Marriott Data Breach

ISE 331 PROJECT BY:
AMBER LI, JAMES HARVEY, YASH MATHUR

Marriott Hotel in Cape Town, South Africa

OUTLINE

- Introduction
- Background Information
- Technology
- Execution
- Impact/Scope
- Responses
- Implications
- Similar Topics
- Conclusion

ABOUT MARRIOTT INTERNATIONAL

Founded in 1927 in Washington D.C.

Manages at least 6500 locations around the world

Operates 30 brands in total including some well-known names such as “The Ritz-Carlton,” “Sheraton Hotels and Resorts,” “Westin Hotels & Resorts”

Generates more than $21 billion in revenue annually

INTRODUCTION

- Marriott's database suffered a data breach
- Began in 2014
- All the hotels and resorts belonging to their "Starwood" division were affected
- Breach detected in October 2018, affecting an estimated 500 million people

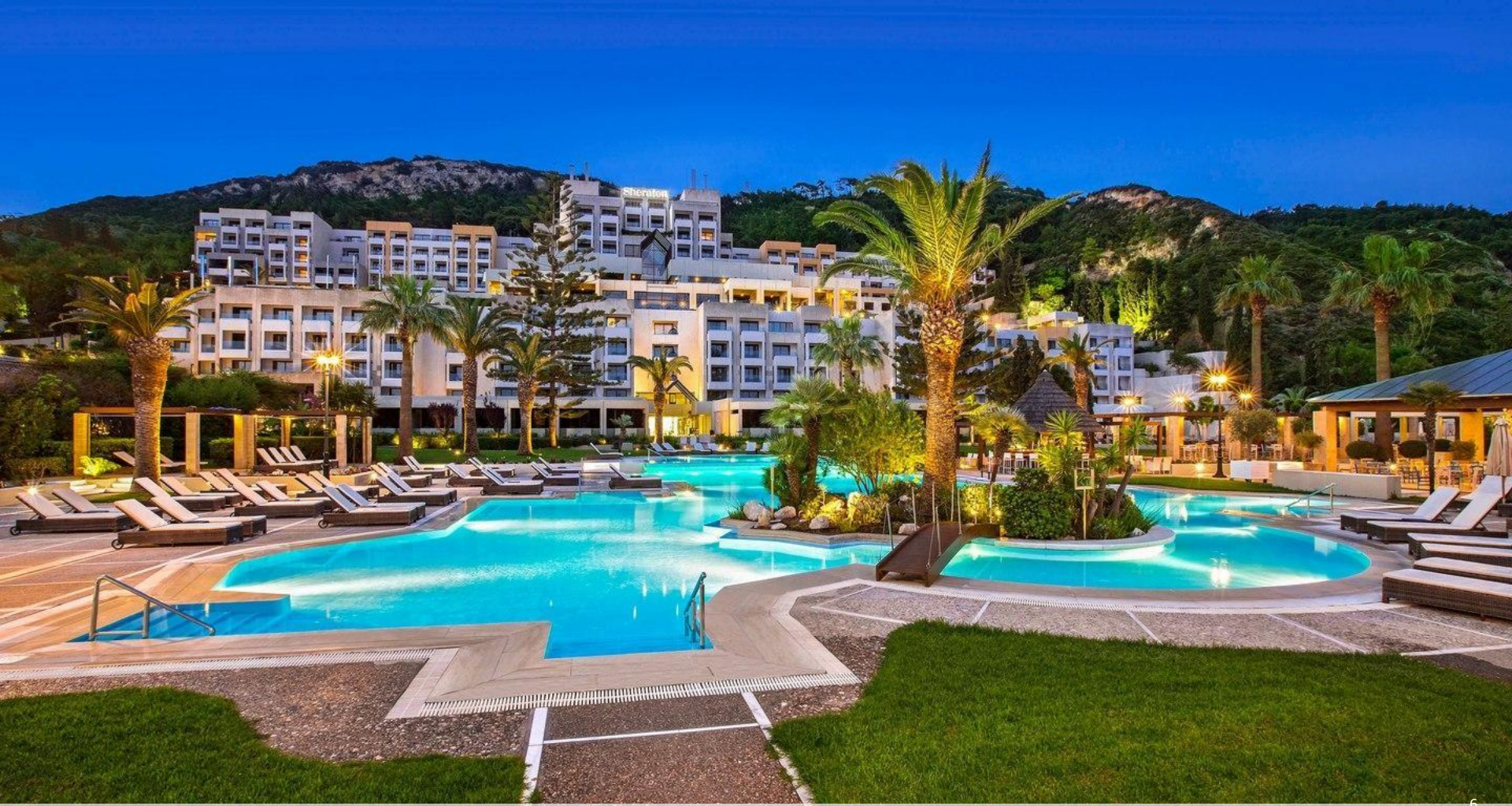
BACKGROUND INFORMATION

Starwood's guest reservation database had a security vulnerability that allowed unrestricted access

Starwood suffered a credit card breach from malware on their point-of-sale systems

Marriott acquired Starwood for $13.6 billion, creating the world's largest hotel chain

Vulnerability in Starwood database discovered through security system alert



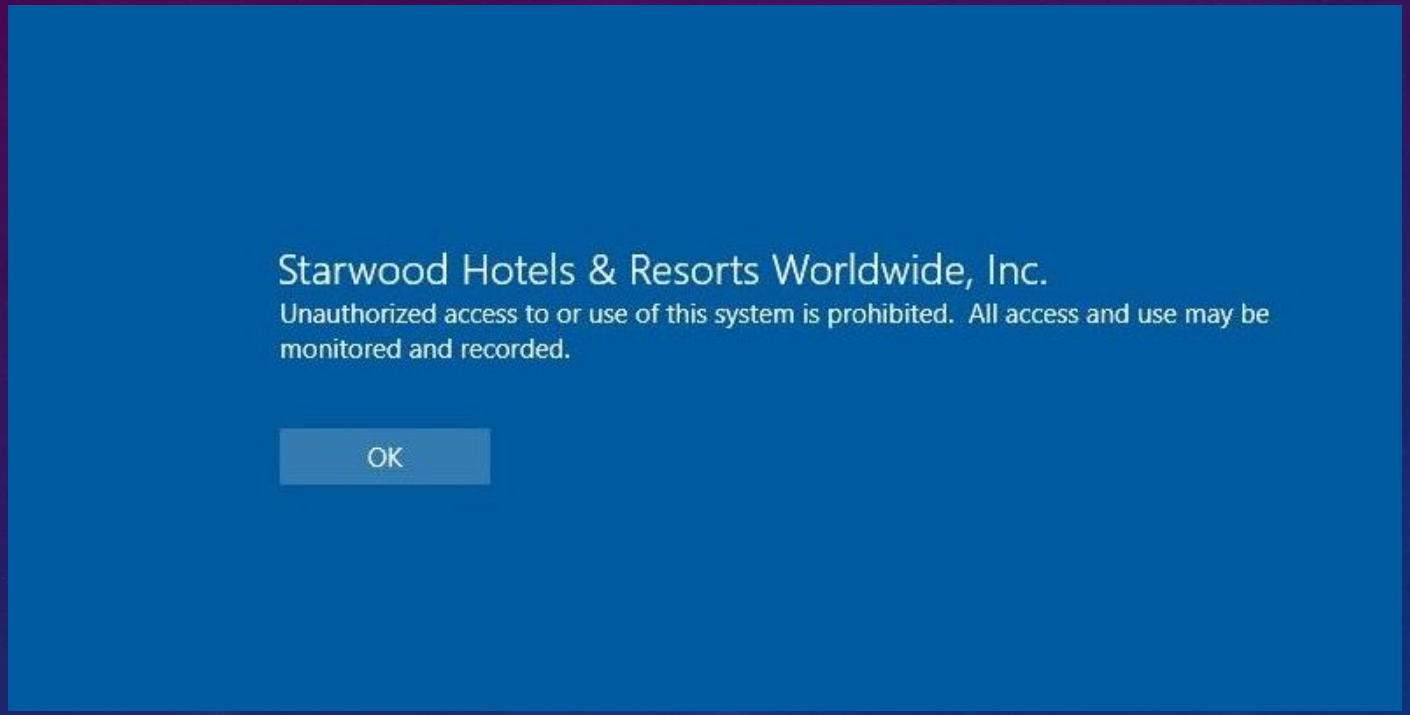
Sheraton

TECHNOLOGY

- Starwood's technology that was most likely at fault was their reservation system ("Valhalla").
- "Valhalla" was designed with modern security features that were adequate for usage by Starwood
- Credit card numbers were encrypted with AES-128
- "Two components needed to decrypt the payment card numbers"
- Decryption keys were compromised
- Outdated versions of Windows Server on the computers

TECHNOLOGY

- Starwood had multiple databases:
  - Starwood Preferred Guest member database
  - Reservation system
  - “Data Warehouse” (analysis and marketing)
- Marriott migrated data from these databases
- Remote access via telnet and RDP was left open to the internet
- Hackers had avoided detection while exfiltrating information for at least 4 years
- Stolen information was re-encrypted by hackers to avoid being flagged as sensitive data passing through system


Starwood Hotels & Resorts Worldwide, Inc.
Unauthorized access to or use of this system is prohibited. All access and use may be monitored and recorded.
OK

SEC standards for cybersecurity disclosure

- In April 2018, the SEC fined Yahoo $35 million for misleading investors by failing to disclose their data breaches to the investing public until more than two years later, in 2016

- The SEC acknowledges that there is no existing requirement in the securities laws that explicitly refers to cybersecurity risks and cyber incidents.

VIEWS FROM SECURITY EXPERTS

- “...Starwood was breached two years prior to the Marriott acquisition, which brings up the question of: 'To what extent should Merger & Acquisition due diligence extend to cybersecurity audit, and if indeed this was done at the time, why did it not uncover this issue?'...” - *Matt Aldridge, senior solutions architect, Webroot*

VIEWS FROM SECURITY EXPERTS

- “...in comparison with banks, hotels have a 400% higher rate of critical software vulnerabilities present in internet-facing systems that store and process sensitive, regulated information. In comparison with healthcare, hotels have a 180% higher rate." - *Kelly White, founder and CEO of RiskRecon*

- “...there were intrinsic gaps in human oversight that resulted in missed warning signs and ultimately, inaction. You can have the best security tools money can buy, but if you don’t invest equally in the people interacting with the technology, then you’re making a costly mistake.” - *Tom Callahan, Director of MDR Services, ControlScan*

EXECUTION

- Hackers remotely accessed the computers and installed a “RAT”
- Covered footsteps by encrypting and deleting data that was stolen
- Exfiltrated data by encrypting it to hide detection
- Suspected Chinese government involvement in the attack
- Targeted vulnerability in Starwood database, which allowed unauthorized access since 2014

IMPACT

- ~9.1 million unique credit card numbers stolen
- ~23.75 million unique passport numbers stolen
- Guests' personal information lost
  - Date of birth, names, etc.
- Loss of membership points/benefits
- Marriott International's stock price (NASDAQ: MAR) dropped 5.6% after releasing statement
  - Ended in low of $100.62 just before Christmas

SCOPE

- Affected ~500 million guests
- Estimated ~$1 billion in damages
- Could face up to $1 billion in legal fines
- Could cost many billions to replace passports
- Attack linked to Chinese government
- Data that was stolen is not being sold on dark web
- Seemingly part of a non-commercial, large-scale campaign to gather data

MARRIOTT'S RESPONSE

- Issued public statement in November 2018 disclosing the breach to its customers
- Attempted to address customers' concerns
- Hired Kroll to provide free year of WebWatcher service
- Dedicated call center about the incident for each country

PUBLIC RESPONSE

- Marriott was heavily criticized by security experts, journalists, customers
- Immense media coverage on data breach
- Paranoia among guests with stolen passport details
- Chinese government denied any involvement in the breach
- Multiple class-action lawsuits filed against Marriott for failing to protect sensitive customer information

IMPLICATIONS

- Database security should be topmost priority
- Detecting mechanisms should be more effective since it took 2 years for Marriott to be notified about the breach
- Defense from international breaches
- Future breaches could be even more dangerous as data becomes increasingly personal
- California Consumer Privacy Act

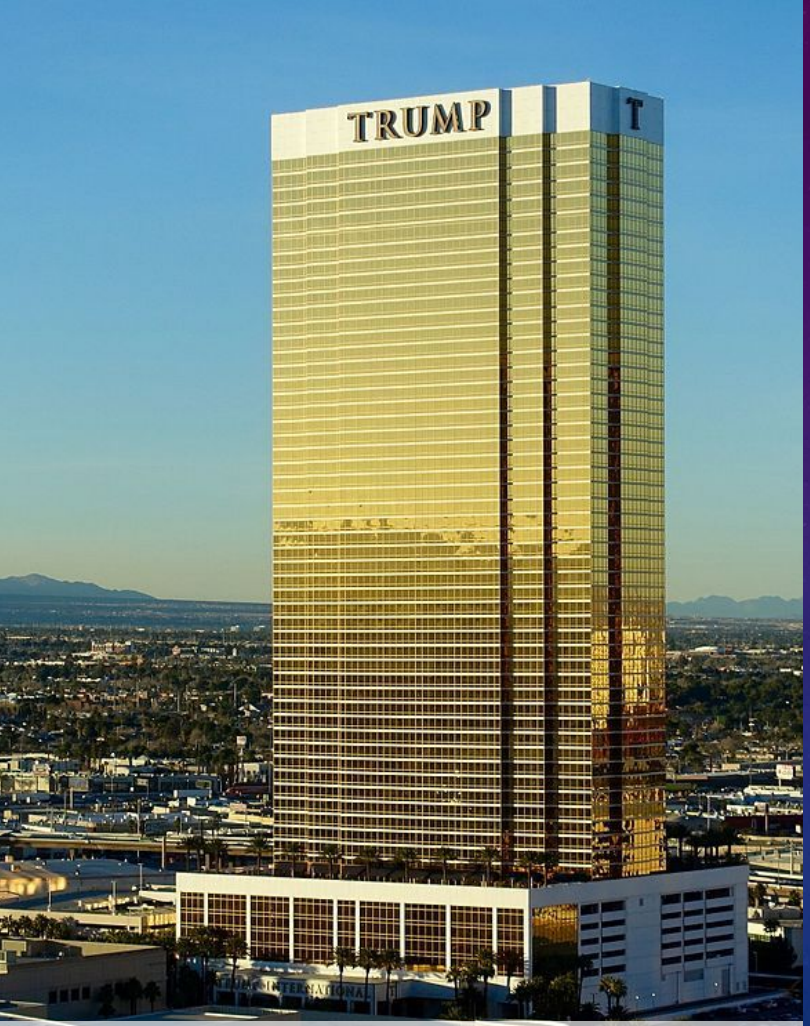
SIMILAR TOPICS

TRUMP HOTELS

HYATT HOTELS

CATHAY PACIFIC AIRWAYS

MANDARIN ORIENTAL



Trump Hotel in Las Vegas, NV

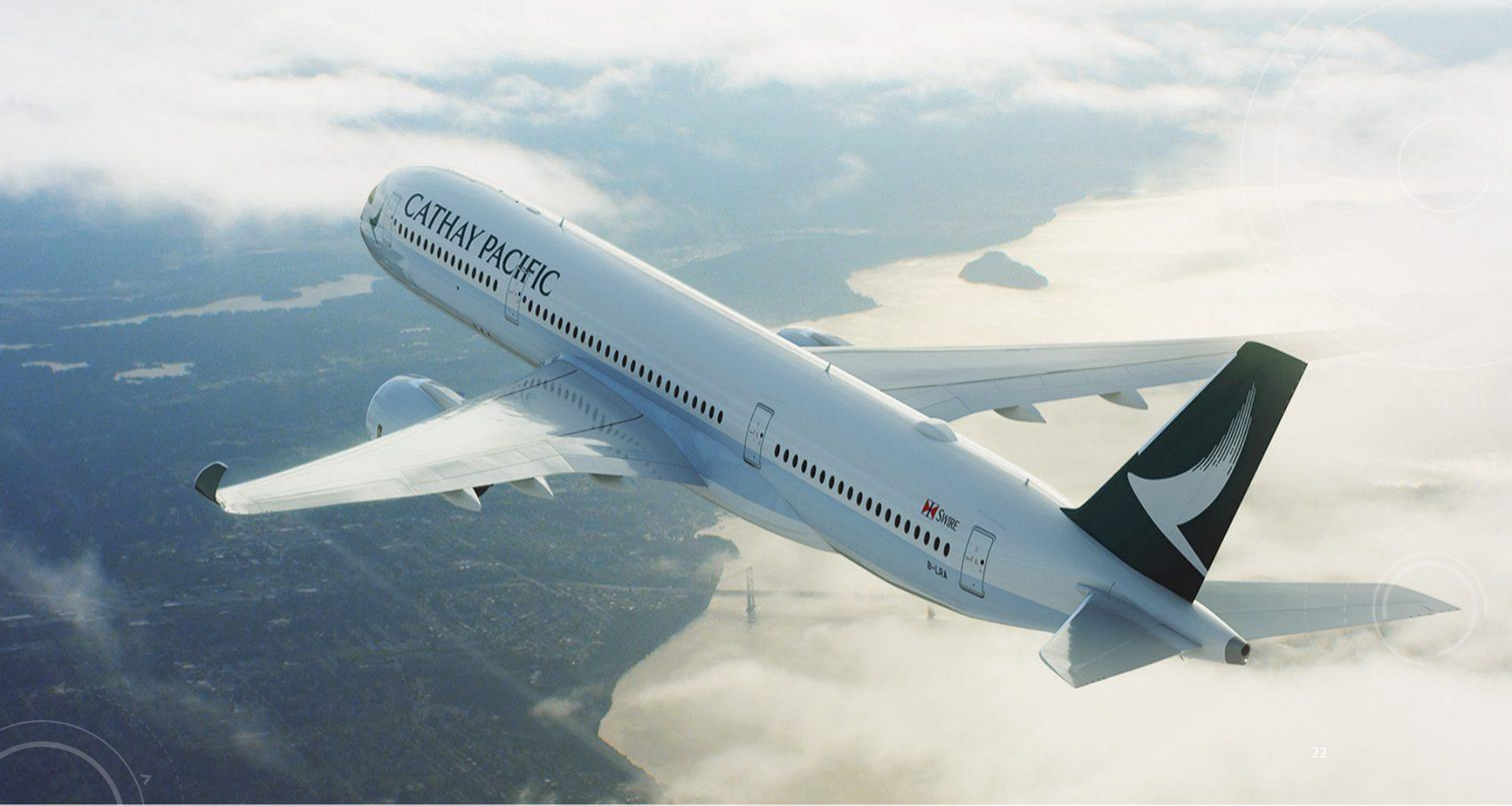
TRUMP HOTELS

- Hotel management company based in the US
- Occurred between August 2016 and March 2017
- 13 hotels affected
- Credit card and transaction details stolen
- “Unauthorized malware access to payment card information as it was input into the payment card systems...”

HYATT HOTELS

- Multinational hotel chain, like Marriott
- Breach occurred between July 2015 and December 2015
- "The investigation identified signs of unauthorized access to payment card data from cards used onsite at certain Hyatt-managed locations, primarily at restaurants." - *Chuck Floyd, Global President of Operations at Hyatt Hotels Corporation*
- The breach impacted 250 properties across 50 countries, mostly in China

Hyatt Regency Sydney, in Darling Harbour, Australia



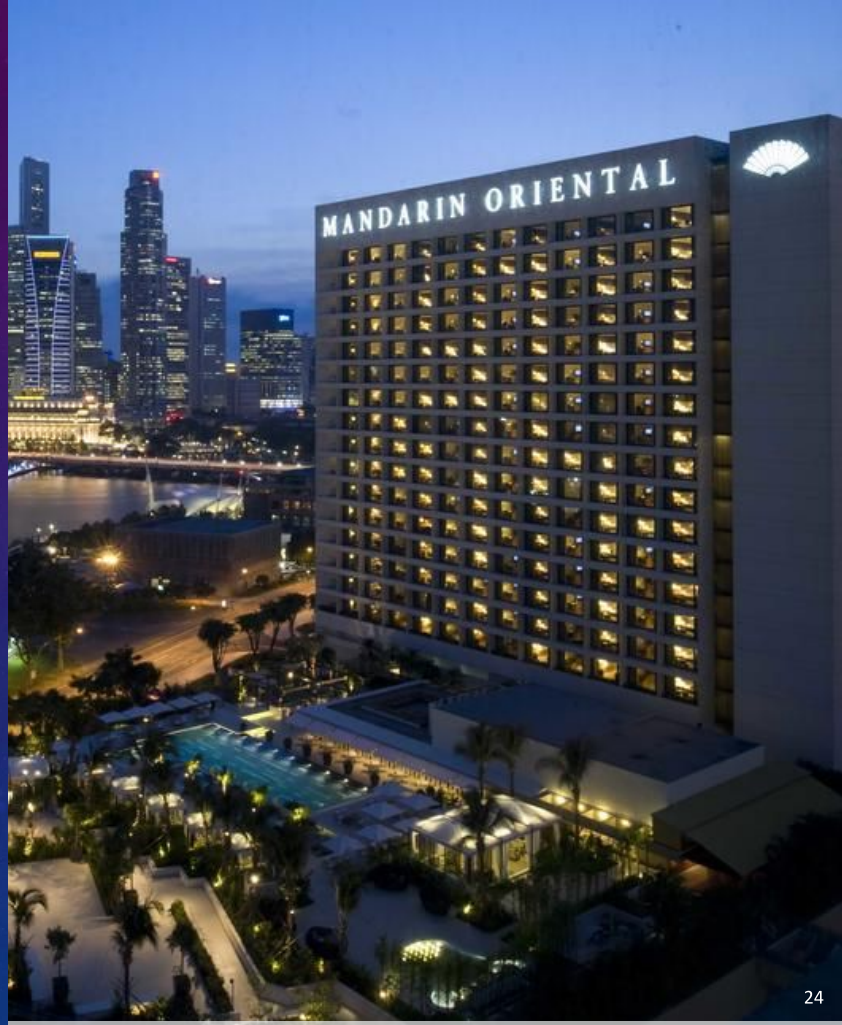
Cathay Pacific Aircraft, somewhere in the stratosphere

CATHAY PACIFIC

- International airline carrier based in Hong Kong
- Hack detected around October, 2018. Over 9.4 million customers affected, about 860,000 passport numbers and 245,000 Hong Kong IDs exposed, has been described as a “sustained three-month-long cyberattack”
- Public outcry over the outdated two decade old privacy laws

MANDARIN ORIENTAL

- International hotel and resort group
- Occurred starting on June 2014, completely resolved by March 2015
- 10 properties in Boston, Florida, Las Vegas, Miami, New York, and Washington D.C. were compromised
- Credit card breach
- Caused by malware attack



Mandarin Oriental Hotel, Singapore

COMPARISONS

- All 5 incidents occurred in the last 10 years
- Several were international hotel management companies
- Credit cards & passport details
- Unauthorized access to system that stored customers' personal data

CONCLUSION

- Exemplifies the importance of cybersecurity practices
- Hotels are especially targeted for their large consumer base and database of personal information
- All businesses that collect personal data should implement more rigorous security policies

REFERENCES

- https://www.bloomberg.com/news/articles/2018-12-14/marriott-cyber-breach-shows-industry-s-hospitality-to-hackers
- https://www.npr.org/2018/12/12/675983642/chinese-hackers-are-responsible-for-marriott-data-breach-reports-say
- https://www.businessinsider.com/marriott-data-breach-which-hotels-affected-2018-11
- https://phys.org/news/2018-12-breaches-marriott-treasure-troves-spammers.html
- https://answers.kroll.com/?gclid=EAIaIQobChMI6IHdkpWR4QIVRIezCh2y8wEUEAAYASAAEgIGCfD_BwE&gclsrc=aw.ds
- https://www.esecurityplanet.com/network-security/trump-hotels-confirms-credit-card-breach.html
- http://fortune.com/2018/10/25/cathay-pacific-biggest-airline-data-breach-hack/
- https://answers.kroll.com/?gclid=EAIaIQobChMI1_rGotb24QIVRlcMCh2luwB4EAAYASAAEgLHrPD_BwE&gclsrc=aw.ds
- https://www.phocuswire.com/Marriott-data-breach-ex-Starwood-perspective
- https://www.hospitalitynet.org/opinion/4078764.html
- https://marriott.gcs-web.com/static-files/733886b2-f409-478a-9986-16044b6fcf58
- https://www.wired.com/story/marriott-hack-protect-yourself/
- https://www.washingtonpost.com/technology/2018/12/12/us-investigators-point-china-marriott-hack-affecting-million-travelers/?noredirect=on&utm_term=.ca4d9d86df92
- https://www.forbes.com/sites/kateoflahertyuk/2019/03/11/marriott-ceo-reveals-new-details-about-mega-breach/#3a34c425155c

REFERENCES (CONT.)

- https://news.marriott.com/2016/09/marriotts-acquisition-of-starwood-complete/
- https://krebsonsecurity.com/2018/11/marriott-data-on-500-million-guests-stolen-in-4-year-breach/
- http://time.com/5467781/marriott-data-breach-information/
- https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach
- https://techwireasia.com/2018/12/what-caused-the-marriott-data-breach/
- https://www.marketwatch.com/story/marriotts-stock-sinks-after-disclosing-data-breach-affecting-up-to-500-million-guests-2018-11-30
- https://krebsonsecurity.com/2015/03/credit-card-breach-at-mandarian-oriental/
- https://hospitalitytech.com/cyber-security-experts-weigh-marriottstarwood-data-breach
- https://www.bloomberg.com/quote/MAR:US
- https://www.mandarinoriental.com/
- https://www.cnbc.com/2017/07/12/trump-hotels-discloses-data-breach-at-14-properties.html
- https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html
- https://www.synack.com/blog/the-marriott-breach-implications-consequences-accountability/
- https://www.businesstraveller.com/business-travel/2018/11/13/cathay-pacifics-data-breach-update/
- https://www.prnewswire.com/news-releases/class-action-lawsuit-filed-on-behalf-of-plaintiffs-whose-sensitive-personal-information-was-stolen-in-breach-of-marriott-servers-300758440.html
- https://krebsonsecurity.com/2015/11/starwood-hotels-warns-of-credit-card-breach/