

Marriot Under Fire

Stevie Johnson

Old Dominion University

Data breaches are increasingly common in today's digital landscape. According to IBM, a data breach is any security incident where unauthorized parties gain access to sensitive or confidential information, such as personal data (e.g., Social Security numbers, bank account details, healthcare data) and corporate data (e.g., customer records, intellectual property, financial information). A significant cybersecurity breach occurred in 2018 when Marriott International experienced an external malware attack that exposed personal information of approximately 500 million guests.

Marriott International bought Starwood in 2016. In 2018, the Starwood Preferred Guest program merged with the Marriott loyalty program. However, the attack on the Starwood database occurred due to trojan malware exploiting vulnerabilities in their outdated Microsoft point-of-sales reservation system, highlighting the system's security weaknesses. Hackers would attack a hotel's system because of its details dealing with personal information (names, dates of births, credit card info, and addresses of their customers) and the simple fact that most customers use the same password for multiple accounts it makes it easier for an hacker to access other accounts.. Another vulnerability of the hospitality industry is their relaxed security mechanisms making it easy for hackers to get inside their systems.” On September 7, 2018, a contractor named Accenture, who supports and manages the databases of Starwood Hotels and Resorts for Marriott International, noticed an unusual SQL query” (Amanulla, Niyaz 2024). This observation prompted them to let Marriott International know.

The aftermath of this monstrous attack led to Marriotts’ brand going through great losses that affected their revenue and reputation due to the corporation’s negligence in discovering the incident in the first stages of the merger which led to them being victims of the second largest

data breach. Marriot ended up paying a huge fine due to the implementation of the General Data Protection Regulation (Manglani 2024). Meanwhile the Customers lost trust in the luxurious company once they were informed of the data breach, and the fact that Starwood has had experience with data being leaked to the Darknet.

Security measures that could have been used to prevent the attack from happening are deploying data leak prevention and prevention mechanisms where UpToDate servers and equipment could have been installed to better prepare for an attack. Marriot could have conducted a background check on Starwood and seen they have been attacked before and could have corrected the issue before the merger. Customer awareness could have helped by customers having stronger passwords and 2 factor authentication making it harder for hackers to access their data.

Even after data breaches are common now days this study has made me aware of how to prevent my own personal information from being hacked, also how cyberattack can grow when it goes undetected, and neglected by companies. Hackers are getting smarter by the day, so our job is to stay sharp by raising awareness of the newest information and keeping up to date equipment to mediate these efforts.

References

- Amanulla, A., Niyaz, S., Samandari, A., & Wingreen, S. C. (2024). Marriot Data Breach: A Case Study Analysis. In *Information Technology Security and Risk Management* (1st ed., Vol. 1, pp. 241–245). Routledge. <https://doi.org/10.1201/9781003264415-35>
- Megha Manglani, "Compromised Systems, Compromised Data: A Technical Analysis of the Marriott Data Breach", *International Journal of Science and Research (IJSR)*, Volume 13 Issue 4, April 2024, pp. 176-180, <https://www.ijsr.net/getabstract.php?paperid=SR24402124923>, DOI: <https://www.doi.org/10.21275/SR24402124923>.