International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Compromised Systems, Compromised Data: A Technical Analysis of the Marriott Data Breach

Megha Manglani

University of Illinois at Urbana Champaign, Illinois, USA
Email: *megha20manglani[at]gmail.com*

Abstract: ***Data breaches continue to be a significant threat to corporations and individuals alike. The 2018 Marriott International data breach, compromising the data of over 500 million guests, underscores the severity and persistence of these attacks. This paper provides a technical analysis of the Marriott breach, examining the attack methodology, root causes, and the devastating repercussions for the company and its customers. Central questions of this paper include: How did attackers exploit vulnerabilities in Marriott's systems, particularly within the acquired Starwood network? What were the consequences in terms of financial loss, reputational damage, and regulatory implications? Could the impact have been mitigated through more robust cybersecurity measures? The research draws upon existing literature on data breaches and cybersecurity, analyzing the Marriott incident in light of common attack patterns and industry best practices. Key recommendations focus on the need for: Data Leak Prevention and Detection (DLPD) mechanisms Thorough security audits during mergers and acquisitions Implementation of stricter data protection laws Increased customer awareness of data security This study highlights the critical role of proactive cybersecurity strategies in the hospitality industry and the broader corporate landscape.***

Keywords: data breach, Information security, cybersecurity, Marriott International, data protection, data leak, Starwood database, SQL injection attack, malware, GDPR, Data Leak Prevention, DLP

1. Introduction

Data breaches have become a very common occurrence in this modern era of digitalization. According to TechTarget, a data breach can be defined as “an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. ” The history of data breaches goes way back to even when companies didn’t store data digitally. As a matter of fact, data breaches have been prevalent since the time organizations have been maintaining records and documents of sensitive information. However, the most intense ones started occurring from 2005 and beyond. This is not surprising since the volume of global data generated has been growing thereafter. The wave of these breaches has since then affected organizations’ reputation adversely, one such of these high magnitude data breaches being the 2018 Marriott data breach.

It wasn’t until September 2018 that one of the pioneers in the hotel industry, the Marriott group of hotels was made aware of a trojan malware that had attacked it’s Starwood database. What's more astonishing is that this leak of customer records was going on since 2014, but the brand had no clue about this. It was a concerning issue that needed to be addressed immediately since sensitive information like encrypted passport numbers, credit card numbers, security codes along with names, email ids, genders, telephone numbers of a database of over 383 million customers had been compromised. Marriott reported that anyone who had been a customer until September 2018 was a potential victim of this attack. Consequently, this massive data leak and sheer negligence to maintain secure systems resulted in the hotel brand paying a fine of around $123 million as a penalty.

This incident costed Marriott more than just monetary damage, it was their reputation built over the years which was at stake. In this particular time period, Marriott shares fell by 5.6% and their revenue went down by 1.9%. The repercussions of this data breach were enormous since the hotel group had a very hard time gaining the trust of its customers back. Considering the fact that this particular chain of hotels owns some of the most luxurious hotel brands like Westin, Sheraton, W, St. Regis and Le Méridien, their customer base consists of highly important and influential people, including government employees. These individuals have data that has private information was very sensitive as compared to normal working people. It was speculated that this malware attack was encouraged by a competitor nation’s government in order to access data of the US government employees because Marriott’s largest customer database comprises of US nationals. Even after data breaches occurring at such an alarming rate, companies are yet to identify their ideal response to these privacy invasions and how to responsibly handle the data that is leaked. This shortcoming exists because not many studies have been conducted to evaluate the repercussions of these attacks, how they affect consumer confidence, social trust, and personal safety along with harming the reputation of the organization. According to me, there should be more awareness and knowledge on the aftereffects of data breaches and how difficult it is to recover back from the losses, especially those which aren’t just financial but affect the company’s brand value and dignity the most. All these thoughts and ideas form the basis of my research paper.

2. Literature Review

Privacy attacks and data breaches have been one of the most pressing concerns for almost all organizations over the past few decades. The Breach Level Index highlighted that security incidents are becoming faster and larger in scope, increasing by 87.5% from 2016 to 2017. (Confente, Siciliano, Gaudenzi, & Eickhoff, 2019) A survey conducted by the Identity Theft Resource Centre in 2018 found out that the number of data breaches occurring in the US between Jan 2005 to March 2018 is around 8741 which has led to around

1, 069, 914, 088 records being exposed to hackers. (Liu, Han, Wang, & Zhou, 2018) Around 80 million records were stolen when the second - largest health insurer in the States was attacked in Feb 2015. The situation got worse when the US Office of Personal Management announced that personal information, including the background checks of 21.5 million federal employees, was compromised. One more incident which made it to the headlines was when the Home Depot's corporate network was penetrated and over 56 million credit card numbers were acquired in September 2014. (Edwards, Hofmeyr, & Forrest, 2016) A more recent data breach that happens to be one of the biggest data breaches of all times was when Marriott International reported that over 500 million of its customer records had been compromised due to a Remote Access Trojan that had infected their Starwood Database. A wide number of studies provide evidence that digital data theft is growing tremendously. A study by Redspin shows that the number of breaches in the healthcare industry increased by 29% from 2011 to 2012. However, the total number of records compromised had a drastic upsurge of around 138% in the same time period. (Edwards, Hofmeyr, & Forrest, 2016)

Owing to this, cybersecurity and data protection has become the top priority for a lot of companies since there is not much information and experience available on what the aftermath of these cyberattacks usually is. Whenever a data breach occurs, in - depth analysis of how it occurred, what caused it and what could prevent it is discussed, but little importance is given to the impact and havoc it creates for both the organization and the customers whose data was stolen. Data breaches are unpredictable, often low probable and high impacting, like "black swans" (Gaudenzi & Siciliano, 2017). They can be categorized into three groups: intentional and internal (e. g., malicious employees stealing customers' data), unintentional and internal (e. g., incorrect security settings that expose private information), and external and intentional (e. g., Ransomware infecting companies' software) (Confente, Siciliano, Gaudenzi, & Eickhoff, 2019)

The volume of data has been growing exponentially year after year because of the widespread incorporation of big data by companies, and this has made it easier for hackers to get into an organizations' database since most of the information is stored on the cloud making it more vulnerable and less secure. The 12th annual Cost of Data Breach Study, which was sponsored by IBM in 2017 tells us that the global average cost of a data breach is around $3.62 million. (Liu, Han, Wang, & Zhou, 2018) A number of studies conducted by Gatzlaff and McCullough found that along with exposing the personal information of customers or employees it may also affect the shareholder wealth of the company which will eventually affect the company's revenue. (Liu, Han, Wang, & Zhou, 2018). While analyzing some of the world's largest data breaches, Chiesa & De Luca Saggese realized that all the 'cybersecurity mechanisms' described in these studies lacked the practice of secure coding. "While browsing through the guidelines published by the ASD, we were surprised to learn that no explicit rules or advice have been given regarding secure coding or secure programming. We have found 'User application configuration hardening, ' in order to address intrusions that exploit the prevalence of Java vulnerabilities or involve malicious macro - code in the Microsoft Office files, and Application whitelisting (#1 in the ASD list), but still not a specific item, related, i. e., to S - SLDC (secure software life development cycle), OWASP Top - Ten, or general warnings and best practices on how to program securely. And, as you will read on your own, no mention of data feeds from the cybercrime intelligence Environments". Cyber intelligence and secure coding can prove to be two effective mechanisms to tackle this unpleasant menace of data leaks. They also observed that in spite of spending heavy budgets on IT security, products, software, and top consultants, most victim organizations had no concrete idea about 'who' or 'what' hit them. (Chiesa & De Luca Saggese, 2016)

Moreover, the information stolen can also result in identity theft in many cases, especially when customer databases consisting of sensitive data are compromised. Since there is large scale sharing of this stolen data by sophisticated underground markets, breached personal information is extremely confidential and concentrated which makes it very easy for hackers to steal customers' identity, resulting in subsequent identity theft. (Wheatley, Maillart, & Sornette, 2016). While mining and analyzing stolen hospital data records, Floyd, Grieco & Reid found that the majority of data stolen were social security numbers, patient names, date of births and patient addresses. They further analyzed that all this data is then sold over the Darknet. (Floyd, T., Grieco, M., & Reid, E. F., 2016) However, researchers argue that in order to combat this identity theft, consumers can take certain measures like enabling 2 - factor authentication, monitoring their financial reports and accounts and using strong passwords. But studies have shown that customers themselves do not take adequate measures to protect their data when hit by data breaches. In a 2014 survey it was found out that the chances of a person being a data breach victim increased from 21% to 32%, yet 66% of the participants chose to "do nothing about it", whereas 56% of them continued using the same password on other sites and 41% chose to 'not opt' for 2 factor authentication when offered. (Zou & Schaub, 2019).

In order to analyze the dreadful effects of password reuse behavior, an experiment was conducted by Poornachandran, Nithun, Pal, Ashok & Ajayan where they conducted their investigation on 62, 148 usernames and passwords leaked from Twitter. The results revealed a 33 % password reuse behavior on Facebook, 26 % reuse behavior on Hotmail, 15 % on Gmail and 12 % on Yahoo. This shows that password reuse behavior is extremely common among users which makes them more vulnerable to data hacking regardless of the password being extremely strong. In addition to these, using password recovery tools like hashcat makes it very easy to obtain passwords offline which can cause adverse effects. (Poornachandran, P., Nithun, M., Pal, S., Ashok, A., & Ajayan, A., 2016).

Classifying data breaches and dealing with the root cause is an effective approach to curb privacy invasions. Data leaks based on their causes are either intentional or unintentional leakage of sensitive data whereas breaches based on their sources can be identified as internal or external threats. Intentional leaks occur due to either external parties or malicious insiders. External data breaches are normally caused by hacker break - ins, malware, virus, and social

engineering. Internal data leakage can be caused by either deliberate actions or inadvertently mistakes. The analysis of over 1259 data leakage incidents revealed that over 60% of those breaches were caused by insiders, which makes it important to consider both technical and non - technical aspects while dodging data leaks. However, some of the biggest data hacks including the Yahoo, Target and Marriott data breach have all occurred due to external malware. Unlike internal attacks which are more tedious to detect because they often involve legitimate users with administrative rights, external data breaches can be avoided by incorporating appropriate DLPD mechanisms. (Cheng, Liu, & Yao, 2017).

3. Description and Analysis

The Attack:

In September 2016, Starwood was acquired by Marriott International and the 'Starwood Preferred Guest' (SPG) was merged with Marriott's loyalty program in August 2018. Very soon after this merger, Marriott disclosed that one of its Starwood databases suffered from one of the largest data breaches, following the Yahoo data leak that compromised data of over 3 billion users. The attack on Starwood database was mostly performed on an outdated and vulnerable security and point of sale reservation systems. Marriott reported that an alert from an internal security tool warned them of an attempt by an unauthorized party to gain access to their Starwood database. Experts say that this hack was due to infiltrating systems using a phishing attack. Such methods can allow attackers to download additional secondary exploits from command and control servers, thus infecting the entire system with sophisticated malware and trojans. The hackers accessed customer personal information along with sensitive data like passport numbers and encrypted payment details. Moreover, the stolen data was copied and secured with data encryption which made it very difficult to determine the contents. There is a high probability that attackers choose hotel groups as they are an abode to rich details of credit card data, which are generally accessible from remote computers for maintenance purposes. Also, the hospitality industry has always had a relaxed security mechanism, making it rather easier for hackers to get into the system in sophisticated ways. The root cause of this attack can be traced back to 2011 when Starwood finished a 10 year - long project called Valhalla to upgrade its reservation system. A variety of payment acquisition methods were combined with Starwood's many acquisitions, which made it difficult to ensure a secure coding network for the hotel's database. The payment systems of hotels are the most vulnerable to attack, says Paul West, a risk management hotel industry consultant. The nature of the data leak is astonishingly similar to some of the other high profile breaches like Equifax's and Target's breach, all three of them were through external malware entering the company's POS. After investigation, it was found out that this attack had been lurking in the system for the past 4 years, and the brand was completely unaware of this. A few days after the merger, Starwood came out and said that it suffered from a massive credit card hack in 2014 and an SQL injection in 2015, which was on a much smaller magnitude. While Marriott says that the two incidents are not related, cybersecurity experts claim that a thorough investigation and appropriate security mechanisms would have helped curb this issue in the early stages itself.

The Aftermath:

We've already discussed how common data breaches have become in this digital era. Most companies have accepted the fact that data leaks are not a matter of if, but when. Marriott faced a lot of criticism due to their negligence in detecting security discrepancies at an early stage which led to it being the victim of the world's second - largest data hack. It is almost impossible to believe that a brand like this, having so many resources at its disposal to maintain and increase its data security, failed to even sniff the attack for over 4 years. Even after discovering the breach in September 2018, the hotel group took 2 whole months to announce it and act on it. Such scenarios should be well thought of beforehand and a strategic mitigation plan must be ready for situations revolving around data ethics and privacy, which was clearly missing in this scenario.

The customer records that were stolen are huge in number, nearly around 500 million. This data leak can cause identity thefts of all of those customers in ways where they won't even realize that this is a repercussion of their stay in one of the most luxurious hotels, the Marriott group. Starwood has a previous experience where the data stolen from the SQL injection attack was sold in the Darknet markets. Most customers are prone to password reuse behavior, which makes all their other social media accounts vulnerable too. Marriott advised all their customers to monitor their bank statements continuously, since hackers have also gained information about credit cards, security codes and Starwood Preferred Guest account information which makes it very convenient for them to gain access to customer finances, especially by using Reward points.

From Marriott's point of view, the brand had to go through great losses that heavily affected its revenue and reputation. What happened with Marriott is very similar to the Equifax data breach, and Equifax had suffered terrible reputation damage. Today, the words Equifax and data breaches have become synonymous and are almost used in conjunction, which shows us how dreadful negligent behavior can be for an organization whose security has been recently compromised. Marriott could have been in the same spot, but they chose to act on this and tried a lot of tactics to gain their customers back. They offered one year of free stay to all the victims across the USA, UK, Canada, and Australia. Shortly after the breach, the hotel group administration also sent out emails to potential victims addressing the entire situation. One smart move that they made here was making the email address used for communication publicly available so that another hack using spam emails pretending to be 'Marriott' can be avoided. Customers were also advised to not click on any links or submit any personal information on forms/websites.

Fortunately or unfortunately, the European Union decided to incorporate the General Data Protection Regulation (GDPR) which was put into action from May 2018 and the Marriott security intrusion was a clear violation of the GDPR. According to U. K Information Commissioner Elizabeth Denham, "The GDPR makes it clear that organizations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition, and putting in place proper

accountability measures to assess not only what personal data has been acquired, but also how it is protected. Personal data has real value so organizations have a legal duty to ensure its security, just like they would do with any other asset. If that doesn't happen, we will not hesitate to take strong action when necessary to protect the rights of the public. " Marriott has become the second organization to receive this hefty $123 million penalty from GDPR, the first being British Airways which had to pay a sum of $229 million.

Ways in which the attack could have been mitigated:

1) Deploying Data Leak Prevention and Detection mechanisms:

On observing closely, we can conclude that all the recent high profile data breaches including Marriott, Yahoo, Target, British Airways, etc have had similar patterns in which their data has been stolen, most of them being external attackers who found a vulnerable point in the system to get in and infiltrate it with malware and trojan. Firstly, attackers gain access to the organization's remote machines and then penetrate into their internal networks, searching for vulnerable machines and systems they can easily get into. Once they're inside the system, the hackers compromise the firm's most vulnerable Point of Sale (POS) systems and deploy data - stealing malware which gives them access to read all sensitive information. In some scenarios like Marriott and Target, the attackers encrypted all the stolen data and moved them from POS to internal compromised hosts, making it difficult to determine what the contents of the data actually are. This kind of threat is becoming increasingly common and can be easily mitigated and avoided altogether, by incorporating appropriate Data Leak Prevention and Detection (DLPD) technical and administrative approaches. DLPD approaches are divided as basic and designated DLPDs, the basic ones being firewall, antivirus software, intrusion detection authentication whereas designated DLPDs are specially designed to deal with data leakage threats. DLPDs are primarily used for identifying, monitoring and securing sensitive information from unauthorized access. In an enterprise environment, there exist multiple sensitive points where complementary DLPD techniques can be deployed, and doing this ensures increased safety and data leak prevention in the organization.

2) *Historical background analysis during acquisitions and mergers:*

This is a step that not just Marriott, but all organizations can ensure to take henceforth. In this case, all the malware and trojan were actually present in Starwood's database, which was actually acquired by Marriott in 2016. Even after being aware of some security discrepancies Starwood had faced, Marriott chose to treat the issue very casually, thinking it would be no big deal. If DLPD mechanisms or a thorough security check would have been performed during the initial stages itself, the damage would not be this massive.

3) *Data Protection Laws:*

The implementation of GDPR in the European Union resulted in Marriott and British Airways paying a huge penalty, which is reasonable enough since the private information of so many people is at stake. It is high time that governments all through the globe start treating data as an asset. Implementing strict Data Protection laws like the GDPR will prove to be a great motivation for companies to start adopting stricter and more efficient security mechanisms since no one would want to pay the hefty fine along with getting a scar on their reputation. It's refreshing to see how strict and unbiased the EU is with GDPR being followed in all aspects, and other nations should use this as an example.

4) Creating customer awareness:

Whenever there have been data leaks, customers usually receive notifications on their system regarding unidentified sources trying to access their information. However, 66% of the users do not even read that warning and just allow whatever permissions are asked for. Customers must be encouraged to use advanced data protection mechanisms like 2 - factor authentication, and strong password awareness should be spread about the ill - effects of password reuse behavior. Taking all these measures will make customers less vulnerable in case of any data attack, and the 2 FA would make it difficult for hackers to decrypt the passwords. These techniques should be incorporated by all organizations immediately, since they require the least resources and finance, and are relatively easier to carry out. Customers should also be educated about data breach notifications, and the immediate measures they should take or the most appropriate person they should reach out to in case of security attacks.

4. Discussions and Conclusion

Even after knowing data breaches are a common occurrence, the research and analysis conducted while reviewing the Marriott case made me realize the intensity and frequency with which it's growing exponentially every day. This has changed my perception in a way that now while measuring the intensity of a data leak, I look not at the volume, but rather on the value of data and what hackers can potentially do with it. This study also made me very educated about the General Data Protection Regulation (GDPR) that went into effect in Europe in May 2018. In my opinion, it's high time countries start adopting similar data protection laws in order to make companies accountable for the cost of their own security. The Marriott case is an epitome of how

Hackers are becoming smarter each day in order to intrude into critical systems.

Interestingly enough, while I was researching other data breaches and comparing it to my chosen case, I found out that most of the hacks are conducted with either the same underlying motive or use similar tactics and strategies to get into the organization's network. While analyzing literature that conducted data mining on hospital data breach records, the researchers found trends that showed that most of the information stolen consisted of personal data which is then used for identity theft and sold over the Darknet. This is what happens with most of the high profile data that is stolen, it is sold in the black market because it contains sensitive information of valuable people like government employees, medical practitioners and so on which are not very easy to hack. To describe how these attacks are done, I found a lot of similarities between how Target's and Marriott's database was hijacked where the attackers entered the system through a vulnerable Point of Sale (POS).

One massive takeaway that I have after this research is that it's absolutely critical to value every person's information, especially if it is sensitive to customer information. Owing to the advent of big data, it's necessary for organizations to ensure this data is not misused and that the trust of their customers is not compromised. Even after having dedicated teams for this purpose, firms fail to identify the malicious attacks that prove to cause detrimental damages by affecting their revenue and reputation. Customers are also negligent and it's important they become their own saviors by practicing advanced data protection mechanisms like enabling 2FA and using strong passwords. We also need to stop reusing passwords on various social media since this makes us very vulnerable and prone to data hacking in spite of having a strong password. The recommendations offered for mitigating Marriott's breach can be applied to most data breaches since the underlying principle remains the same in all. One positive take - home message that I would want all defenders to know is that there are numerous mechanisms and opportunities to identify and mitigate these risks. Deploying security defense mechanisms like anomaly - based traffic monitoring, verification of code loading and educating employees about phishing attacks in a strategic and efficient manner can aid in increasing the difficulty level of attacks and thus secure the organization's data.

Future work can comprise conducting an in - depth analysis of how the entire data breach was executed, including the exfiltration of data along with the mechanisms and practices used to manipulate data integrity. By utilizing online spoofing activities along with big data tactics, cyber specialists can track the stolen data records and try finding a pattern if any. They can also gain information about how hackers are customizing this information, and what networks and individuals are involved in this.

References

[1] Confente, I., Siciliano, G. G., Gaudenzi, B., & Eickhoff, M. (2019). Effects of data breaches from user - generated content: A corporate reputation analysis. *European Management Journal*, *37* (4), 492–504. https: //doi. org/10.1016/j. emj.2019.01.007

[2] Liu, L., Han, M., Wang, Y., & Zhou, Y. (2018). Understanding Data Breach: A Visualization Aspect. *Wireless Algorithms, Systems, and Applications*, 883–892. https: //doi. org/10.1007/978 - 3 - 319 - 94268 - 1_81

[3] Edwards, B., Hofmeyr, S., & Forrest, S. (2016). Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity*, *2* (1), 3–14. https: //doi. org/10.1093/cybsec/tyw003

[4] Chiesa, R., & De Luca Saggese, M. (2016). Data Breaches, Data Leaks, Web Defacements: Why Secure Coding Is Important. *Proceedings of 4th International Conference in Software Engineering for Defence Applications*, 261–271. https: //doi. org/10.1007/978 - 3 - 319 - 27896 - 4_22

[5] Wheatley, S., Maillart, T., & Sornette, D. (2016). The extreme risk of personal data breaches and the erosion of privacy. *The European Physical Journal B*, *89* (1). https: //doi. org/10.1140/epjb/e2015 - 60754 - 4

[6] Zou, Y., & Schaub, F. (2019). Beyond Mandatory: Making Data Breach Notifications Useful for Consumers. *IEEE Security & Privacy*, *17* (2), 67–72. https: //doi. org/10.1109/msec.2019.2897834

[7] Floyd, T., Grieco, M., & Reid, E. F. (2016). Mining hospital data breach records: Cyber threats to U. S. hospitals.*2016 IEEE Conference on Intelligence and Security Informatics (ISI)*. https: //doi. org/10.1109/isi.2016.7745441

[8] Poornachandran, P., Nithun, M., Pal, S., Ashok, A., & Ajayan, A. (2016). Password Reuse Behavior: How Massive Online Data Breaches Impacts Personal Data in Web. *Advances in Intelligent Systems and Computing*, 199–210. https: //doi. org/10.1007/978 - 981 - 10 - 0419 - 3_24

[9] Cheng, L., Liu, F., & Yao, D. D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7* (5), e1211. https: //doi. org/10.1002/widm.1211

[10] https: //threatpost. com/2014 - marriott - data - breach - exposed - 500m - guests - impacted/139507/

[11] https: //www.forbes. com/sites/davidvolodzko/2018/12/04/marriott - breach - exposes - far - more - than - just - data/#4df1871a6297

[12] https: //www.synack. com/blog/the - marriott - breach - implications - consequences - accountability

[13] https: //krebsonsecurity. com/2018/11/marriott - data - on - 500 - million - guests - stolen - in - 4 - year - breach/

[14] https: //www.theweek. co. uk/cyber - crime/98262/marriott - starwood - data - breach - what - happened - are - you - affected - claim - compensation - share - price

[15] https: //www.thesslstore. com/blog/autopsying - the - marriott - data - breach - this - is - why - insurance - matters/

[16] https: //www.wsj. com/articles/marriotts - starwood - missed - chance - to - detect - huge - data - breach - years - earlier - 1543788659