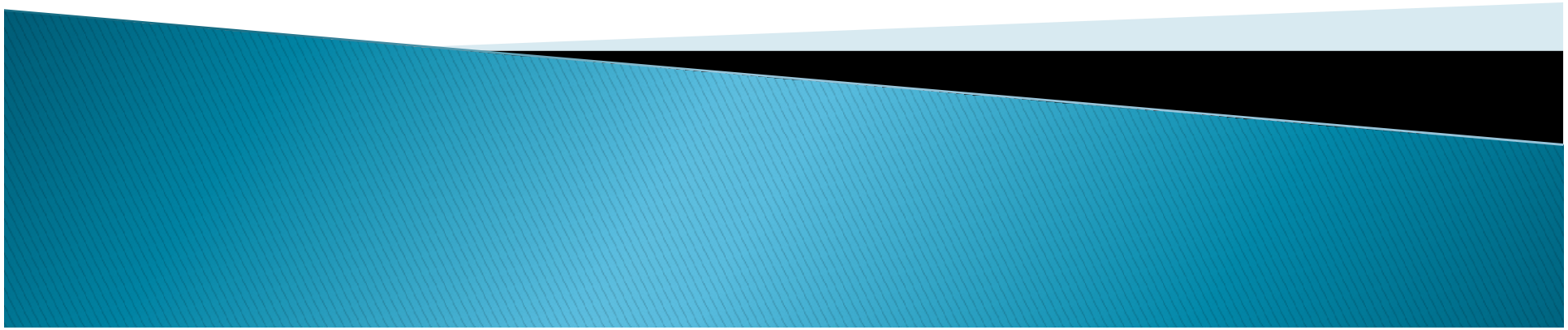
Data breach case study – Marriot International (Starwood)

Group 1

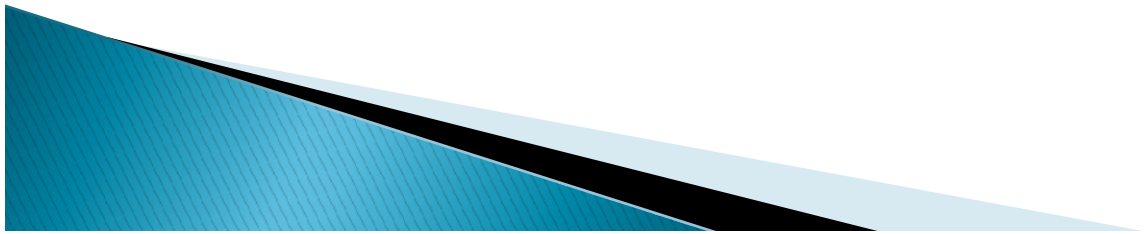


What types of data were affected ?

- Personally Identifiable Information (PII):

- Guest 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

- In some cases encrypted payment card numbers and expiration dates.

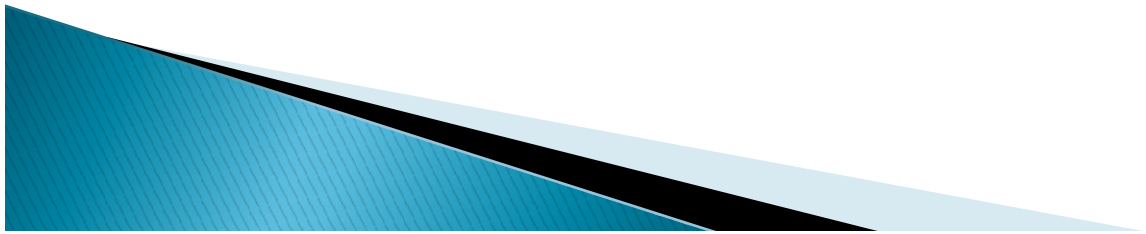


What happened ?

- Hackers gained unauthorized access to the Starwood network in 2014.
- Typical example of an Advanced Persistent Threat (APT).
- The attacker copied and encrypted information and took steps to delete the data.

Who was responsible?

- An article by New York Times attributed the attack to a Chinese intelligence group seeking to gather data on US citizens (The New York Times Company, 2021).



Were any escalation stopped and how?

- Yes, on September 8, 2018, Marriot received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database.
- Marriot engaged security experts to determine what occured.
- Two tools were used by hackers to take control of the administrator account:
  - Remote Access Trojana (RAT)
  - MimiKatz – Tool for sniffing username/ password combinations in system memory (Fruhlinger, 2020)
- Containment and access control measures were implemented (Sorenson, 2019)
- The system was retired in December 18 2018.

Was the Business Continuity Plan instigated?

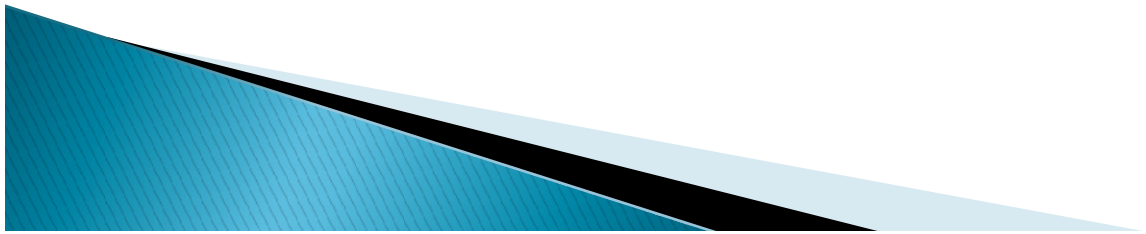
- Marriot carried out an investigation assisted by security experts following the breach and announced plans to phase out Starwood systems and accelerate security enhancements to its network.

Was the ICO notified?

- Yes, consequently ICO has fined Marriot International £ 18.4 million for failing millions of customers' personal data secure (ICO, 2020)

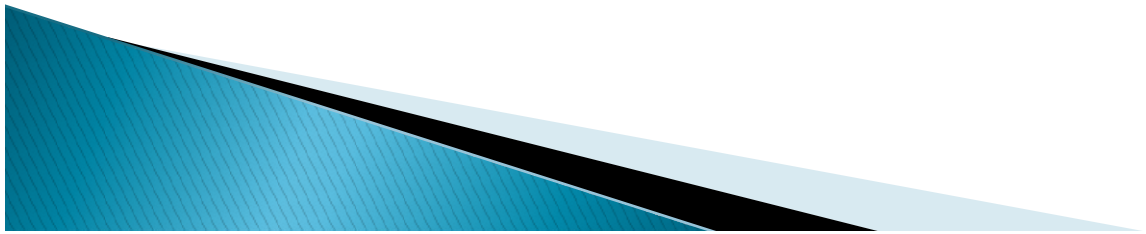
Were affected individuals notified?

- Yes, furthermore a website was setup to determine if a specific client's information was breached (Sorenson, 2019).



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

- The company was eventually fined £18.4 million (reduced from £99 million) by UK data governing body the Information Commissioner's Office (ICO) in 2020 for failing to keep more than 500 million customers' personal data secure.



References

- 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].

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

- 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 26January 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].

- 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].