The Marriot Data Breach

This report explores the intrusion into the Starwood Hotel Reservation System, the resulting data loss and mitigation strategies

Author:

Casey Munga

Teacher:

Luis Guadeloupe

Course:

Principles of Information Systems Security

The Betrayal by Marriott

In 2014 Marriot International, a family chain named after their founders Alice and John Willard Marriott, was in negotiations to acquire Starwood Hotel Chain a group of luxury hotels that were an extremely profitable enterprise. The deal only became a reality on November 16th, 2015, at a cost of 13.6 Billion Dollars.

On November 20th, 2015, Starwood's president announced that 54 of the hotel's chain was attacked by a malware virus whose focus was to acquire credit card information such as the name, credit card number, security code and expiration date. The breach compromised the company's Point of Sale System in their restaurants, gift shops (Washington post) and bars. Third party experts were hired with the requisite forensics experience who determined that the Reservation System and their Preferred Guest Membership System was excluded from the breach.

At that time, the management team indicated that security measures were going to be put in place to protect their customers' data. It was confirmed that the breach happened between Nov 2014 - October 2015 before Marriott International bought the chain. As a courtesy, the company offered to cover their clients by paying for free identity and credit checks

By September 23rd, 2016, the Starwood Preferred Program (SPG), was given access to link into the Marriott Members Program. The virus hidden in the Starwood reservation system was passed and proliferated throughout the Marriott System.

On September 18th 2018 , an issue was discovered by Accenture, who was Starwood's internal Cyber Security team. They discovered that a breach had occurred. The tool, IBM Security Guardium, that they were using detected that an administrator account was accessing an unusual set of database queries. After investigating the latest security incident, it was determined that the account had been hijacked. A Remote Access Trojan, possibly an act of email phishing was the culprit. Accompanied with the RAT was MimiKatz, a worm whose focus was stealing passwords.

MimiKatz works as an exploitation device that roots the memory and gains access to passwords, PINS and hashes. It uses destructive forces such as pass-the-hash attack or pass-the-ticket attacks.

Pass-the-hash intrusion modus-operandi is used to gain access to passwords that have been scraped from the system ram. The already hashed password is captured and used as authentication to the system. No decryption is necessary.

Pass-the-hash is used on Windows, Linux, and Unix systems where Single Sign On (SSO) are easily exploited. Windows OS is especially vulnerable as the hashed passwords are deposited in the Security Accounts Manager. Any time a login occurs, a footprint of the credentials is stored. Other places such as AD (Active Directory), LSASS (Local Security Authority Subsystem) and the Credit Manager are fruitful stores of authorization credentials.

Pass-the-ticket is quite similar to Pass-the-hash except it uses Kerberos tickets and its expiration time is a mere 10 hours which can be extended to 7 days. Both Pass-the-hash and pass-the-ticket attacks are extremely dangerous as it escalates privileges as it steals more credentials.

Marriott did encrypt a lot of the data, but they stored the encryption keys on the same server. Both data and those keys were compressed and removed from the system by the hackers.

Prior to the merger, Starwood contractors had been using IBM Guardium software to protect their infrastructure. The virus seemed to have been planted after the deal and subsequent to when the negotiations between Marriot and Starwood had started. During this shakeup, we can be sure that some employee turn-over had started. However, when Marriott merged with Starwood, most of the IT staff who were designated to protect the system were fired. The system was left vulnerable and open to attack on a bigger scale and the hackers, understanding that deficit, took advantage of the ensuing security gaps.

Marriott was able to reduce the expenses as the payout in employee salaries decreased, but they would pay a much bigger price as unprotected data and trojans were left unsecured. The trojan had access to:

- 383 M client records
- 18.5 M encrypted passport id numbers
- 9.1 M encrypted credit card numbers
- 5.25 M unencrypted passports id numbers
- 385,000 valid credit card numbers.

As a result of the breach, Marriott was sued. Countries affected were Asia, Canada, Europe, and USA. The class action lawsuit suit levied a potential worth of $12.5 Billion dollars at the company. Given the fact that Marriott had a presence in the European Union they were obligated to be in compliance with the GDPR (General Data Protection Regulation), which stringently regulates the access and protection of its citizens data. Marriott is being sued by the GDPR for the sum of $123 Million dollars.

Marriott should have done their due diligence. Not only did they fail to protect the customer's data, they broke the following USA laws.

1. Fair and Accurate Credit Transactions Act9FACTA) (15 U.S. code -1681) requiring the truncation and secure destruction of card information and they must obey the Payment Card Industry Data Security Standard (PCI-DSS)
2. Gramm-Leach-Bliley Act, which states guidelines on the protection of sensitive data.
3. Though there is currently no Federal breach laws many states have enacted data breach laws.
4. FTC has broad language but has indicated that the security of data must be 'reasonable'.
5. Federal Information Processing Standards (FIPS)

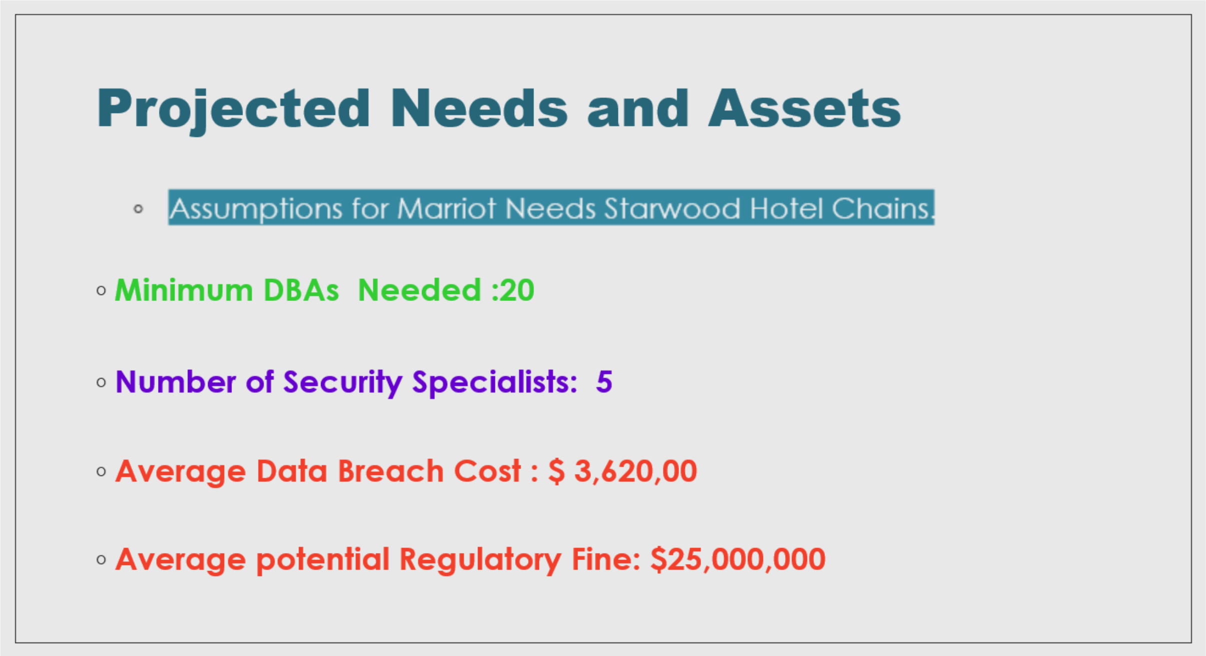
FCC has produced a Cyber Security Planning Guide that lists specifically the desired protections and outcomes under the "Scams and Frauds" Best Practices. What is obvious is Marriot did not do what was "reasonable".

Here is where Marriott failed.

1. They did not "Train Employees to recognize Social Engineering": Someone let the virus in.
2. They did not "Protect Against On-line Fraud":
3. They did not "Protect Against Phishing".
4. They did not "Protect against Malware": They fired most of the IT Cyber infrastructure.
5. They did not "Develop a layered approach to guard against Malicious Software": In fact, it stayed hidden on the system.
6. They did not have "Strong Password policies"
7. They did not" Encrypt sensitive data": 5.25 million unencrypted passports were left on the system.

What is shocking is that Marriot already knew that Starwood had a breach prior on their POS systems, and they had the IBM Guardium System available and already in use. Yet, they neglected to use it effectively and traded the added cash that they had retained from the fired IT and Network Specialists and did not use the money to enhance their security.

In projecting the minimum needs of Starwood, (Figure 1) we have estimated that with the projection and the cost of a data breach and consequent regulatory fines.

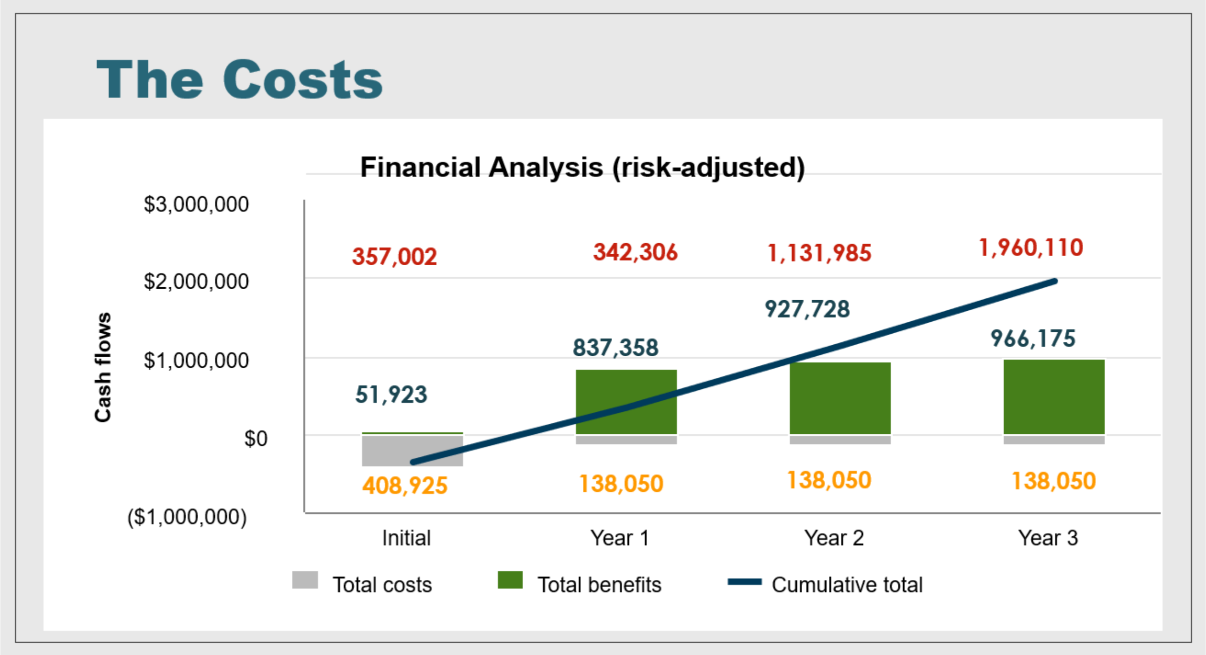


Projected Needs and Assets

- Assumptions for Marriot Needs Starwood Hotel Chains.

- Minimum DBAs Needed :20
- Number of Security Specialists: 5
- Average Data Breach Cost : $ 3,620,00
- Average potential Regulatory Fine: $25,000,000

Figure 1: Minimum needs for Starwood and Marriott



The Costs

IBM Benefit Calculator

Figure 2: Costs for Implementing IBM Guardium System.

The costs to maximize and implement the Guardium System is self-explanatory.

The initial investment for the Needs in fig1 is $408,925 and the immediate benefit is approx. $52,000. The total cost for end-to-end security is approximately $357,000.

The cost for year 1 is $138,000.

We must consider the cost still owed for the initial year:138,000+ 408,925=$546.925

The Benefit for year 1 =$837,358 - $546,925

Total benefit after costs are paid is S342,306.

We can see that by the end of the first year the software initial investments costs would have been paid off and there is a benefit.

If we follow this trend, then we can see that the cumulative benefits in year 3 is $1,960,110.

This system would have protected Marriott had it been properly implemented as the software guards against viruses, malicious attacks, and "monitors unauthorized transactions" by external hackers' and internal threats. It also lends itself to compliance and firewall-blocking, quarantines, auditing, and compliancy to FIPS.

The cost of $100,000 over 3 years to implement and safeguard its customers came instead with a 126-million-dollar charge tag, in fines and a suit by April 2019 on Marriott. In July 2019, GRPR Lodged a fine of 120 million. Some $25 million dollars of the monies were covered by cyber insurance.

One would have hoped that the promises made, and the lessons learned, would have improved Marriot's concept of the importance of cybersecurity. That is not the case. This year, on March 31st, 2020 , hackers intruded into the internal system and stole 5.2Million guests' private information. This is proof positive that Marriott has not hardened its defenses and information technology systems remains out of compliance.

Governmental controls need to be implemented regarding cybersecurity practices and engrained into law. Stiffer penalties need to be levied at firms falling out of compliance and routine audits by outside watchdogs should be instituted. Accountability, safety and security should be paramount.

Citations

Armental, M. (2019, August 5). Marriott Takes $126 Million Charge Related to Data Breach. Retrieved April 23, 2020, from https://www.wsj.com/articles/marriott-take-126-million-charge-related-to-data-breach-11565040121

IBM Corporation, (2016,December). Security Data sheet IBM Security Guardium Data Protection for Databases,.Retrieved April 22,2020 from https://www.ibm.com/downloads/cas/DV7O2GZN

Leonhardt, M. (2020, March 31). The latest Marriott data breach impacts up to 5.2 million people-here's what to do if you were affected. Retrieved April 23, 2020, from https://www.cnbc.com/2020/03/31/what-to-do-if-you-were-affected-by-the-latest-marriott-data-breach.htm

IBM Security Guardium Benefit Estimator. (2018). Retrieved April 23, 2020, from https://tools.totaleconomicimpact.com/go/ibm/Guardium/

McMillan, R. (2018, December 2). Marriott's Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say. Retrieved April 23, 2020, from https://www.wsj.com/articles/marriotts-starwood-missed-chance-to-detect-huge-data-breach-years-earlier-1543788659