Marriott
HOTELS · RESORTS · SUITES

Marriott INTERNATIONAL

Data Security Breach (2018)

DETAILS OF THE ORGANISATION

The Marriott International Data Security Breach of 2018 stands as a significant incident in the realm of cybersecurity, impacting a global hospitality giant with an extensive presence. The breach, initially identified in September 2018, unfolded during the integration of Starwood Hotels, revealing unauthorised access that had persisted since 2014. Marriott promptly notified affected individuals, underscoring the critical importance of transparency in such events.

DETAILS OF THE BREACH

The breach's scope was extensive, compromising personal data of approximately 500 million guests. The exposed information encompassed a range of sensitive details, including names, contact information, passport numbers, and, in some cases, encrypted credit card data. This breach not only posed a substantial risk to individual privacy but also triggered legal ramifications and financial consequences for Marriott International.

LAWS THAT WERE BREACHED

General Data Protection Regulation (GDPR)	Given the global nature of the breach, GDPR was implicated due to the exposure of personal data of European Union citizens.
Various State Data Breach Notification Laws	As the breach affected residents of multiple U.S. states, various state-level data breach notification laws were triggered

DATA INVOLVED

PERSONAL INFORMATION

Names
Addresses
Phone numbers
Email addresses

PAYMENT CARD DATA

Some payment card numbers
Expiration dates though encrypted, were compromised

PASSPORT INFORMATION

Approximately 327 million guests had their passport details exposed

COST OF THE INCIDENT

FINANCIAL IMPACT

Estimated to be over $3 billion, including the cost of investigating and remediation, legal settlements, and a decline in customer trust

REPUTATION DAMAGE

Significant damage to Marriott's brand reputation, resulting in a decline in customer loyalty and trust

ADVICE TO AVOID A REPEAT INCIDENT IN THE FUTURE

1. **Implement Robust Security Measures:**
   - Regularly update and patch systems to address vulnerabilities.
   - Utilise advanced threat detection and prevention tools to identify and respond to potential breaches.

2. **Enhance Access Controls:**
   - Implement the principle of least privilege to restrict access to sensitive data.
   - Conduct regular audits of user access rights to ensure they align with job roles.

3. **Encrypt Sensitive Data:**
   - Employ strong encryption mechanisms, especially for payment card information and passport details.
   - Regularly assess and update encryption protocols to align with industry standards.

4. **Improve Incident Response Planning:**
   - Establish a comprehensive incident response plan to ensure a swift and effective response to security incidents.
   - Conduct regular drills and simulations to test the efficacy of the incident response plan.

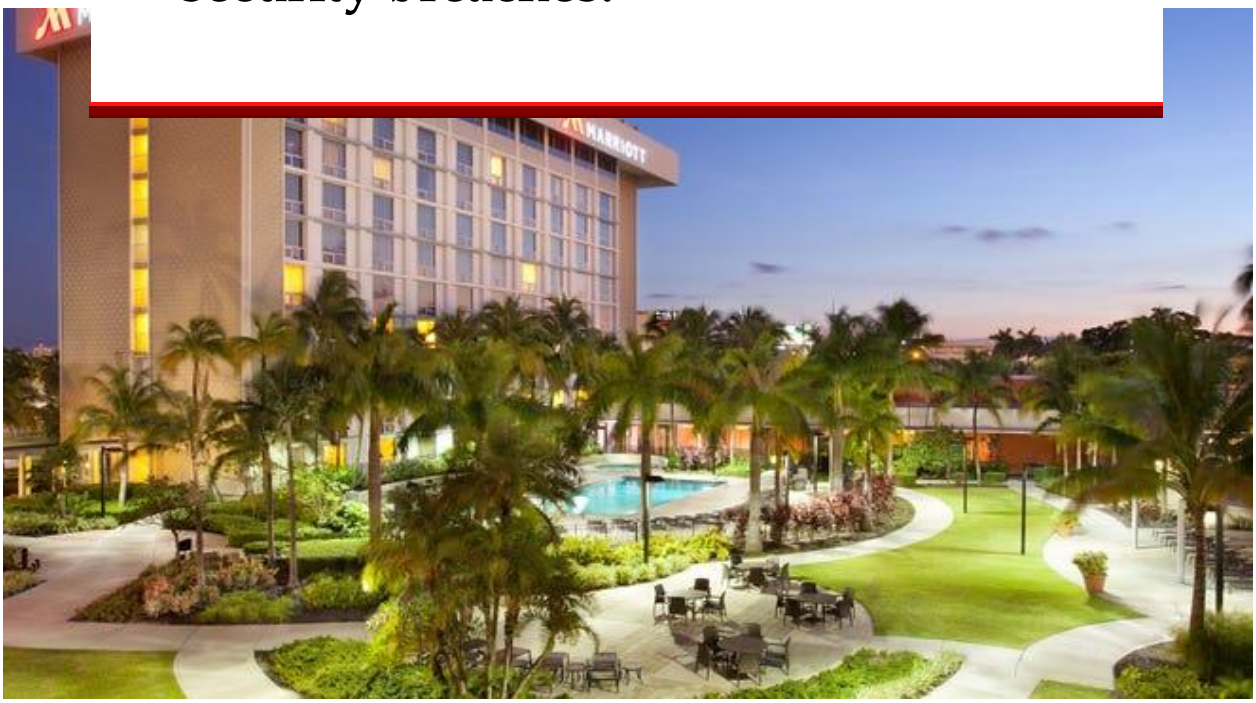
5. **Conduct Regular Security Audits:**
   - Perform regular security audits and assessments to identify and address potential vulnerabilities.
   - Engage third-party security experts to conduct independent assessments.

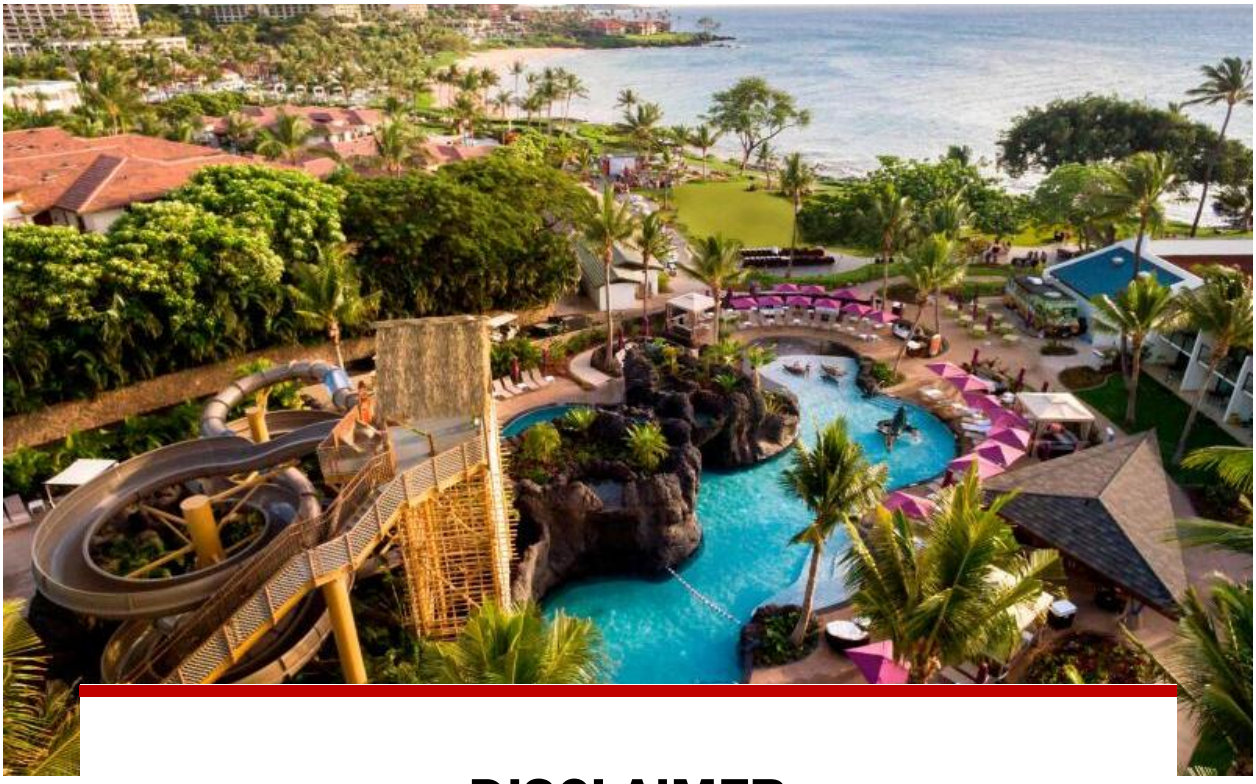
6. **Enhance Employee Training:**
   - Provide ongoing training and awareness programs for employees regarding data security best practices.
   - Emphasise the importance of identifying and reporting suspicious activities.

7. **Strengthen Third-Party Security:**
   - Assess and monitor the security practices of third-party vendors.
   - Include stringent security requirements in contracts with suppliers and partners.

SUMMARY

The Marriott International data breach of 2018 serves as a stark reminder of the critical importance of proactive and robust cybersecurity measures. Organisations must continuously evolve their security practices, conduct thorough risk assessments, and stay vigilant against emerging threats to prevent and mitigate the impact of data security breaches.





DISCLAIMER

This report has been created for educational purposes only. All information presented is based on publicly available sources, and any images used in this report were gathered from the Marriott News Center website. The purpose of this report is to analyse and discuss the high-profile data security breach that occurred at Marriott International in 2018. The content is not intended to harm the reputation of Marriott International or any related entities.

The use of images from the Marriott News Center website is solely for illustrative and educational purposes, and any trademarks, logos, or copyrighted material belonging to Marriott International are acknowledged and respected. This report does not claim to represent the official views or statements of Marriott International, and it is not endorsed by the company.