Group 5: My Pham, Cody Blanchard, Sukruta Srinivas, William Marty, Reshma Maliakkal

Professor Joseph Mauriello

ACCT 6336-501

10 April, 2019

Assignment 3

Cyber Security Risk - Marriott

1. Overview of Marriott International

Marriott International is known as the world's largest hotel company based in Bethesda, Maryland, USA by providing "the most powerful portfolio in the industry" ("We Are Marriott International"). Founded in 1927 by J. Willard and Alice Marriott, the company now offers 30 brands and over 6,900 properties in 130 countries and territories ("We Are Marriott International"). According to Marriott.com, the company has remained their core values as "put people first," "pursue excellence," "embrace change," "act with integrity," and "serve our world". Their competitive advantage is mainly their brand name with "pricing power, recurring fee business model, significant switching costs for its property owners, long contracts and scale" ("Overview Of Marriott's Business Model."). Marriott.com also claims that the company's asset-light franchise and management contracts account for over 95% of their operating profit.

Marriott has a big team of executive members to serve the company. According to Marriott.com, J. W. Marriott, Jr. is the Executive Chairman and Chairman of the Board, while Arne M. Sorenson is the President and Chief Executive Officer, and Bao Giang Val Bauduin is the Controller and Chief Accounting Office. Regarding the other executive members, David J. Grissen serves as the Group President, Leeny Oberg serves as the Chief Financial Officer, while Deborah Marriott Harrison and Ronald T. Harrison serve as Glober Officer of Culture and Business Councils and Global Officer of Architecture and Construction, respectively ("Executive Leadership"). Marriott also has vice presidents for different departments. Anthony G. Capuano is the Executive Vice President and the Global Chief Development Officer, whereas Bancroft S. Gordon is both the Vice President and the Assistant General Counsel and Corporate Secretary. Carolyn B. Handlon works as the Executive Vice President of Finance and Global Treasurer, whereas David A. Rodriguez works as the Executive Vice President & Global Chief Human Resources Officer, and Rena H. Reiss serves as the Executive Vice President and General Counsel ("Executive Leadership"). Marriott.com informs that in 2002, the company chose Ernst & Young as their independent auditor, replacing Arthur Andersen LLP, which had served as their independent accountants since 1959.

2. Data Breach in 2018

Marriott International announced a large-scale data breach on November 30, 2018 with their Starwood subsidiary. Marriott acquired Starwood in 2016 for $13.6 billion ("Marriott Starwood Data Breach Highlights Silent Cyber Risk in Acquisitions"). Within days of announcing the deal, Starwood disclosed of their security breach. Also, with the acquisition, Marriott expected the popular loyalty program of Starwood would bring more customers to their Courtyards and Residence Inns, but little did they know that they were getting involved in a major data breach, according to Insurance Journal.

When the internal security tool of Marriott, IBM Guardium, alerted an unauthorized access into the customer database on September 8, 2018, Marriott discovered the hackers had access to the information from 2014 (O'Flaherty). An anomaly in the database was found when a query from the administrator returned the count of rows. This indicated a human interference with the database (O'Flaherty). When Marriott engaged security officials in an investigation, they discovered that the hackers had encrypted the data and were attempting to extract it. Upon decryption, they discovered it to be the Starwood reservation database ("Starwood Guest Reservation Database Security Incident"). The intense investigation revealed the malware that was present in Starwood system. A remote access trojan (RAT) was found in the system which the hackers used to gain access, surveil and have power over the computers. With Marriott's further investigation, a penetration tool called Mimikatz was found which raised suspicions as the tool could be used to gain usernames and passwords. Investigators suspected that the hackers used the tool to obtain the data and moved from Starwood to other parts of the network (O'Flaherty).

The data breach exposed customer information of up to 500 million people. It involved all customers who made reservations from 2014 to September 2018 (Perlroth). Hackers accessed sensitive information such as name, address, phone numbers, email address, passport number, date of birth, gender, Starwood loyalty program account and reservation information. Along with customer information, their payment card details were also stolen. Though the payment card numbers were encrypted, Marriott expressed that they were not sure if the hackers had decrypted the numbers and expiration dates. All the Starwood properties were affected by the breach, including Sheraton, Westin, W Hotels, St. Regis, Four Points, Aloft, Le Meridien, Tribute, Design Hotels, Element and Luxury Collection ("The Marriott Data Breach"). It is speculated that Marriott was the target of nation-state hackers who tracked down movements of diplomats, spies, military officials and business executives. Even if the speculation is ruled out, and if the hack was the action of a mere profit seeker, the valuable data could be used for misdeeds such as identity theft, fraud and credential stuffing (Telford, Taylor, and Craig Timberg).

Marriott's biggest asset is their brand and network of customers, and this hack definitely caused an impact on the brand name. With the fraught acquisition, Marriott failed to recognize the already prevalent data breach and could not anticipate the damages they were embarking into. As a result, they left a great number of customers dissatisfied. Hackers' foothold in Starwood system caused Marriott's share to dip to 5% ("Marriott Starwood Data Breach Highlights Silent Cyber Risk in Acquisitions"). The onslaught costed Marriott $28 million, before tax, but the expense of $25 million was recovered by insurance (Ting, Deanna, and Deanna Ting). Along with the expenses, Marriott faced class-action lawsuits filed by customers and investors. Though Marriott had to shed a small amount for the breach, they now had to consider the cybersecurity incident lawsuits, which were expected to cost them more than $10 million (SecurityWeek). Apart from the incident, Marriott was the target of many labor strikes at their hotels throughout US and faced an incentive loss of about $7 million (Ting, Deanna, and Deanna Ting).

There were many speculations pointing to Chinese government with goals of espionage rather than a financial gain. The clues left behind by the hackers indicated that they were working for Chinese government's intelligence (CNBC). Many private investigators claimed the tools and techniques used in this data breach were previously found in attacks associated with Chinese hackers. Identification of the attackers was complicated by the fact that the tools were also used by other hackers, and since China had the lead in this case, it was assumed to be the work of Chinese hackers (CNBC). There are other speculations where the attackers were considered to be government-specific as they utilized enough time and worked quietly inside the network, unlike cyber criminals who work for a financial gain and get the work done in a quick span of time (CNBC). Also, according to Brewster, there were botnets playing a major role in the breach and the prime suspects were the Russians. There were vulnerabilities in the company website which became a prey to SQL injection bug which could have led to hackers exploiting the vulnerability. Marriott claimed to be working on finding out what occurred and how they could serve the customers best in light of the incident; however, they did not find the identity of the attackers yet (New York Times: Chinese Hackers behind Massive Marriott Breach).

3. Controls Involved

The data breach incident appears to have taken multiple failures in order to have gone unaddressed and un-resolved since 2014. Although there is not an exact report detailing the controls that failed, what has been reported as possible failures include human errors, website forms protection mechanisms, data loss prevention controls, network controls, and anti-malware controls (Brewster).

According to Thomas Brewster, before Starwood was acquired by Marriott in 2015, Starwood's website had been vulnerable to a SQL Injection attacks in 2014. Brewster stated that, "known as an SQL injection bug, it could have been exploited to gain access to Starwood databases," and "such vulnerabilities and even services offering to hack Starwood were being offered amongst hackers on the dark Web back in 2014" (Brewster). Marriott became aware of the issue after they completed their purchase of Starwood. Usually such a vulnerability could have been resolved by the company's implementing sanitization and validation of a user input on Starwood's website, making it difficult for any malicious injection code to execute on their servers.

Brewster also noted that internally, Starwood's ServiceNow cloud computing service contained a guessable non-complex password for one of its service accounts, making it easy for a malicious actor to guess the password, access important records, and do more reconnaissance of where crown jewels were being stored. Better practices for password use could have prevented a malicious actor from guessing passwords or running brute dictionary attacks to gain access.

On the network level, KrebsonSecurity.com noted that the malicious actors were getting away with the 4-year data breach because they were able to encrypt stolen data, making it difficult for Data Loss Prevention software to detect information being stolen in network transit. Even though credit card information was being protected by encryption, Marriott would not rule out the possibility of the encryption key being stolen as well and being included with the encrypted stolen data. ("Marriott: Data On 500 Million Guests Stolen In 4-Year Breach — Krebs On Security"). According to Brewster, ties to Russian hacking groups were found as principle malicious actors, botnets were used to access victim systems in Starwood's network (Brewster). Intrusion Protection/Detection Security control and SIEM tool could have been used to notice incoming/outgoing traffic from databases to external IP where the malicious actor could have been performing acts.

4. Recommendations

Given the vast scale of the Marriott data breach, it can't be overstated how crucial it is that the company takes proper steps to address their security issues. If consumers lose confidence in their information security with Marriott, it could have a significant impact on their business moving forward, and as such it is vital that Marriott both takes steps to help customers that were affected by the breach, as well as implement controls that will stop such attacks from succeeding in the future.

First and foremost, Marriott must make amends with those guests that had their data stolen in the hacks. Fortunately, the company has already taken steps to do exactly that. According to The Federal Trade Commission, a website was set up so that customers can search for steps they should take next to protect themselves and their identity moving forward (The Marriott Data Breach). Unfortunately, it appears that Marriott was still struggling to pinpoint exactly how many of their customers were affected. As of March 2019, they only had estimates for the raw number of customers with stolen data, and this was months after the incident was first made public (Starwood Guest Reservation). More emphasis should be placed on protecting those customers affected by the breach, or Marriott's business could suffer immensely in the future.

While reactive actions are obviously necessary in a situation like this, preventing these circumstances from repeating is even more important. Marriott's Starwoods subsidiaries, acquired in 2015, have had numerous security issues in the past prior to that acquisition. Indeed, just days after Marriott acquired the chain, Starwood fell victim to malware that stole credit card numbers at 54 Starwood locations across the country (Telford & Timberg). In spite of these glaring red flags, Marriott was lax in phasing Starwood's vulnerable software out in favor of their own more secure systems (Romm). Given that Marriott has several other subsidiaries and is a constantly growing brand, it is imperative they ensure those subsidiaries all have proper security systems in place so that this breach is not repeated in the near future.

5. Disclosure Discussion

The Marriott Hotels first found out about their potential vulnerability on September 8, 2018; management then issued an official statement announcing the breach November 30, 2018 (Curtis 1). The attack was undetected for four years prior to the announcement (Curtis 1). Marriott did disclose the breach immediately after being aware of it and confirming that it had occurred. The company followed the best policy in regards to disclosure by informing the public of what had occurred as early as they did, and it was necessary to disclose the data breach due to the sheer volume and types of data that were stolen with "27 million users ha[ving lost] some combination of the following details compromised: name, mailing address, phone number, email address, passport number, Starwood Preferred Guest (SPG) account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences" (Curtis 2).

A company should always be transparent when customer data is compromised, because failure to do so can risk hurting the company image and promote consumer distrust of a company, especially if the company were later found out to have intentionally hidden or omitted what had happened from their customers. In the current marketplace, consumer loyalty is incredibly important, and creating a relationship between consumers and companies is the best way to ensure repeat business. Although revealing a data breach can weaken a company's stock prices and immediate consumer perception of the company, addressing the issue directly promotes transparency and allows consumers to feel as though the company cares about maintaining their relationship with customers through honesty. Additionally, revealing a data breach allows a company to control the narrative in which a data breach is exposed to the public, and also gives it the opportunity to list measures that are being placed to prevent further damage and minimize current risk.

Works Cited

Brewster, Thomas. "Revealed: Marriott's 500 Million Hack Came After A String Of Security Breaches". *Forbes.Com*, 2019, https://www.forbes.com/sites/thomasbrewster/2018/12/03/revealed-marriotts-500-million-hack-came-after-a-string-of-security-breaches/#3f2081f3546f.

Curtis, Ammon. "Marriott: Starwood Data Breach Affected Up To 500 Million Guests". Blog.Infoarmor.Com, 2018, https://blog.infoarmor.com/employees/marriott-starwood-data-breach-500-million-guests. Accessed 4 Apr 2019.

CNBC. “Clues in Marriott Hack Are Said to Implicate China.” *CNBC*, CNBC, 6 Dec. 2018, www.cnbc.com/2018/12/06/clues-in-marriott-hack-are-said-to-implicate-china.html.

“Data Breach Cost Marriott $28 Million So Far.” *SecurityWeek*, www.securityweek.com/data-breach-cost-marriott-28-million-so-far.

“Executive Leadership.” *Marriot.com*, news.marriott.com/p/executive-leadership/.

"Marriott: Data On 500 Million Guests Stolen In 4-Year Breach — Krebs On Security". *Krebsonsecurity.Com*, 2019, https://krebsonsecurity.com/2018/11/marriott-data-on-500-million-guests-stolen-in-4-year-breach/. Accessed 8 Apr 2019.

“Marriott Selects Ernst & Young as Independent Auditor.” *Marriot.com*, marriott.gcs-web.com/news-releases/news-release-details/marriott-selects-ernst-young-independent-auditor.

“Marriott Starwood Data Breach Highlights Silent Cyber Risk in Acquisitions.” *Insurance Journal*, 3 Dec. 2018, www.insurancejournal.com/news/national/2018/12/03/510811.htm.

O'Flaherty, Kate. “Marriott CEO Reveals New Details About Mega Breach.” *Forbes*, Forbes Magazine, 11 Mar. 2019, www.forbes.com/sites/kateoflahertyuk/2019/03/11/marriott-ceo-reveals-new-details-about-mega-breach/#179bdec1155c.

"Overview Of Marriott's Business Model." *Seeking Alpha*, seekingalpha.com/article/4032181-overview-marriotts-business-model.

Perlroth, Nicole, et al. "Marriott Hacking Exposes Data of Up to 500 Million Guests." *The New York Times*, The New York Times, 30 Nov. 2018,

www.nytimes.com/2018/11/30/business/marriott-data-breach.html

Romm, Tony. "Senators Slam Equifax, Marriott Executives for Massive Data Breaches." *The Washington Post*, WP Company, 7 Mar. 2019, www.washingtonpost.com/technology/2019/03/07/senators-slam-equifax-marriott-executives-massive-data-breaches/?utm_term=.ea990c1eaba5.

"Starwood Guest Reservation Database Security Incident." *Starwood Reservation Database Security Incident*, answers.kroll.com/.

Telford, Taylor, and Craig Timberg. "Marriott Discloses Massive Data Breach Affecting up to 500 Million Guests." *The Washington Post*, WP Company, 30 Nov. 2018, www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/?noredirect=on&utm_term=.3e99ce0257b9.

"The Marriott Data Breach." *Consumer Information*, 4 Dec. 2018, www.consumer.ftc.gov/blog/2018/12/marriott-data-breach.

Ting, Deanna, and Deanna Ting. "Marriott Cites Growing Pains Following Data Breach, Labor Strikes." *Skift*, Skift, 2 Mar. 2019, skift.com/2019/03/01/marriott-cites-growing-pains-following-data-breach-labor-strikes/.

"We Are Marriott International." *Marriot.com*, www.marriott.com/marriott/aboutmarriott.mi.

“New York Times: Chinese Hackers behind Massive Marriott Breach.” *FOX2now.Com*, 12 Dec. 2018,

fox2now.com/2018/12/12/new-york-times-chinese-hackers-behind-massive-marriott-breach/.