Instructions

Build an attack case study report using this template. If you need help, refer to the instructional video.

There are five content slides plus a title slide in this template. You can receive up to 20 points for each content slide. You need 80 points to pass this assignment.

For your best chance of success, pick an attack or breach with enough information and data so that you will be able to report the required information.

Replace the red text on each slide with your information and change the text color to black or white, depending on the background. You can change the font size, if needed.

When your report is complete, delete this slide and save your file as a PDF to submit for review.

Case Study

Advanced Persistent Threat (APT).

Marriott International

Attack Category: Advanced Persistent Threat (APT)

*APTs are responsible for a significant portion of major data breaches.

*APTs are often carried out by nation-state actors or highly skilled cybercriminals.

*APTs are typically well-resourced and patient, allowing them to remain undetected for extended periods of time.

Sources:

-Marriott International Data Breach FAQ (Marriott International)
-Marriott Data Breach: What You Need to Know (The New York Times)
-Marriott Data Breach Timeline (Security Week)

Company Description and Breach Summary

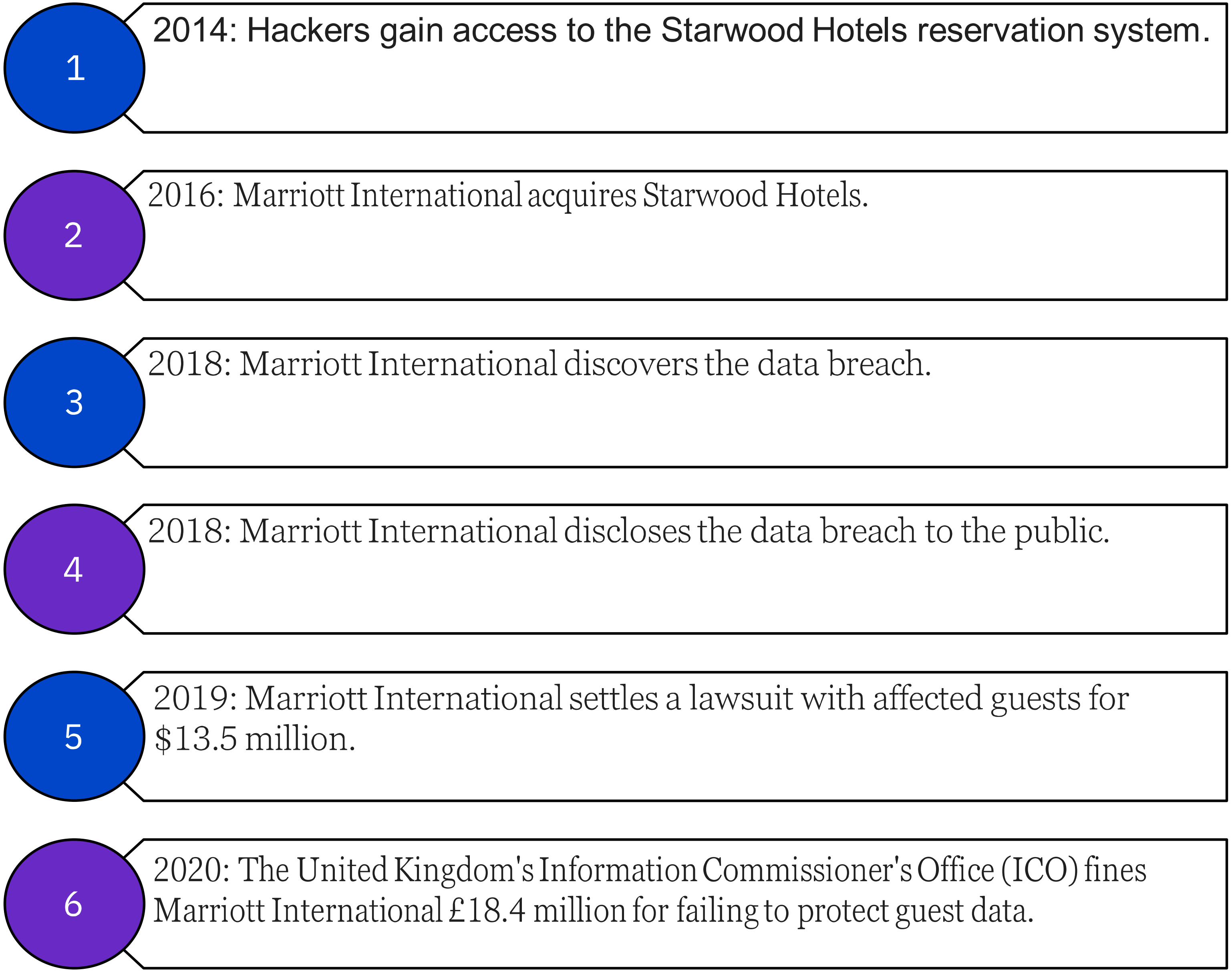
Marriott International, Inc. is an American multinational hospitality company that operates, franchises, and licenses lodging including hotel, residential, and timeshare properties. Founded in 1927 by J. Willard Marriott, the company is headquartered in Bethesda, Maryland.

Marriott International is the largest hotel chain in the world by number of rooms, with over 8,000 properties in 138 countries and territories. The company's portfolio includes 30 brands, ranging from luxury hotels such as The Ritz-Carlton and JW Marriott to select-service hotels such as Courtyard by Marriott and Fairfield Inn & Suites.

Marriott International is a major employer, with over 200,000 associates worldwide. The company is committed to social responsibility and sustainability, and has been recognized for its efforts in these areas

Incident summary: In 2018, Marriott International disclosed a data breach that affected up to 500 million guests. The breach occurred in 2014, when hackers gained access to the Starwood Hotels reservation system. The hackers were able to steal personal information such as names, addresses, passport numbers, and dates of birth. In some cases, the hackers also stole credit card numbers and expiration dates.

Timeline



1. 2014: Hackers gain access to the Starwood Hotels reservation system.
2. 2016: Marriott International acquires Starwood Hotels.
3. 2018: Marriott International discovers the data breach.
4. 2018: Marriott International discloses the data breach to the public.
5. 2019: Marriott International settles a lawsuit with affected guests for $13.5 million.
6. 2020: The United Kingdom's Information Commissioner's Office (ICO) fines Marriott International £18.4 million for failing to protect guest data.

Vulnerabilities

he Marriott data breach was a result of a number of vulnerabilities, including:

- Failure to migrate Starwood Hotels' reservation system to Marriott International's secure system. This allowed the hackers to continue to exploit vulnerabilities in the Starwood system.
- Lack of adequate security controls on the Starwood Hotels reservation system. The system was not adequately patched or monitored for suspicious activity.
- Failure to encrypt sensitive guest data. This allowed the hackers to steal sensitive information such as passport numbers and credit card numbers.
- Failure to adequately monitor the Starwood Hotels reservation system for suspicious activity. This allowed the hackers to remain undetected for an extended period of time.

These vulnerabilities allowed the hackers to gain access to the Starwood Hotels reservation system and steal the personal information of millions of guests.

Vulnerability 1

- Failure to migrate Starwood Hotels' reservation system to Marriott International's secure system.

Vulnerability 2

Lack of adequate security controls on the Starwood Hotels reservation system

Vulnerability 3

- Failure to adequately monitor the Starwood Hotels reservation system for suspicious activity.

Vulnerability 4

- Failure to encrypt sensitive guest data.

Costs and Prevention

Costs

•Marriott International has incurred significant costs as a result of the data breach, including:

- Legal fees
- Credit monitoring services for affected guests
- Public relations expenses
- Regulatory fines

Prevention

•Companies can take a number of steps to prevent data breaches, such as:

- Implementing a comprehensive security program
- Regularly monitoring for suspicious activity
- Encrypting sensitive data
- Providing security awareness training to employees
- Conducting regular security audits