Marriott International (2018) Case Study

Marriott Starwood Properties and Guests

Attack Category

Sophisticated Cyber Attack

The attack category for the Marriott International data breach in 2018 was a sophisticated cyber attack. The attackers gained unauthorized access to the Starwood reservation database, compromising personal information of over 500 million guests, making it one of the largest data breaches in history. The attack highlights the need for companies to have robust security measures in place to protect sensitive information and reduce the risk of cyber attacks.

- According to the Identity Theft Resource Center, the Marriott breach was the second largest data breach in the history of the United States at the time, affecting over 500 million guests.
- A study by Bitglass found that the hospitality industry had the highest rate of data breaches among all industries, with almost 60% of breaches in the sector occurring in the first half of 2018.
- The same study found that the average cost of a data breach for a hotel or resort was estimated to be $41.67 per compromised record.

Marriott International is a multinational hospitality company with a portfolio of hotels and resorts spanning across 130 countries. In 2018, the company suffered a data breach that affected over 500 million guests who had made reservations at any of Marriott's Starwood properties.

The security incident involved unauthorized access to the Starwood guest reservation database, which contained sensitive information such as names, addresses, phone numbers, passport numbers, dates of birth, and more. The breach was discovered in September 2018 and was found to have begun in 2014. The investigation revealed that the attackers had used a sophisticated hacking technique and had accessed the database using stolen login credentials.

The data breach had significant consequences for Marriott and its guests. The company faced multiple lawsuits, investigations, and fines, and it also had to invest in extensive remediation efforts to protect the affected guests from potential harm. The breach also had a significant impact on Marriott's reputation, as the company was widely criticized for its poor handling of the incident and its slow response to the breach.

Timeline: Marriott Intl.

- 2014: The breach is believed to have started with unauthorized access to the Starwood reservation database.
- September 8, 2018: Marriott International announced the discovery of a data breach affecting its Starwood reservation system.
- November 30, 2018: Marriott International revealed that the data breach was more extensive than previously thought and that the personal information of up to 500 million guests was compromised
- December 2018: Marriott International began informing affected guests and offering them free identity theft monitoring and fraud consultation services.
- 2019: Marriott International faced numerous lawsuits over the data breach and reached settlements with various state attorneys general and financial institutions.

Vulnerabilities

- **Lack of proper encryption**: Marriott failed to properly encrypt sensitive information such as passport numbers, dates of birth, and other personal details, making it easier for attackers to access and steal the information.
- **Unsecured third-party systems**: Marriott relied on third-party systems to manage customer data, and some of these systems were not properly secured, leading to the compromise of customer information.
- **Outdated software**: Marriott used an outdated version of software, which had known vulnerabilities that the attackers were able to exploit.
- **Insufficient security monitoring**: Marriott did not have adequate systems in place to detect and respond to security incidents, which allowed the attackers to remain undetected for an extended period of time.

Rundown

- Overall, the data breach at Marriott International was the result of a combination of technical vulnerabilities, inadequate security measures, and a lack of proper data protection protocols. The company failed to adequately protect sensitive customer information, making it easier for attackers to gain access and steal the data.

Costs

•**Cost of investigating the breach**: Marriott reportedly spent around $28 million on the investigation and the remediation of the breach.
•**Legal expenses**: Marriott was facing several lawsuits from affected customers and shareholders. These lawsuits can be costly, both in terms of financial expenses and time spent in court.
•**Reputation damage**: The breach resulted in a loss of trust and reputation for Marriott, which could lead to a decline in business and reduced customer loyalty.
•**Customer compensation**: Marriott offered compensation to affected customers, including free identity theft protection and credit monitoring services. This cost could have been substantial, depending on the number of customers affected.
•**Implementation of security measures**: Marriott had to implement new security measures and upgrade its existing systems to prevent future breaches, which could have been expensive.
•**Loss of business**: Some customers may have chosen to avoid Marriott hotels in the wake of the breach, leading to a decline in revenue and potential loss of business.

Preventions

- **Improved Security Measures**: Marriott implemented stronger security measures to protect their systems and the sensitive data stored in them.
- **Enhanced Data Privacy Protections**: Marriott updated its privacy policies and procedures to better protect the personal information of its guests.
- **Improved Detection and Response Capabilities**: Marriott invested in advanced technology and trained its staff to better detect and respond to potential security incidents.
- **Third-Party Vendor Management**: Marriott reviewed and strengthened its relationship with third-party vendors to better manage and secure their access to Marriott's systems.
- **Customer Notification and Support**: Marriott notified affected customers about the data breach and provided them with resources and support to help them protect themselves from potential harm.