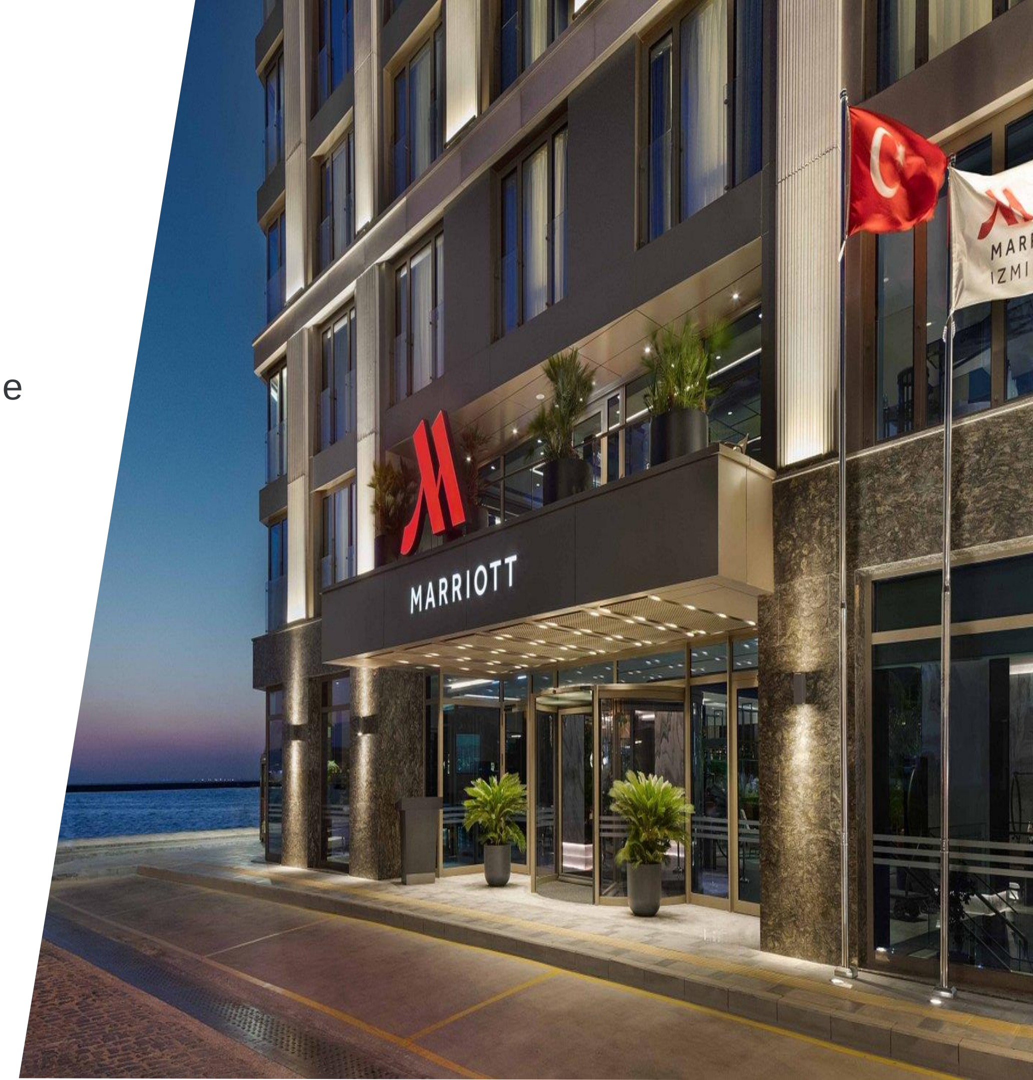
Breach Analysis Case Study

Unit 4 Seminar

by Andrius Busilas

What happened?

In September 2018, Marriott International announced that it had discovered a significant data breach affecting the guest reservation database of its subsidiary, Starwood Hotels. The breach exposed the personal information of approximately 500 million guests.



What types of data were affected?

The data breach at Marriott International's Starwood Hotels exposed a wide range of personal information about guests. The affected data types included:

- Personal Identification Information
- Reservation Details
- Payment Information

Who was responsible?

Were any escalation(s) stopped - how?

Marriott International took several steps to address and stop the escalation of the breach once it was discovered. Here are the key actions taken to mitigate the impact and enhance security:

1. Internal Security Alert
2. Engagement of Security Experts
3. Investigation and Decryption
4. Containment and Removal
5. System Phase-out and Security Enhancements
6. Regulatory Compliance and Fines

These actions collectively helped Marriott to stop the escalation of the breach, secure its systems, and prevent further unauthorized access to sensitive customer information.

Was the Business Continuity Plan instigated?

Marriott International's response to the Starwood data breach likely involved elements of their Business Continuity Plan (BCP), although specific details about the BCP's activation have not been publicly disclosed. Here are the indicative steps that align with typical BCP measures:

1. Immediate Response and Crisis Management
2. Investigation and Containment
3. Communication and Notification
4. Mitigation and Recovery
5. Long-term Improvements

Was the ICO notified?

The Information Commissioner's Office (ICO) was notified about the data breach. This is evident from the fact that the ICO conducted an investigation and subsequently fined Marriott International for failing to keep customers' personal data secure. The fine, initially set at £99 million, was eventually reduced to £18.4 million. This regulatory action indicates that Marriott complied with the requirement to report the breach to the ICO, which is a critical step in managing the aftermath of such incidents and part of regulatory compliance protocols.

Were affected individuals notified?

Yes, affected individuals were notified by Marriott International following the discovery of the data breach. In accordance with data protection regulations and best practices for handling data breaches, notifying affected individuals is a crucial step. Marriott made public statements and informed customers about the breach, including details about the types of data that were exposed.

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

The decisions made by Marriott International in response to the data breach had significant social, legal, and ethical implications:

Social Implications:

1. Loss of Trust
2. Customer Anxiety
3. Public Perception

Legal Implications:

1. Regulatory Fines
2. Compliance Requirements
3. Potential Lawsuits

Ethical Implications:

1. Responsibility and Accountability
2. Transparency
3. Preventive Measures

Conclusion

The Marriott data breach serves as a critical reminder of the importance of cybersecurity in protecting sensitive customer information. Despite Marriott’s efforts to manage the fallout and enhance security, the breach had lasting social, legal, and ethical implications. Companies must prioritize robust data protection measures, ensure compliance with regulatory standards, and act transparently and responsibly in the event of a data breach to maintain trust and safeguard against future incidents.

References

Denuwan, R. (2023) *Marriott International Data Breach. University of Plymouth*. https://www.researchgate.net/publication/372524901_Marriott_International_Data_Breach

Fruhlinger, J. (2020) *Marriott Data Breach FAQ: How did it happen and what was the impact?*, *CSO Online*. Available at: https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html#:~:text=In%20late%202018%2C%20the%20Marriott,being%20exfiltrated%20by%20the%20attackers. [Accessed: 03 July 2024].

Marriott (2018) *Marriott announces Starwood Guest Reservation Database Security Incident*, *Marriott News Center*. Available at: https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident (Accessed: 02 July 2024).

Perlroth, N., Tsang, A. & Satariano, A. (2018) *Marriott hacking exposes data of up to 500 million guests*, *The New York Times*. Available at: https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html [Accessed: 02 July 2024].

Swinhoe, D. (2022) *The 15 biggest data breaches of the 21st Century*, *CSO Online*. Available at: https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html [Accessed: 02 July 2024].

Young, K. (2021) Cyber case study: Marriott Data Breach, CoverLink Insurance - Ohio Insurance Agency. Available at: https://coverlink.com/case-study/marriott-data-breach/ [Accessed: 03 July 2024].