**Assignment**

**Brief**

**Discuss and present a Security Vilnerabilities and Cyberattacks**

* What happen?
* What is the effect?
* How it did happen?
* How they solve the problem?
* How to prevent?

**Topic Example:**

* 2010 - WeWork Network Vulnerabilities
* 2014 - Cyber Attack on Yahoo
* 2017 - WannaCry ransomware attack.
* 2018 - A Cyber Attack on Marriott Hotels

You may pick some other topic that related to security and present it.

**Submission**

* Submit the URL of the GitHub Repository that contains your work to NTU black board.

**2018 - A Cyber Attack on Marriott Hotels**

**What happen?**

The breach took place sometime in 2014, but it wasn’t discovered until 2018, when an internal security tool caught a suspicious attempt to access the internal guest reservation database for [Marriott’s Starwood brands](https://hoteltechreport.com/news/marriott-hotel-brands). Starwood Hotels was acquired by Marriott in 2016, adding 11 new brands to add to Marriott International’s original 19 assets.

The internal security alert prompted an investigation which discovered that the Starwood network was compromised in 2014, before the acquisition. Starwood had not migrated Mariott’s reservation system in 2018; Starwood brands were still using legacy IT infrastructure, which contributed to the scope and scale of the data breach.

In their internal investigation, Marriott found that hackers had encrypted data and removed it from the Starwood system. That information included information from up to [500 million guest records](https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html) – although some of those records were duplicates. When they announced the breach, Marriott said that the hackers [stole guest information](https://www.zdnet.com/article/marriott-announces-data-breach-affecting-500-million-hotel-guests/) that included “a name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some of these guests, payment card data was also stolen, but Marriott did not say for how many.”

**What is the effect?**

Financially, Marriott faced significant penalties as a result of this data breach. Multiple [class-action lawsuits](https://www.vox.com/the-goods/2019/1/11/18178733/marriott-starwood-hack-lawsuit) were filed against the brand targeting Marriott’s failure to perform its due diligence on Starwood’s IT systems. In addition to the lawsuits, Marriott agreed to pay for [passport replacements](https://topclassactions.com/lawsuit-settlements/data-breach/marriott-data-breach-class-action-allowed-to-proceed/) for customers who victims of the data breach.

Separately, the United Kingdom’s [Information Commissioner’s Office](https://ico.org.uk/about-the-ico/) (ICO), a consumer rights watchdog, fined Marriott [$23.8 million](https://techcrunch.com/2020/10/30/uk-watchdog-reduces-marriott-data-breach-fine-to-23-8m-down-from-123m/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAAQ19qZlPfFRYWIkouWSoP08mPT-jQKBlX4_ExvMcGOReLxo_tlVDRQmUGilw3qDtKtc27yUtKf-rjYOqKOuMNVhGRBrtffeNEh38e39p1okFLf8tuOBUiToYpCEACjAB8UCBS5USUkUpdqBnT9ae0L3KgJWTfC9jsBOLvWVJcKA) (down from the original penalty of $123 million) for failing to meet security standards required by [GDPR](https://hoteltechreport.com/news/data-protection-act) (General Data Protection Regulation). The [ICO argues](https://www.zdnet.com/article/marriott-fined-gbp18-4-million-by-uk-watchdog-over-customer-data-breach/) that Marriott failed to "put appropriate technical or organizational measures in place" when processing data, though it also acknowledged that Marriott has since taken the proper measures to improve security. Notably, the original fine of $123 million would have been one of the largest penalties issued under GDPR, representing around [3% of Marriott’s total revenue](https://techcrunch.com/2020/10/30/uk-watchdog-reduces-marriott-data-breach-fine-to-23-8m-down-from-123m/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAAQ19qZlPfFRYWIkouWSoP08mPT-jQKBlX4_ExvMcGOReLxo_tlVDRQmUGilw3qDtKtc27yUtKf-rjYOqKOuMNVhGRBrtffeNEh38e39p1okFLf8tuOBUiToYpCEACjAB8UCBS5USUkUpdqBnT9ae0L3KgJWTfC9jsBOLvWVJcKA).

It’s true that financially, Marriott will likely survive this data breach. Customer satisfaction scores, however, [dipped in 2019](https://www.statista.com/statistics/194728/customer-satisfaction-with-us-marriott-hotels-since-2008/), bringing the brand [even with Hilton](https://bethesdamagazine.com/bethesda-beat/business/marriott-continues-to-get-high-marks-in-customer-satisfaction/) and suggesting that the breach may cause more long-term harm to guest loyalty. Studies show that nearly [a quarter of Americans](https://www.zdnet.com/article/one-in-four-americans-wont-do-business-with-data-breached-companies/) will stop doing business with a company that has been hacked, while more than two in three people trust a company less after a data breach.

**How it did happen?**

The actual specifics of the attack get pretty technical, but there were some business and cultural practices at Starwood that underpin how easy it was for a bad actor to access that many guest records.

[Crowdstrike](https://www.crowdstrike.com/) cybersecurity expert Ryan Cornateanu [told Hotel Tech Report](https://hoteltechreport.com/news/marriott-hacked), “The attack on Marriott was hapless and a popular entry point for adversaries is through email spoofing. This tactic is used in phishing in order to get malware onto a target network to then move laterally across all systems.  From there hackers can leverage account numbers, driver's license numbers and other sensitive information from loyalty programs and reservations systems.  The general data protection regulation has gone a long way to protect consumers but there's only so much that can be done when a hacker is able to secure login credentials or access servers directly.”

Starwood was notorious for having an [insecure reservation system](https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/); a separate attack in 2015 compromised data and wasn’t detected for [eight months](https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html). Marriott then compounded the issue by laying off Starwoods IT staff during the acquisition in 2016. The lack of personnel prevented Marriott from quickly integrating newly added hotel properties into its own in-house reservation system. Starwood’s already-insecure guest reservation system, therefore, “limped on, zombie-like, infected with malware, breached by hackers, and without much by way of continuity of care, for another two years before the breach was finally discovered,” reports [CSO Online](https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html).

As to the question of who hacked Marriott, that answer is even more complicated. Both the [New York Times](https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html) and the [Washington Post](https://www.washingtonpost.com/technology/2018/12/12/us-investigators-point-china-marriott-hack-affecting-million-travelers/) reported that the attack was part of a state-sponsored intelligence-gathering effort on behalf of the Chinese government. Patterns in the code as well as the method of the attack echo techniques previously employed by Chinese hackers, and none of the guest records ended up for sale on the dark web – a clue that this wasn’t a hack for profit.

**How they solve the problem?**

We may never know all the details behind this breach, but just from what we've discussed here, a lot of important things should have come into focus:

* Starwood and Marriott were guilty of [basic security failings](https://www.computerweekly.com/news/252453521/Marriott-data-breach-highlights-basic-failings): Lack of defense in depth that allowed attackers to stay in the system for years after breaching it, for instance, and failure to keep encrypted data and the keys used to encrypt it separate. Marriott failed to follow the most important cybersecurity rule: [assume you are compromised](https://krebsonsecurity.com/2018/12/what-the-marriott-breach-says-about-security/) and act accordingly.
* The [bumpy transition associated with the Marriott-Starwood merger](https://hbr.org/2019/03/the-marriott-breach-shows-just-how-inadequate-cyber-risk-disclosures-are) — the firing of Starwood's IT staff, and the long period during which Starwood's legacy systems were maintained in limbo — exacerbated the problem. The big UK fine is a hint that regulators will be holding post-merger corporations liable for these kinds of issues.
* Travel data is rich in information that can offer [key insights into the lifestyles, tastes, and relationships](https://krebsonsecurity.com/2018/12/what-the-marriott-breach-says-about-security/) of individuals, but the travel industry is far behind sectors like banking when it comes to cybersecurity and needs to catch up now.

**How to prevent?**

Ultimately independents are far safer than brands because they have less attractive loot for hackers.  Less loot means less incentive.  Further, independents often work with best of breed tech vendors rather than attempting to develop systems in-house.  These vendors are venture-backed and take great measures to ensure data security.  Hoteliers should look for software vendors who meet rigorous standards with regards to modern regulatory frameworks like [SOC-2](https://hoteltechreport.com/news/oaky-soc-2-certification), GDPR, [PSD2 and PCI](https://hoteltechreport.com/news/pci-psd2-hotel-industry) compliance.

But still, even amongst independents - the hospitality industry is an attractive target for hackers. There’s a huge amount of personally-identifiable information collected by hotels, and often outdated or few security protocols protecting this valuable data. It’s not out of the question that your hotel could be the target of a cyber attack in the future: however, it’s crucial to avoid the mistakes that Marriott made in failing to find the breach for four years.

The first priority of any hotel’s IT team should be to encrypt guest data and set up alerts to immediately warn when there’s been a potential security breach. Legacy IT must be brought up-to-date; make sure the newest version of your software is installed on all devices. Security updates often contain patches and new fixes that evolve with the threat landscape. And, have a plan to communicate with customers as soon as you sense there’s been a breach. The question shouldn’t be “if” there will be a [cyberattack](https://hoteltechreport.com/news/geopolitics-cybersecurity) – but when.