 30, 2018*. Available from: <http://starwoodstag.wpengine.com/wp-content/uploads/2019/05/us-en_First-Response.pdf> [Accessed 26 January 2022].

The New York Times Company (2021). Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing. Available from: <https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html> [Accessed 26 January 2022].

Hill, M. & Swinhoe, D (2021). 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 26 January 2022].

ICO (2020). ICO fines Marriott International Inc £18.4million for failing to keep customers’ personal data secure. Available from: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/> [Accessed 27 January 2022].

Fruhlinger, J (2020) Marriott data breach FAQ: How did it happen and what was the impact? Available from: <https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html> [Accessed 27 January 2022].

Sorenson, A (2019) Testimony of Arne Sorenson. Available from: <https://www.hsgac.senate.gov/imo/media/doc/Soresnson%20Testimony.pdf> [Accessed 27 January 2022].