Memorandum

To: Dr. Susan Helser

From: Muhammad Zainul Zahid

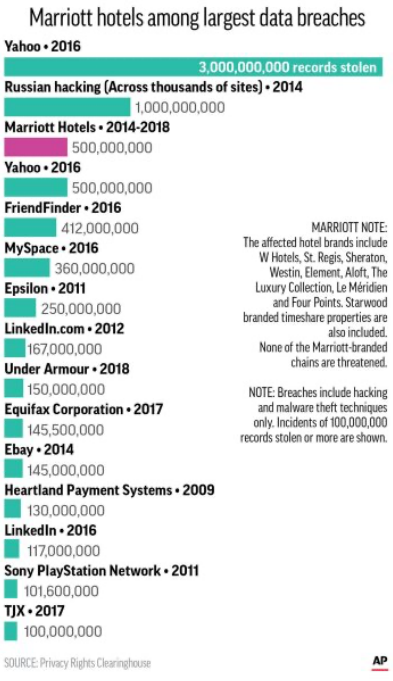
MBA BIS-521 Central Michigan University

Date: February 2, 2024

Subject: Marriott Hotel Cyberattack: Analysis and Conclusions

I. Overview

The investigation of the cyberattack on Marriott Hotels is described in this letter, with particular attention paid to monetary damages, the exposure of employee data, and possible hostile takeovers of Internet of Things devices or other cloud-related occurrences. Data belonging to an estimated 339 million guests was exposed as a result of the breach, which happened in 2014 but was not discovered until 2018.



II. Context

The hack started in Starwood Hotels' antiquated IT system, which Marriott purchased in 2016. Due to its persistent weaknesses, the compromised system added to the massive data leak. The Starwood system was breached by hackers who encrypted and erased data, exposing private guest data such as names, addresses, passport numbers, and credit card information.

III. The Nature of the Breach

By taking advantage of flaws in Starwood's unsecure reservation system, phishing and email spoofing were used to enable the attack against Marriott. The scenario was made worse by Starwood's IT systems not being integrated after the acquisition and the subsequent IT staff layoffs, which prolonged the damaged system's existence.

IV. Attack's Attribution

There are hints that the attack was funded by the state and connected to a Chinese espionage operation. The attack techniques and coding patterns match Chinese hackers' prior endeavors. It's noteworthy that there may have been ulterior intentions for the stolen guest records because they weren't put up for sale on the dark web.

V. Consequences for Marriott

Because of the data breach, Marriott was subject to large financial penalties as well as class-action lawsuits. Marriott was fined $23.8 million by the Information Commissioner's Office (ICO) of the United Kingdom for violating the security standards mandated by the General Data

Protection Regulation (GDPR). The brand also experienced a drop in consumer satisfaction ratings and perhaps long-term damage to visitor loyalty.

VI. Preventive Actions

Hotels, particularly those in the hospitality sector, should give priority to the following in order to prevent a similar data breach:

1. Encrypt visitor Data: To protect visitor data, put strong encryption methods in place.

2. Frequent Security Updates: To fix vulnerabilities, keep all systems updated with the newest software versions and security patches.

3. Alert Systems: Install alert systems to quickly recognize and address possible security breaches.

4. Communication Plan: Create a thorough plan that outlines how you will notify customers in the case of a security breach, with a focus on prompt and transparent disclosure.

5. Awareness and Training for Employees: Security Training Courses. Provide thorough cybersecurity training courses and put them into action for every employee.

Stress how crucial it is to identify and report phishing attacks.

6. Drills for Incident Response: Test the IT team's incident response capabilities on a regular basis by conducting drills. Make certain that every employee is aware of the procedures for reporting and handling security incidents.

7. Management of Vendors and Third Parties:

Vendor Security Evaluations: To review and verify the security procedures of outside service providers, implement a thorough vendor security evaluation procedure.

8. Agreements for Data Protection: Include strict data protection provisions in vendor contracts that highlight the importance of adhering to security standards.

VII. Concluding Remarks

Proactive cybersecurity precautions are crucial, as demonstrated by the Marriott Hotels cyberattack. Hotels may reduce the risk of data breaches and preserve consumer trust by fixing vulnerabilities, putting encryption in place, and keeping up with security updates. The investigation's conclusions emphasize the necessity of continuing diligence and implementing best practices to guarantee the security of sensitive data.

References

1. Jordan Hollander. (2020, December 9). Marriott Data Breach FAQ: What Really Happened? Hotel Tech Report. https://hoteltechreport.com/news/marriott-data-breach.
1. Carter, L. (2021, September 27). 10 Biggest Cyber Attacks in History. Clear Insurance. https://clearinsurance.com.au/10-biggest-cyber-attacks-in-history/.
2. Whitman, M. (2021). *Principles of Information Security* (7th ed.). Cengage Learning US. https://online.vitalsource.com/books/9780357506561.
3. Grama, J. L. (2020). *Legal and Privacy Issues in Information Security* (3rd ed.). Jones & Bartlett Learning. https://online.vitalsource.com/books/9781284231465.
4. Fazzini, K. (n.d.). The Marriott hack that stole data from 500 million people started four years ago — investors should ask how the company missed it. CNBC. https://www.cnbc.com/2018/11/30/marriott-hack-raises-questions-about-merger-diligence-tools-in-use.html.
5. Marriott security breach exposed data of up to 500M guests. (2018, November 30). AP News. https://apnews.com/article/d496fce7a77347d6aa058470d38a69bc.