GDPR Case Study: Marriott International, Inc.

Paul Biberstein
Brown University

Sreshtaa Rajesh
Brown University

Abstract

In November of 2018, Marriott International Inc., a multinational hotel corporation, notified customers of a data breach resulting in the possible disclosure of credit cards, passport numbers, and other personally identifying info belonging to 300 million customers. The breach was the result of an unknown attacker who had gained access to the systems of Starwood hotels in 2014, who then merged with Marriott in 2015. The Information Commisioner's Office (ICO) of the United Kingdom fined Marriott £18.4 million for the breach, citing the General Data Protection Regulation article 32 which states that companies serving EU residents must take appropriate measures regarding securing personal data. The penalty set a notable precedent for GDPR-related adjudication due to the ICO citing COVID-19 and Marriott's cooperation in the investigation as reasons for lessening the resulting fine.

1 Background

1.1 GDPR

The General Data Protection Regulation (GDPR) is a privacy regulation enacted by the European Union in 2018 that guarantees certain rights to customers when they provide personal data to corporations. In GDPR parlance, the corporation is the *Data Controller*, any companies the corporation orders to process or store data is a *Data Processor*, and the customer whose data is being processed is the *Data Subject*. In the case of violations, the EU will appoint a *Lead Supervisory Authority* as adjudicator. We can examine the relevant background for this case study by seeing who each of the data controller, processor, and subject were in this case, as well as which member state ran the lead supervisory authority.

1.2 The Parties Involved

Data Controller. Marriott International, Inc. is a hotel operator and franchise based in Maryland, U.S.A. Taking into account franchising agreements, Marriott has over 7,000 properties spread across 131 countries [6], including numerous EU member states. In 2015, Marriott acquired Starwood Hotels and Resorts, Inc., another hotel operator and franchise with over 1,000 properties, in a $13 billion merger [7]. During the period immediately following the merger, the Starwood and Marriott computer systems remained separate pending future integration. The system which suffered the data breach was the Starwood reservation system, which was in charge of storing and processing customer data regarding room bookings.

Data Processor. Since Marriott stored and processed their data in-house, they are also the data processor in this case [3].

Data Subject. Although Marriott is based in the U.S.A., the GDPR applies to any companies with customers physically in the EU. This means that by storing the records of 7 million U.K. customers (who, at the time, were in the Union), Marriott ensured they fell under the purview of the GDPR [3, 1].

Lead Supervisory Authority. The data breach was reported to the U.K.'s ICO on the 22nd of November, 2018. The ICO proceeded with their own investigation and eventually became the lead supervisory authority to determine the extent of violation of the GDPR and associated penalty.

2 The Data Breach

On the 29th of July 2014, an attacker gained physical access to a machine on the Starwood network and installed

a web shell. The machine was connected to the internet and had administrative privileges since it was running a service that allowed employees to make changes to the Starwood website. Using the web shell, the attacker installed a remote access trojan on the system, which gave the attacker access to a shell with root-level privileges on the effected machine and network-adjacent machines.

From here, the attacker utilized software to harvest user credentials from memory. This allowed the attacker to escalate their privileges by leap frogging to higher-privileged users. We will discuss later why this was possible despite Starwood employing multi factor authentication on employee accounts.

After a dormant period of approximately one year, the attacker returns and proceeds to export tables from many Starwood databases. This proceeds infrequently until September 2018, when the user scans a database containing credit card information. This sets off an alert in the Marriott system, triggering a response team investigation. 10 days later, the attackers trojans were identified and remote access was blocked, but not before a number of tables with sensitive data were exported.

Following detection of the breach, Marriott reported the incident to the FBI and the ICO, 1 month later and 2 months later respectively. Shortly after notifying the ICO, Marriott notified their customers via email and set up a dedicated call centre for affected customers, as well as offering 1 year of fraud detection to all affected customers.

3 GDPR Violation

The fine imposed on Marriott by the ICO in 2018 is a result of a violation of Article 32 of the GDPR, but the ICO also referenced shortcomings in the Marriott's fulfillment of Articles 33 and 34 that were not ultimately included in the final penalty.

1. **Article 32.** Article 32 specifies that any stored information that can be used to identify a natural person must be protected with appropriate security measures, such as encryption and access control policies [1]. During their investigation, the ICO found 1) a lack of monitoring privileged accounts and database activity, 2) a lack of encryption-at-rest for certain classes of data (passport numbers being one), and 3) a lack of strict access control policies on a server with personally identifiable information [5]. Previous fines involving violation of article 32 include a €27.8 million fine of British Airways by the ICO in 2020 and a €12.3 million fine of Vodafone Italy by the Italian Data Protection Authority also in 2020 [2, 4].
2. **Article 33.** Article 33 states that in the event of a likely security breach, the data controller must notify an appropriate authority within 72 hours where feasible, or provide valid reasons for the delay [1]. The ICO argued that while the Marriott waited until they were *certain* that a breach had occurred to notify, the GDPR specifically states that the data controller should report whenever they find the possibility of a breach *likely*, even if not certain [5]. This ruling was not considered in the fine.
3. **Article 34.** Article 34 states that in the event of a data breach, the controller must inform data subjects, in clear language and without delay, that their data may have been compromised [1]. While the Marriott did take prompt action, the ICO identified a few minor shortcomings in their communication to subjects, such as failing to provide a phone number to their call center in the email they sent out [5]. These few errors were also not considered in the fine.

Who is Responsible? A variety of contributing factors were cited by the ICO that led to the data breach, which will we discuss when talking about what could have prevented the attack. However, one specific technical factor is of special note: the lack of multi factor authentication of high level accounts that let the attacker escalate their privileges. Why did Marriott not ensure that multi factor authentication was in place? It turns out, they did, with two independent audits. How the oversight occurred is unclear, but we can see that this is one case where Marriott remains blameless. The ICO agrees with us, as they chose not to fine Marriott for lacking multi factor authentication since they had made reasonable efforts to ensure the opposite was the case when acquiring Starwood.

What Could Have Prevented This? We can make a list of recommendations for Marriott's security and privacy team by examining the list of shortcomings the ICO cited. Specifically, we can make the following recommendations:

1. Add monitoring on privileged accounts
2. Add monitoring of database activity
3. Improve encryption schemes for at rest data
4. Increased levels of access control on servers with PII

Implementing the above would have either lessened the impact of the attack or facilitated earlier detection. These are all standard practices at large tech corporations where data is central to their business model, but for companies like Marriott data protection standards can fall by

the wayside. As Systems researchers, we can develop software that provide these features off-the-shelf to encourage their widespread adoption.

4 Discussion

Overall, the breach and ensuing penalty seem to be a textbook case of GDPR enforcement helping the people. Marriott knew that existing as a large corporation in the 21st century required hiring teams of security and privacy engineers and auditing company practices. However, as revealed by the ICO, some of their security and privacy efforts appeared to be an afterthought, such as the lack of access control policies that allowed an attacker to compromise a Starwood machine, and the lack of at-rest encryption that allowed them to view personally identifying information. However, the Marriott represents a close-to-ideal data controller in terms of their *response* to the breach. They did not attempt to hide the incident, rather they owned up to their mistakes (evident in their decision not to appeal the notice of GDPR violation) and actively assisted the ICO in their investigation. The Marriott also provided ample support to customers—they established a call center for affected individuals to seek help, and also offered them one free year of data monitoring by WebWatcher (paid for by the Marriott). At the same time, the £18.4 million penalty imposed on them was significant (rightfully so, due to the fact that close to seven million customers' information *could* have potentially been leaked). This fine sends a clear message to the Marriott about adopting adequate precautions in the future, and sends a message to similarly sized companies that privacy cannot be an afterthought and that those who treat it as such will be punished accordingly.

Something else notable about this case is the fact that the ICO specifically cited Marriott's cooperation in the ensuing investigation as well as econonmic hardship from the COVID-19 pandemic as reasons for lessening the fine from £28 million to £18.4 million. This serves as a lesson to future companies that the customer-centric breach response that Marriott employed, like opening a call centre and providing fraud detection services, can make supervisory authorities look more kindly when deciding on a penalty.

This

References

[1] European Commission. 2018 reform of eu data protection rules. https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf, 2020. [Online; accessed 24-September-2021].

[2] Information Commissioner's Office. British airways penalty notice. https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf, 2020. [Online; accessed 24-September-2021].

[3] Information Commissioner's Office. Marriott international, inc. penalty notice. https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf, 2020. [Online; accessed 24-September-2021].

[4] Italian Data Protection Authority. Garante per la protezione dei dati personali. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9485681, 2020. [Online; accessed 24-September-2021].

[5] Michael Drury. £18.4 million marriott international gdpr fine announced by ipo: What did we learn? https://www.lawyer-monthly.com/2020/11/18-4-million-marriott-international-gdpr-fine-announced-by-ipo-what-did-we-learn/, 2020. [Online; accessed 24-September-2021].

[6] Wikipedia contributors. Marriott international — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Marriott_International&oldid=1042859437, 2021. [Online; accessed 24-September-2021].

[7] Wikipedia contributors. Starwood — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Starwood&oldid=1022905391, 2021. [Online; accessed 24-September-2021].