The Case of Marriott International Data Breach

Case Overview

The Case of Marriott International Data Breach

a. **Description:**
   - Marriott International revealed a massive data breach that exposed the personal details of over 500 million guests. The breach involved the Starwood guest reservation database and went undetected for four years, affecting guests between 2014 and 2018.

b. Location and Date:
   - Location of the offence and legal procedures: United States, United Kingdom
   - Date when the breach was discovered: November 2018
   - Date when the breach began: approximately around 2014
   - Date when investigations commenced: 2018

Reflection questions

- Are the employees of your company educated enough about cybersecurity measures they need to take in their everyday work?
- How quickly would you react and respond to a data breach or security incident?
- What methods would you take to make sure that customer trust in your data security practices is maintained and communicated effectively?
- If you encounter an email with an unverified link, what would be the next step you would take?
- How would you handle a situation where you were asked to bend the rules to meet a client's request? (e.g., a client asks you to backdate a document to help them meet a deadline).
- What steps would you take if you made an error that could potentially harm a project, but no one else is aware of it?
- What would you do if you overheard confidential information being discussed openly by a colleague in a public space?
- What would you do if you noticed that a colleague is using weak passwords or reusing the same password across multiple systems?

Impact

1. **Outcome:** The UK Information Commissioner's Office (ICO) fined Marriott £18.4 million for failing to secure guest data under the GDPR regulations. The hotel chain faced lawsuits and class-action claims in the UK and the U.S. The company implemented enhanced cybersecurity measures following the breach.
2. **Judgements/Penalties:** £18.4 Million with additional penalties, as well as civil lawsuits.

Integrity Issue

Specific concern:

- The breach exposed sensitive personal information of 500 million customers, including passport numbers and credit card data.
- The breach eroded trust in Marriott's ability to safeguard personal data, a key aspect of corporate accountability in today's digital world.
- The breach went undetected for four years (from 2014-2018), suggesting a significant failure in monitoring systems.
- Marriott did not adequately secure customer data, which violated the GDPR.
- Marriott faced hefty fines for failing to comply with GDPR standards, showing the importance of adhering to legal requirements regarding data privacy and breach notification timelines.
- The acquisition of Starwood Hotels (where the breach originated) did not include proper due diligence regarding the security infrastructure.

Related SDGs:

- SDG 8: Decent Work and Economic Growth
  The breach negatively impacted consumer trust and resulted in significant financial losses for Marriott, which in turn could affect job security and growth opportunities.

- SDG 12: Responsible Consumption and Production
  By failing to protect personal data, Marriott demonstrated irresponsible data management. SDG 12 emphasizes responsible business practices, including managing digital data responsibly and safeguarding consumer privacy.

- SDG 9: Industry, Innovation and Infrastructure
  The breach exposed weaknesses in Marriott's digital infrastructure, showing a lack of adequate cybersecurity measures to protect customer data, which is a critical component of a sustainable digital economy.

Public Response

The breach caused widespread concern about privacy and corporate responsibility, leading to significant reputational damage for Marriott. The scale and duration of the breach were especially troubling for the public and data privacy advocates. Marriott's stock temporarily dipped after the news broke.

Learnings:

Key takeaways:

- Companies that store sensitive customer information must have reliable cybersecurity protocols.
- Any delay in identifying breaches can significantly exacerbate the damage and increase regulatory penalties.

- Companies need to conduct cybersecurity audits during acquisitions to ensure that they are not inheriting vulnerabilities.
- Non-compliance with data protection regulations like GDPR can lead to hefty fines and reputational damage.

Impact on sustainability:

- Trust and transparency are key to a company's sustainability image. A data breach can damage customer loyalty and public trust, which can, in turn, affect the credibility of Marriott's sustainability initiatives.
- Stakeholders who felt that Marriott mishandled their data may have questioned its commitment to other aspects of corporate responsibility, including sustainability.
- Marriott's Environmental, Social, and Governance (ESG) ratings were impacted by the breach, as data privacy is a significant factor in these assessments. Lower ESG scores reduced the company's appeal to sustainability-focused investors, potentially impacting funding for environmentally conscious projects.

Applying Learnings in Your Organization

- Ensure the use of firewalls, encryption, and multi-factor authentication.
- Use security monitoring tools like Intrusion Detection Systems and real-time security information and event management system which flags suspicious activity.
- Encrypt sensitive customer data at rest and in transit. Implement strict access controls to limit who can access sensitive data, both internally and externally.
- During acquisitions or partnerships, ensure that cybersecurity due diligence is part of the deal process to identify any weaknesses that could lead to future breaches.
- Employees should create passwords that are long and complex, containing a mix of upper- and lower-case letters, numbers, and symbols. Avoid using the same password across multiple platforms.
- Enable multi-factor authentication, which provides an extra layer of security requiring additional verification of employee' identity (through a mobile app or a text message code).
- Employees should update their passwords periodically and avoid sharing them with others.
- Employees should be trained to identify red flags such as unexpected attachments, unfamiliar senders, or requests for personal information.
- Encourage employees to enable automatic updates for both work and personal devices they use for work.
- Use VPN (Virtual Private Networks) for your personal device when connecting to company networks, in that way encrypting data and ensuring that communications remain private.

References

News Articles:

- Marriott Agrees $52m Settlement for Massive Data Breach - Infosecurity Magazine (infosecurity-magazine.com)
- Marriott Hotels fined £18.4m for data breach that hit millions (bbc.com)

Videos:

- Marriott data breach affects a half-billion guests (youtube.com)
- Marriott data breach: 500 million Starwood hotel guests potentially affected (youtube.com)