British Airways Breach

Prasanthi Desiraju, Vittorio Pepe, and Will Shin

MSDS 485 Data Governance, Ethics & Law

May 9, 2021

INTRODUCTION

British Airways is one of the leading air carriers and is part of the International Airlines Group, the world's third-largest airline group founded in 2011 from the merger of BA and Iberia, and that owns BMI, Vueling, Aer Lingus, and Air Europa.

Between August 21 and September 5, 2018, BA suffered a cyber-attack that exposed the personal information data of over 400,000 customers. It included usernames, passwords, credit card details but no passport details[1]. The attack was a form of card skimming that is usually obtained using hidden credit card readers on ATMs or other machines where people use the credit card to pay. In the case of BA, the skimming was through a fake BA payments site that would collect the user data [2]. In 2020 the Information Commissioner Office (ICO), an independent body that upholds information right in the UK, imposed a 20 mln pounds fine on BA.

ISSUE

The attack was staged by the threat group Magecart, which exploited a well-known vulnerability of the open-source code Modernizr. This JavaScript library detects the feature available in a user's browser. Both the app and website of BA used Modernizr to operate.

The hackers come into possession of the remote login credential of an employee of a third-party supplier of BA. Once in the system, the hackers were able to move in the network of BA, modify the user privileges to administrator and consequently edit the javascript of the baggage claim webpage to point to a fake BA payment page that would collect the data for the hackers. The

hack was in place for 15 days, and it was able to collect the details of the transactions executed in that timeframe.

On September 6, 2018, BA issued a notice (no longer available) that it had suffered a data breach and subsequently started collaborating with the investigators.

In 2017 ICO issued a notice of intent to fine BA more than 183m pounds under the General Data Protection Regulation (GDPR), but then reduced the fine to 30m and applied discounts for 10m, of which 60% were due to mitigating factors as the company's cooperation with ICO investigation and the prompt notification to the users. The remaining 40% was awarded because of the impact the COVID pandemic had on the airline business [3].

Although the attack is sophisticated in the execution, especially regarding the infrastructure used by the hackers as similar-looking web pages and SSL certificates, it could have been avoided using better authentication protocol, i.e., multi-factor authentication, and better management of the access control. BA also lacked proper security monitoring (a third party notified them regarding the breach) and did not perform penetration testing and scanning [1].

IMPLICATIONS

The data contained the full details of the user, card number, and CCV code, so they could be used to do transactions in the name. There is one reported instance of a card being used, but the transaction was rejected [4].

BA also notified the affected customers and urged them to contact their credit card issuer to check for suspicious transactions [4].

Credit card operators notified the customer that they would be able to monitor and detect fraudulent usage. BA stated that it would compensate anyone who had been financially impacted by the data breach [5].

The data breach resulted in a fine from the authority and brand image damage, although BA assured its customers that they would tighten and increase the security of their IT systems.

It is worth noticing that this data breach, although it targeted BA and its customers, was ultimately directed at credit card issuers and that they had safety systems (fraud detection) in place that helped to limit the financial impact.

DATA LEGISLATION

The GDPR is the European commission's revamped rules on data protection and is in effect since May 2018. All companies operating in the EU should comply with GDPR. GDPR imposes strict regulations on how the user data is to be processed and stored. The companies have to receive consent from users before sharing their data and alert the users if it chooses to transfer the data outside the EU. In addition to this, the company is also liable for a data breach due to a lack of security. Under GDPR, companies can be fined up to 4% of their worldwide turnover in a given year for each data breach.

In this instance, British Airlines is faced with infringement of GDPR due to Poor data security and according to the ICO statement, the British Airways breach was caused by poor and inadequate security arrangements. As a result ICO imposed one of the largest penalties highlighting the seriousness of regulations and that Organizations need to act more responsibly to protect the consumer data. This is one of the first examples of the EU's GDPR in action, and according to ICO's information commissioner Elizabeth Denham "The law is clear, when you are

entrusted with personal data you must look after it" thus stating there is no exception for a data breach though unintentional.

The final amount of £20 million is significantly lower than the initial Notice of intent to fine BA £183.39 million (equating to 1.5% of British Airways worldwide turnover in 2017) is an indication that irrespective of stringent data privacy laws, ICO's primary focus is to bring about awareness and companies can benefit from full cooperation and adapting to GDPR as soon as possible. Though the penalty is reduced, ICO succeeded in increasing the awareness of the risks posed by cyberattacks and the seriousness it places on how companies need to be more vigilant and proactive in taking the data processing responsibilities.

As the digital footprint grows, companies inevitably face unexpected challenges like a sophisticated cybersecurity attack or internal data leaks. While these can't be prevented, any company that deals with vast amounts of data should anticipate being likely targets of such attacks and be prepared by having their security systems up to date to protect their user information. Companies should work towards building fore-sighted response procedures to handle unsought data breaches with appropriate remediation measures will reduce the legal implications and help retain the brand reputations. [6]

DATA BREACH RISK MINIMIZATION STRATEGY

The first step towards data breach readiness is for companies to have a proper incident response plan to apply in a data breach. With increasing inescapable cyberattacks and unforgiving regulations like the GDPR, CCPA for inadequate security practices, companies need to become proficient at cyber resiliency to avoid financial and brand losses. An effective way to minimize

such risks to be well-prepared, and this paper talks about some best practices to achieve the goal.[7][8]

1. Enforce Security Policies: Companies will be able to hold their ground in this digital era by creating and enforcing policies to minimize cybersecurity attacks by training their employees. Most of the security risks resulting from human errors, something as simple as clicking on an unknown link or not disposing of sensitive information promptly. Having policies to train and communicate with employees regularly about the importance of data security and their role in protecting it will help build the necessary foundation to avoid human-prone errors.
2. Monitor Data Outflow : Allowing external systems to access the company's user database could potentially lead to misuse of information if the external systems (vendor) do not comply with the company's security policies. Therefore, it is important to carefully choose a vendor who has written contracts on how this data can be used and user consent for all applicable scenarios before sharing the data. This is a task for all (technical, business, and legal teams) to understand and classify the data sensitivity before integrating with a third-party system.
3. Invest in Cybersecurity Tools : IT systems should be updated periodically with the latest security patches and invest in latest technologies to keep up with sophisticated cyber attacks. This could be enabling multi factor authentication to access any data repository and encrypting all official email communications and documents and so on.
4. Internal Audits, Real Time Monitoring : Building software to detect abnormal activities, say number of failed login attempts, access large volumes of data, etc., allows companies to be proactive and stay ahead of a possible data breach. Additionally, real-time threat

analytics and periodic internal audits say if systems are being updated promptly or not, will highlight the underlying gaps and vulnerabilities, providing greater visibility and mitigating the risks.

5. Build An Incident Response Team: Even with the best possible security measures in place, there can be an unwarranted data breach, and companies must be prepared to react and handle such scenarios effectively. This includes building a team, each with a dedicated role and responsibilities to respond to a data breach by evaluating the level of risk, identifying the people to notify, analyze legal implications, and all such applicable remediations.

Though there is no guaranteed solution to avoid a data breach with ever-growing digital footprint and cloud solutions, there are ways companies can be proactive and at least work towards mitigating the after-effects of such unintentional consequences. With more stringent legal obligations and increased customer awareness about data privacy, organizations should prioritize data privacy and stewardship to avoid damaging penalties caused due to intentional or unintentional non-compliance of data protection laws.

REFERENCES

[1] 'British Airways Data Breach of 2018: A synopsis', 2021, accessed May 8. https://www.cyberclaire.com/blog/BA2018

[2] 'Inside the Magecart Breach of British Airways: how 22 Lines of Code Claimed 380,000 Victims, 2018, accessed May 8. https://www.riskiq.com/blog/external-threat-management/magecart-british-airways-breach/

[3] 'British Airways fined £20m over GDPR breach', 2020, accessed May 8.

https://www.pinsentmasons.com/out-law/news/british-airways-fined-20m-over-gdpr-breach#:~:text=British%20Airways%20(BA)%20has%20been,than%20400%2C000%20of%20its%20customers.

[4] 'British Airways faces record £183m fine for data breach', 2019, accessed May 8. https://www.bbc.com/news/business-48905907

[5] 'BA apologizes after 380,000 customers hit in cyber attack', 2018, accessed May 8. https://www.reuters.com/article/us-iag-cybercrime-british-airways/ba-apologizes-after-380000-customers-hit-in-cyber-attack-idUSKCN1LM2P6

[6]"British Airways Faces Significantly Reduced £20M Fine for GDPR Breach." 2021. The National Law Review. Accessed May 8. https://www.natlawreview.com/article/british-airways-faces-significantly-reduced-20m-fine-gdpr-breach

[7]Thompson, Jerry, and Hilary Tuttle. 2018. "Home." *Risk Management*. November 29. http://www.rmmagazine.com/2018/08/01/data-breach-readiness/

[8]"6 Data Breach Protection Strategies." 2019. *Secuvant*. September 3. https://secuvant.com/6-ways-data-breach-protection/