

Starwood Hotel Business Impact Analyze



June 1, 2019

Marriot Hotel inc.

By : bohan zhang

Course code: info-6027

ID: 0814917

Assignment 1

Submission Date: 6/8/2019

# Introduction

# Since 2016, Marriott has gradually migrated IT system from Starwood. As the system migrating, it is necessary to assess Starwood’s IT system and find potential risk and vulnerability exists in the system. In this assessment, the reservation system will be examined to ensure the confidentiality and integrity of a thousand million users information. The risks will be covered from every perspective in IT includes human, technologies, and physical. Each risk will be rated and ranked based on its probability of occurrence and impact.

# BIA

# Please see attachment for the documented BIA form.

# Marriott Starwood Incidence timeline:

# Sep 7, 2018 - IBM Guardium detect an anomaly query at Starwood reservation database

# Sep 8, 2018 - Accenture informed Marriott IT that they found anomaly activity on Starwood reservation database

# Sep 10, 2018 - Marriott brought in a third party forensic investigator to help it’s IT staff uncover the severity of the hack

# Sep 17, 2018 - Forensic Investigators found RAT on Starwood network

# Oct 2018 - Forensic Investigators found Mimikats on Starwood IT system

# Nov 2018 - Forensic found this hack starts way back to July 2014

# Nov 13, 2018 - Investigators uncovered two encrypted files suggested potentially are sensitive customer data

# Nov 19, 2018- The files are decrypted and confirmed they are customer sensitive data

# Nov 30, 2018 - Marriott announced to public and informed authorities that it experienced a breach and affect over 500 million users [[1]](#footnote-1)

# Summary

In this assessment, we listed 6 risks potentially could harm Marriott hotel. The phishing attack ended up being the number one threat that could exploit the reservation system. Due to phishing attack (email, phone calls) usually hard spot, we recommend doing a phishing awareness training every three months in Starwood and Marriott hotels. This awareness training will help examine the ability the staffs handle social engineering. Also, we would recommend continuing rolling out new procedures to deal with social engineering and train employees to strictly follow these procedures.

The second threat Marriott hotel should strategically mitigate is the DDOS attack. This type of attack sometimes could bring a long downtime and hard to prevent. Allocating necessary budget to a third party company for handling DDOS traffic is necessary to mitigate this risk.

The third threat would exploit the reservation system is the Zero-day attack. This type of attack often is hard to predict since organized crime or individual constantly seeks ways to exploit the system. We recommend Marriott and Starwood hire professional pen-testers constantly penetrating the system and find vulnerabilities before the black hat hacker does. Ideally, this type of testing should conduct every three months. Also, the development team should strictly follow the SDLC to ensure the quality of the code. In addition, adding alarm systems, IPS/IDS would greatly reduce the risk of hackers get into the system through the zero-day.

Since the physical attacking and natural disaster could vary based on location, we recommend when layout the facility, considering the local environment and adding proper protection if it's necessary. Also, We recommend Marriot build hot sites to ensure high availability when a natural disaster or physical attacking happen.

# References

1. Gibson S. “Security Now Episode #705”, *Gibson Research Cop.* Accessed at June 1 2019. <https://www.grc.com/sn/sn-705.pdf>

2. “AIR Estimates Marriott Cyber Breach Direct Losses Could Reach $600 Million”, *Insurance Journal*, Dec 2018. <https://www.insurancejournal.com/news/national/2018/12/21/512741.htm>

3. “Marriott Breach – Learn From One of the Largest Breaches in History”, *IT Chapter,* <https://itchapter.com/wp-content/uploads/2019/01/Marriott-Breach-From-Info-Tech-Research-Group-Courtesy-of-IT-Chapter-2019-01-04.pdf>

4. Bhaktavatsalam S., Clark P., “Marriott Hit by Starwood Hack That Ranks Among Biggest Ever”, *Bloomberg,* <https://www.bloomberg.com/news/articles/2018-11-30/marriott-found-unauthorized-starwood-database-access-since-2014-jp3xbq64>

1. Gibson S. “Security Now Episode #705”, *Gibson Research Cop.* Accessed at June 1 2019. <https://www.grc.com/sn/sn-705.pdf> [↑](#footnote-ref-1)