LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC4004NI Cyber Security Fundamentals

Assessment Weightage & Type

50% Individual Coursework

Year

AY 2023 - 2024

Student Name: Evani Raut

London Met ID: 23047473

College ID: NP01NT4A230151

Assignment Due Date: 5th MAY 2024, Sunday

Assignment Submission Date: 4th May 2024, Saturday

Word Count: 3292

I confirm that I understand my coursework needs to be submitted online via MySecondTeacher under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Acknowledgment:

I am deeply grateful for the opportunity to explore the captivating subject matter of this coursework. The idea itself has been a source of inspiration and motivation throughout this journey, guiding my research and shaping the direction of my study. I am thankful for the chance to explore into this fascinating topic and gain deeper insights into Marriott International data breach. Additionally, I appreciate the support and encouragement of my mentors and instructors for their valuable assistance with literature review and methodology, whose guidance has significantly influenced the direction of this work. The enthusiasm for this academic exploration has fueled my own passion for learning and discovery.

The insights gained from studying the data breach have not only enhanced my academic journey but have also opened my eyes to the broader challenges and opportunities in the realm of cybersecurity. I am excited to apply the knowledge and experience gained from this coursework to future projects and pursuits in the field. This project has sparked a deep interest in how businesses can proactively protect their systems and customers, and it has given me a profound respect for the importance of safeguarding data. I am excited to apply the knowledge and experience gained from this coursework to future projects and pursuits in the field, continually striving to improve data security and contribute meaningfully to the industry.

Table of contents:

Contents

Table of figure:

Abstract:

The Marriott International data breach, discovered in late 2018, it stands as one of the most consequential cybersecurity incidents in the hospitality sector. This study investigates the breach's timeline, revealing unauthorized access to Marriott's Starwood guest reservation database between 2014 and 2018, ultimately compromising the personal data of approximately 383 million guests worldwide. Drawing upon extensive research, including forensic investigations and regulatory disclosures, this analysis uncovers the multifaceted impact of the breach on Marriott International, its guests, and stakeholders. Financial damage, legal repercussions, and reputational damage are examined, emphasizing the breach's profound implications for data privacy and security in the digital age. Root causes and vulnerabilities contributing to the breach are studied, clarifying on systemic deficiencies in cybersecurity governance, legacy IT infrastructure, and threat detection mechanisms within the hospitality giant's operations. Furthermore, this study evaluates Marriott's response and remediation efforts, including communication strategies, regulatory compliance initiatives, and cybersecurity enhancement measures aimed at strengthening defenses and restoring trust in the aftermath of the breach. Conclusions drawn from this examination guide practical suggestions for companies aiming to strengthen their ability to bounce back from cyber threats. This highlights proactive risk management, investing in cutting-edge security tools, and nurturing a solid cybersecurity mindset within the organization. After a careful review of the Marriott International data breach, this study highlights the need for stronger attention to data security and smart planning to protect sensitive information. It emphasizes the importance of maintaining trust in a digital world that is becoming more connected.

Introduction:

About APT attack:

Advanced Persistent Threat (APT) attacks are a complex and ongoing cyber threat executed by highly skilled and well-funded adversaries. Unlike traditional cyberattacks, which may be opportunistic, APT attacks are carefully **planned and target specific organizations or individuals** over a long period. The goal is to infiltrate networks, steal sensitive data, and **maintain unauthorized access while evading detection.**

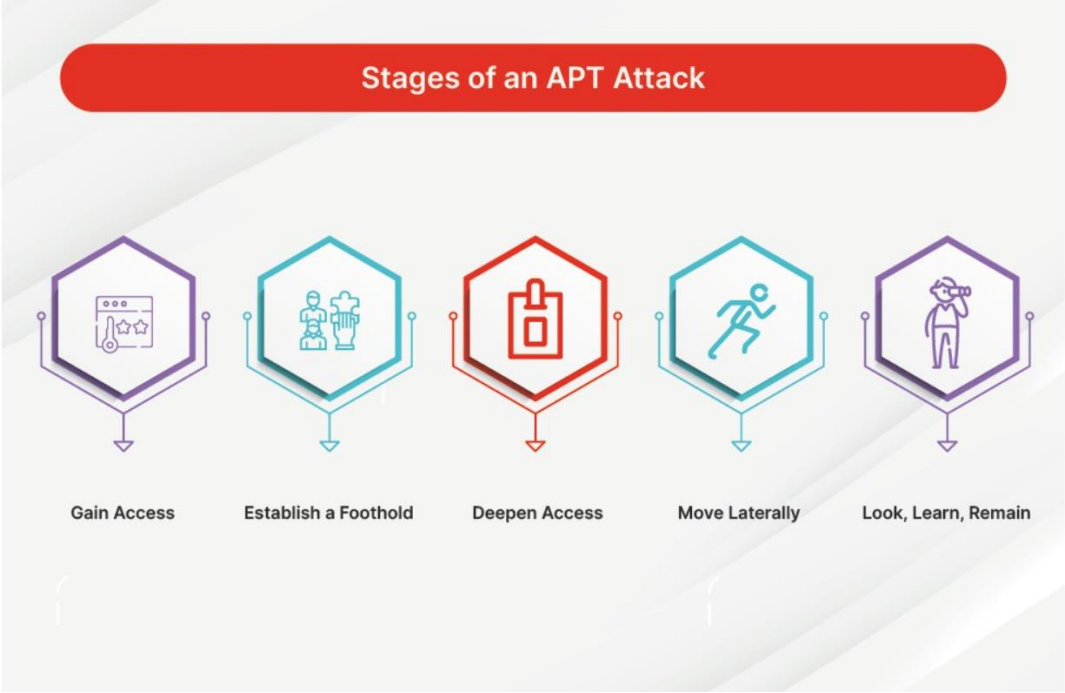

Figure 1: Stages of APT attack

To **Gain Access**, cyber criminals often use infected files, junk email, a vulnerable app, or a weak spot on the network. Attackers **Establish a Foothold** by planting malware that enables them to set up a network of tunnels and backdoors that allow them to navigate within the system without being detected. The malware can also help them cover their tracks by rewriting code. After attackers get inside, they **Deepen Access** by

compromising passwords to access administrator rights. They then use these to manipulate more aspects of the system and obtain greater access. Once they are fully inside, attackers may **Move Laterally** to other areas of the network, such as servers and other devices. They may also expand the attack, gaining and then deepening access in connected areas. **Look, Learn, Remain** while inside the system, attackers can closely examine how it works as well as where it is vulnerable. Once they have done this, it is easy to grab the information they need. They can then remain in the system until they achieve their goal or stay inside without any plans of ever exiting (fortinet, 2024).

What and when it happened:

Figure 2: Marriot International

In today's era of rapid digitalization, the hospitality industry has become a prime target for cyber threats, given its reliance on vast amounts of sensitive guest data. Among the notable instances of such attacks is the Marriott International data breach, which shook the hospitality industry and raised concerns about the security of customer data.

In November 30, 2018, Marriott International announced that it had discovered a massive data breach affecting its Starwood hotel brand reservation system. The breach exposed the personal information of up to 500 million guests who had made reservations at Starwood properties. This included names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, date of birth, gender, arrival and departure information, reservation dates, and communication preferences. For about 327 million of these guests, the exposed information also included payment card numbers and expiration dates. However, Marriott said the payment card numbers were encrypted and it was unknown if the cyber thieves were able to decrypt the information. Marriott said it had reported the incident to law enforcement and was supporting the investigation. The company also offered affected guests free WebWatcher identity theft monitoring for one year. This breach, which was ultimately caused by existing security vulnerabilities that remained after Marriott's 2016 acquisition of Starwood, has since become known as one of the world's largest cyber incidents, highlighting the importance of prioritizing cybersecurity during merger and acquisition (M&A) events. Businesses can learn a variety of cybersecurity lessons by studying the circumstances of this incident, its consequences, and the mistakes Marriott made along the way (Josh Fruhlinger, 2020).

Inside this report:

In this report, we undertake a comprehensive examination of the Advanced Persistent Threat (APT) attack directed at Marriott International. Our analysis unfolds across three distinct sections. Firstly, we dig into the specifics of the APT attack on Marriott,

explaining its timeline, motives, and repercussions on customers. Through precise research, we uncover the attack vectors and vulnerabilities exploited, shedding light on the company's proneness to cyber violations. Moving forward, we navigate the regulatory landscape governing cyber-attacks, exploring the obligations of companies and the potential fines imposed by national and international governing bodies. This investigation extends to post-breach obligations and liabilities, underscoring the imperative for robust regulatory compliance frameworks. Finally, assuming the role of Chief Information Security Officer for Marriott International, we suggest strategic insights into preventative measures and post-breach remediation strategies. From securing cybersecurity protocols to encouraging a mindset of alertness, we outline a roadmap towards enhancing Marriott's defenses and mitigating future vulnerabilities. Through this diverse analysis, we aim to explain the complexities of the Marriott International APT attack, offering strategic recommendations to strengthen cybersecurity durability and mitigate digital risks.

Section 1:

Facts of the APT attack:

Discovery: Marriott first discovered the data breach in September 2018, but the initial unauthorized access to the Starwood network had occurred as early as 2014.

Impact: The breach exposed the personal data of up to 500 million guests from Starwood properties, including names, addresses, phone numbers, emails, passport numbers, birth dates, and some encrypted payment card details.

Duration: The hackers had continuous access to the Starwood network for about four years, from 2014 to 2018, before the breach was detected and contained.

Investigation: Investigations suggest the attack may have been carried out by hackers affiliated with Chinese intelligence services, rather than traditional cybercriminals. The use of cloud-hosting services and code patterns common to Chinese hackers supported this theory.

Motives: The attackers goals appeared to extend beyond financial gain, potentially aiming to collect data on American government employees and intelligence officers for state intelligence purposes. The stolen data was not sold on the dark web, suggesting a strategic motive rather than immediate financial profit.

Broader Campaign: The Marriott breach was linked to other significant cyber incidents, such as the Equifax breach in 2017, indicating a broader campaign to collect large amounts of data for analysis.

Consequences: As a result of the breach, Marriott faced approximately $30 million in total recovery costs and suffered reputational damages due to widespread criticism for its cybersecurity shortcomings. This led to a nearly immediate 5% drop in Marriott's stock and projected losses of over $1 billion in revenue due to declining customer loyalty. Marriott also faced a fine of over $120 million from the UK's Information Commissioner's Office for violating British consumers' privacy rights under GDPR.

Notification: Marriott notified affected guests and relevant authorities, including the FBI and regulatory bodies, about the data breach in late November 2018.

Remediation: Marriott implemented enhanced security measures, such as data encryption, multifactor authentication, and improved monitoring systems, to prevent similar incidents in the future (Nicole Perlroth, Amie Tsang , Adam Satariano, 2018) (Kate O'Flaherty, 2018) (Allen St. John, 2018).

Timeline of APT attack:

Figure 3: Timeline

- **July 29, 2014**: An attacker gained physical access to a machine on the Starwood network, which was connected to the internet and had administrative privileges.
- **2014-2018**: The attacker established a foothold in the Starwood network, deploying malware and maintaining a long-term, undetected presence.
- **2015**: A separate incident occurred where Starwood's workplace devices were infected with malware by other attackers.
- **2016**: Marriott acquired Starwood but failed to properly audit Starwood's compromised networks during the acquisition process.
- **2016-2018**: Marriott continued using the compromised guest reservation system and malware-infected devices. Marriott also began migrating Starwood's customer databases into its own systems.
- **September 8, 2018**: Marriott's internal security tool raised an alert regarding an unauthorized attempt to access the Starwood guest reservation database.
- **September 2018**: An internal investigation and forensic analysis revealed potential irregularities in Starwood's systems.

- **November 2018**: Marriott publicly disclosed that up to 500 million customers globally had data exposed in the breach (costar, 2020).

Motive behind targeting Marriott International:

Valuable Data Target: Cybercriminals targeted Starwood and Marriott for their guest reservation data, including personal and financial details of millions of travelers, which is valuable on the black market as Hospitality is the third-most targeted industry after retail and finance this made Starwood's systems an appealing target (Patrick Clark, 2018).

Hotel Convenience for APT Hackers: Large hotel chains like Marriott attract APT hackers due to business travelers connecting corporate devices to hotel networks globally, providing cybercriminals with opportunities to access corporate systems (STEPHEN COOPER, 2023).

Global Presence and High Traffic Volume: Marriott's global presence and heavy guest traffic provide numerous access points into corporate networks. Business travelers create a constant flow of potential entry points for APT groups.

Scalability of a Large Hotel Chain: Marriott's vast network of 7,000+ properties in 131 countries makes it a prime target. Frequent new device connections to Marriott's networks provide attackers with ample opportunities to access corporate systems.

Starwood's Security Vulnerabilities: The report reveals Starwood's major security flaws like outdated software and open RDP ports, making it an easier target. The missed 2014 breach indicates poor security monitoring and response.

Undetected Cybercriminal Activity: Starwood's data richness, security gaps, and large scale made it an appealing, vulnerable target for cybercriminals, who remained undetected for years due to weak detection and incident response.

Affects on customers:

The Marriott/Starwood data breach significantly impacted nearly **500 million guests** by compromising their personal records. Sensitive information stolen included names, addresses, phone numbers, email addresses, dates of birth, **9.1 million unique credit card details**, **23.75 million unique passport numbers**, SPG account information, gender, arrival and departure information, reservation dates, and communication preferences. For around **327 million guests**, the breach also exposed payment card numbers and expiration dates, putting them at risk of credit card fraud and abuse (Jordan Hollander, 2023).

Deployment of the APT on the system:

The APT was deployed on the system following the stages of APT attack:

1. **Gain Access**:
    - On July 29, 2014, an attacker gained physical access to a machine on the Starwood network that was connected to the internet and had administrative privileges. This machine was running a service that allowed employees to make changes to the Starwood website.
    - The attacker exploited this access by deploying a web shell on the machine, enabling further infiltration.
2. **Establish a Foothold**:
    - The attacker installed a Remote Access Trojan (RAT) and the post-exploitation tool MimiKatz using the web shell.
    - These tools allowed the attacker to extract passwords, PINs and other credentials from system memory, giving them elevated privileges on the compromised machine.

3. **Deepen Access**:
    - The attacker gained access to administrative rights by compromising passwords.
    - They used these elevated privileges to manipulate more aspects of the system and obtain greater access, potentially reaching sensitive data.
4. **Move Laterally**:
    - Once inside, the attacker laterally moved to other systems on the Starwood network, such as other machines, servers, and databases containing customer data.
    - They exploited vulnerabilities such as outdated Windows servers and open remote access services.
5. **Look, Learn, Remain**:
    - The attackers closely examined the network and its vulnerabilities, allowing them to access and exfiltrate sensitive personal information like names, contact details, passport numbers, and payment data.
    - They remained undetected for a long period, re-encrypting data to avoid detection (fortinet, 2024) (Kelli Young, 2021).

Section 2:

Compliance with National and International Regulations:

When a company learns it has been the victim of a cyber-attack, these governing bodies require certain actions:

Immediate Response: The company should assess the scope and nature of the attack, then contain and eradicate the threat to prevent further damage.

Investigation and Forensics: The company should investigate the attack's source, methods, and impact, preserving evidence and documenting findings for legal and regulatory use.

Data Breach Notification: The company must inform affected customers and regulatory bodies per applicable laws, offering clear details about the breach and its potential impact.

Offer Support to Affected Individuals: The company should offer resources like credit monitoring and set up a dedicated helpline for affected customers.

Compliance with Legal and Regulatory Requirements: The company must cooperate with data protection laws like GDPR in the EU and work with regulatory authorities and law enforcement.

Remediation and Security Enhancements: The company should fix vulnerabilities and prevent future attacks by patching software, updating security protocols, and training employees.

Communication and Transparency: The company should keep stakeholders informed of the situation and the actions being taken to address it, providing regular updates as more information becomes available (wickr, 2021).

Potential Fines from Governing Bodies for Data Breach:

1.European Union's General Data Protection Regulation (GDPR):

- Marriott could face fines of up to €20 million or 4% of its global annual revenue, whichever is higher.
- Given Marriott's global scale, the GDPR fine could potentially reach hundreds of millions of euros (Paul Biberstein, Sreshtaa Rajesh, 2023).

2.UK's Information Commissioner's Office (ICO):

- The ICO announced its intention to fine Marriott £99.2 million (approximately $123 million) for the breach.
- This is one of the largest GDPR penalties issued to date and highlights the severity of large-scale data protection failures (Joe Tidy, 2020) (reuters, 2020).

3.United States Federal Trade Commission (FTC):

- The FTC is likely to lead the investigation in the US and has the authority to impose civil penalties of up to $43,280 per violation of consumer protection laws.
- Given the breach impacted hundreds of millions of customers, cumulative FTC fines could reach hundreds of millions of dollars (Philippa Donn, 2020).

Section 3:

Prevention:

As the Chief Information Security Officer for Marriott International, I would have taken a multi-pronged approach to prevent the devastating cyber-attack that ultimately exposed the personal and financial data of up to 500 million guests.

1. First and foremost, I would have ensured that all of our servers, operating systems, and other critical software were kept up-to-date with the latest security patches and updates. Maintaining a **robust patch management program** and avoiding the use of vulnerable, outdated technologies would have been a top priority.

2. Secondly, I would have implemented tough **access controls and monitoring around remote desktop protocol (RDP)** connections. The report indicates that Starwood had left its RDP ports openly exposed to the internet. I would have restricted and closely monitored all remote access, while ensuring our firewalls and other security tools were effectively limiting unauthorized connections.

3. Additionally, I would have placed a strong emphasis on **network segmentation** across Marriott's global infrastructure. By dividing the network into smaller, isolated segments and restricting access between them, I could have dramatically limited the ability of an attacker to move laterally and spread the infection.

4. **Enhancing our security monitoring and incident response** capabilities would have also been crucial. Deploying advanced security tools to quickly detect anomalous activity, coupled with a well-defined incident response plan, would have given us a better chance of identifying and containing the breach.

5**. Robust access controls**, including the enforcement of **multi-factor authentication**, would have been another key defense. Closely managing and auditing privileged accounts would have made it exponentially harder for the attackers to gain and maintain the level of system access they ultimately achieved.

6.Lastly,I would prioritize **security awareness training** for all Marriott employees. Combining layered security measures like updated software, strict access controls, segmented networks, and enhanced monitoring with security-savvy employees could have prevented the APT attack (solarwindssoftware, 2019) (axaxl, 2020).

Preventative measures:

As the Chief Information Security Officer for Marriott International, I would have implemented a comprehensive set of preventative measures to protect the company against the type of advanced persistent threat (APT) attack that ultimately led to the massive data breach.

1.One critical measure would have been the enforcement of a **robust password policy across the organization**. This would have included requirements for strong, complex passwords that are changed regularly, as well as the implementation of multi-factor authentication for all critical systems and accounts. By making it exponentially harder for attackers to gain unauthorized access, a **stringent password policy** would have been a key line of defense.

2.In addition to strong access controls, I would have placed a heavy emphasis on **keeping all software and systems up-to-date with the latest security patches and updates**. Maintaining a robust patch management program and avoiding the use of vulnerable, outdated technologies would have been a top priority.

3.Closely monitoring and restricting remote access would have also been a critical preventative measure. I would have implemented strict access controls, logging, and monitoring around all remote connections to quickly identify and shut down any suspicious activity.

4. Network segmentation could have limited an attacker's lateral movement by dividing Marriott's infrastructure into smaller, isolated segments and carefully controlling access between them.

5**.Security awareness training** for all employees would have improved their ability to spot and report suspicious activity, like phishing and social engineering, before it could compromise systems.

6. Investing in advanced **security monitoring and incident response** could have helped rapidly detect and address breaches, enabling the team to stop APT attacks before they escalated (Dan Daniels, 2019).

Response:

Now that the cyber-attack has happened these are the following measures that should be taken for it not to happen again:

1.Activate the **incident response plan** immediately to contain the breach and minimize further damage. Engage leading cybersecurity firms to conduct a comprehensive **forensic investigation** to understand the full scope, tactics, and entry points utilized by the attackers. Collaborate closely with law enforcement agencies to aid in their criminal investigation and potentially identify the threat actors.

2. Conduct comprehensive **vulnerability assessments and penetration testing.** Implement a strong patch management program and decommission outdated systems that cannot be secured (searchinform, 2019).

3.Enforce **strict access controls**, including the mandatory use of **multi-factor authentatio**n for all privileged and administrative accounts. Implement privileged

access management solutions to tightly control and monitor the use of elevated privileges within the environment. Conduct a comprehensive review of all user accounts and permissions, revoking or adjusting excessive privileges as needed (solarwindssoftware, 2019).

4. Enhance **network segmentation** into smaller, isolated zones with strict communication controls. Use advanced SIEM tools for real-time threat detection and comprehensive logging for effective incident investigation and forensics.

5. Conduct mandatory **security awareness training** on recognizing and reporting threats. Use regular phishing simulations to assess and improve employees' ability to identify and respond to attacks.

6.Update the **incident response plan** using lessons from the breach. Regularly test and exercise the plan, including tabletop simulations and real-world scenarios. Strengthen business continuity and recovery plans to enhance resilience and minimize disruptions during cyber-attacks.

7.**Implement a robust third-party risk management program** to assess and monitor vendors with access to systems or data. Set strict security standards and contractual obligations for third parties (axaxl, 2020).

8.Ensure full compliance with all relevant data protection regulations, such as GDPR and state-specific breach notification laws. **Communicate transparently with customers**, keeping them informed about the breach, the steps being taken to address it, and the measures being implemented to safeguard their data moving forward.

Conclusion:

Main findings:

1.Scope and Impact: The Marriott International data breach affected nearly 500 million guests who had made reservations at Starwood properties. Compromised data included sensitive personal information. Additionally, around 327 million guests had their payment card numbers and expiration dates exposed.

2.Root Causes: The Marriott data breach originated from a mix of security issues such as outdated software, open RDP ports, and poor data encryption, which gave attackers multiple entry points. Inadequate security monitoring allowed cybercriminals to remain undetected for around four years, while lack of due diligence during Starwood's acquisition left compromised networks unaddressed. Weak access controls and inconsistent security practices across properties also heightened vulnerability.

3.Governing Bodies' Response: Governing bodies such as the General Data Protection Regulation (GDPR), the UK's Information Commissioner's Office (ICO), and the United States Federal Trade Commission (FTC) imposed substantial penalties on Marriott for failing to adequately protect customer data.

4.Proactive Cybersecurity Measures: The breach underscored the necessity for companies to strengthen cybersecurity defenses by implementing advanced security tools, conducting regular assessments, promoting employee training, and enforcing strict access controls.

5.Lessons Learned and Future Preparedness: Organizations must prioritize data security and compliance to protect information and maintain customer trust. Learning from the Marriott breach can guide businesses in preparing for future cyber threats.

About the governing bodies:

- The Marriott data breach highlighted the need for stronger regulatory oversight and cybersecurity standards.
- It led to calls for increased scrutiny and enforcement by bodies like the Federal Trade Commission for data protection.
- The breach prompted discussions about national data privacy legislation to establish clearer rules for securing customer information.
- Authorities such as the EU's GDPR, the UK's ICO, and the U.S. FTC impose strict regulations and fines on companies experiencing data breaches.

References:

Patrick Clark. (2018, December 14). Retrieved from bloomberg: https://www.bloomberg.com/news/articles/2018-12-14/marriott-cyber-breach-shows-industry-s-hospitality-to-hackers

Allen St. John. (2018, November 30). Retrieved from consumerreports: https://www.consumerreports.org/electronics/data-theft/marriott-data-breach-a8216923749/

axaxl. (2020, June 22). Retrieved from axaxl: https://axaxl.com/fast-fast-forward/articles/the-cyber-incident-response-lifecycle

axaxl. (2020, June 22). Retrieved from axaxl: https://axaxl.com/fast-fast-forward/articles/the-cyber-incident-response-lifecycle

costar. (2020, April 7). Retrieved from costar: https://www.costar.com/article/139958097/timeline-the-growing-number-of-hotel-data-breaches

Dan Daniels. (2019, JUNE 13). Retrieved from gigamon: https://blog.gigamon.com/2019/06/13/what-is-network-security-14-tools-and-techniques-to-know/

fortinet. (2024). Retrieved from fortinet: https://www.fortinet.com/resources/cyberglossary/advanced-persistent-threat

fortinet. (2024). Retrieved from fortinet: https://www.fortinet.com/resources/cyberglossary/advanced-persistent-threat

Joe Tidy. (2020, October 30). Retrieved from BBC: https://www.bbc.com/news/technology-54748843

Jordan Hollander. (2023, February 16). Retrieved from hoteltechreport: https://hoteltechreport.com/news/marriott-data-breach

Josh Fruhlinger. (2020, Feb 12,). Retrieved from CSO: https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html

Kate O'Flaherty. (2018, Nov 30). Retrieved from forbes: https://www.forbes.com/sites/kateoflahertyuk/2018/11/30/marriott-breach-what-happened-how-serious-is-it-and-who-is-impacted/?sh=461487ca7d25

Kelli Young. (2021, Oct 11). Retrieved from coverlink: https://coverlink.com/case-study/marriott-data-breach/

Nicole Perlroth, Amie Tsang , Adam Satariano. (2018, Nov 30). Retrieved from nytimes: https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html

Paul Biberstein, Sreshtaa Rajesh. (2023, July 20). Retrieved from cs.brown: https://cs.brown.edu/courses/csci2390/2021/assign/gdpr/pbiberst-srajesh1-mariott.pdf

Philippa Donn. (2020, November). Retrieved from DPN: https://dpnetwork.org.uk/data-breach-costs-marriott-18-million/

reuters. (2020, October 30). Retrieved from reuters: https://www.reuters.com/article/idUSKBN27F1LG/

searchinform. (2019, 09 20). Retrieved from searchinform: https://searchinform.com/infosec-blog/2019/09/20/security-risk-management-assessments/

solarwindssoftware. (2019, October 31). Retrieved from dnsstuff: https://www.dnsstuff.com/rbac-vs-abac-access-control

solarwindssoftware. (2019, October 31). Retrieved from dnsstuff: https://www.dnsstuff.com/rbac-vs-abac-access-control

STEPHEN COOPER. (2023, December 28). Retrieved from comparitech: https://www.comparitech.com/blog/vpn-privacy/hotel-hackers/#:~:text=Hotels%20are%20very%20convenient%20nests%20for%20APT%20hackers,with%20the%20office%20while%20they%20are%20on%20leave.

wickr. (2021, January 28). Retrieved from wickr: https://wickr.com/7-steps-to-take-during-a-cyber-attack/#:~:text=7%20Essential%20Steps%20to%20Manage%20a%20Cyber%20Attack,...%207%207.%20Learn%20from%20the%20Experience%20

Appendix:

- Marriott's initial response to the data breach was criticized for being slow and inadequate. The breach was discovered in September 2018, but it was not until November of that year that Marriott publicly disclosed the incident. Additionally, the company's response to customer inquiries and concerns was considered poor, as it took several weeks for Marriott to set up a call center to handle customer inquiries

- The breach underscored the importance of proactive measures such as immediate incident response, thorough investigation and forensics, and timely data breach notification. Companies must comply with legal and regulatory requirements, including offering support to affected individuals, communicating transparently with stakeholders, and implementing security enhancements to prevent future breaches. The governing bodies' actions in response to the Marriott breach illustrate the necessity for organizations to prioritize cybersecurity and data protection to mitigate risks and avoid severe regulatory penalties

- In the aftermath of the breach, Marriott has taken several steps to improve its cybersecurity measures and restore customer confidence. This includes offering affected customers free identity theft protection, implementing additional security measures, and conducting a comprehensive review of its systems and processes. The Marriott data breach highlights the importance of robust cybersecurity measures and prompt communication with customers in the event of a breach. It also emphasizes the need for organizations to prioritize the protection of customer data and take all necessary steps to prevent future breaches from occurring. As data breaches continue to be a significant threat to businesses and individuals, it is essential for all organizations to remain vigilant and invest in cybersecurity measures to protect against such incidents.