|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  | |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |
| **Name** | | Bohan Zhang | | | | | | |  | INFO6027 |  | Specific Details: |  |  |  |  |  |  |
| **ID** | | 0814917 | | | | | **Date:** | 6/1/2019 |  | Assignment 1 |  | Make, Model, Serial Number: |  |  |  |  |  |  |
|  | |  | |  |  | |  |  |  |  |  | Configuration: |  |  |  |  |  |  |
| **Business Impact Analysis** | | | | | | | | | | | |  |  |  |  |  |  |  |
|  |  | |  | |  |  | |  |  |  |  |  |  |  |  |  |  |  |
| **Risk ID** | **Threat** | | **Asset Affected** | | **Risk Description** | **Risk Type** | | **Probability (High/Medium/Low)** | **Risk Impact (High/Medium/Low)** | **Primary Effect-(Cost of Downtime)** | **Trigger (Initial Cause)** | **Avoidance Plan** | **DAP to DRP Ratio (% avoided)** | **Incident Management Required** | **DR Process** | **Risk Owner** | **Status** | **Ranking**  **L/I** |
| **1** | **Hacking or unauthorized access by external hackers** | | **Customer sensitive Data such as Personal Identification , Credit Card etc.** | | **Due to human error fall into the phishing attack, the hacker could drop RAT and get into the reservation system stealing or modify user data** | **Human Risks, Cyber Terrorism** | | **High** | **High** | **The major effect of hacking for the reservation system is loss of brand reputation. If 500 million users data lost, could lead fine and direct loss from $200 million to $1 billion[[1]](#footnote-1) also could lead to stock price drop dramatically [[2]](#footnote-2)** | **Hacker use email targeting spear phishing trick Starwood staff download RAT on their computers and gain remote initial access. Unusual database query risen security flag,**  **Data stealing** | **Install Anti phishing software or let third party scan each email in real time to determine if is phishing email or not, and doing user phishing email awareness training and ongoing phishing email penetration testing training [[3]](#footnote-3)** | **99%** | **Contain** | **Inform authorities and user the breach. Retrain people, educate them how to not fall into phishing emails. Isolate the affected machines and eradiate the RAT and Mimikats.** | **Marriott Inc, Customers** | **Active** | **5/5** |
| **2** | **Internal staff or previous employees modify or access in unauthorized manner** | | **Customer sensitive data such as Personal Identification, credit card etc/** | | **Internal staff intentional or unintentionally modify ,access, and steal customer data** | **Human risks** | | **Low** | **High** | **The major effect of internal unauthorized access to the reservation system could lead to exploit user data confidentially and integrity. Since internal staffs usually have more ability compared to outsiders. $100 - 500 million per-night** | **Internal staff accidently or intentionally unauthorized adding, modifying or deleting user records, data modify and stealing** | **1.Using logging software keep tracking insiders activities on the reservation system. 2.To performing an modifying to the reservation system database, using separation of duties. To sure at least one person two people perform one task. 3. Strictly follow least privilege principle on each job function. For example, hotel front desk staff only can reserve, modify and delete reservation but he/she can not see stored credit card info. 4. User data backup at off site if the data accidently deleted** | **99%** | **recover** | **Recover from backup** | **Marriott Inc** | **Future** | **2/5** |
| **3** | **DDOS attack** | | **Reservation system availability** | | **Hacker launch DDOS attack by using botnet** | **Cyber terrorism** | | **high** | **high** | **The major effect of DDOS could lead to long downtime of the reservation system. Could lead to hundreds millions dollar lost per day** | **Botnet sending massive requests** | **Risk transfer. Use Security as a service company take these DDOS request and allow legit user into the reservation system.** | **100%** | **recover** | **Outsource the traffic to third party companies and have a SLA with them** | **Marriott Inc** | **Future** | **5/5** |
| **4** | **Earthquake, flood, tornado or other extreme weather condition** | | **Reservation system physical servers** | | **Extreme Weather or unexpected nature disaster could destroy the servers** | **Nature events** | | **Low (It depends on which location your server based on, usually a place where weather tends to stable is preferred )** | **High** | **Cost of downtime from destroyed servers are high and hard to recover. Usually involves to hundreds million dollar losing per day** | **Nature disaster** | **Risk mitigation. Such as build hot site or warm site allows immediate recover from the disaster** | **90%** | **recover** | **Building the redundant the backup site for immediate recover from the disaster, however it may require a high budget to run a hot site** | **Marriott Inc** | **Future** | **1/5** |
| **5** | **Physical attacking from human to the server room which serves up reservation system** | | **Reservation system physical servers** | | **Malicious people will get into the server room at after hour to steal , destroy, or harm data and servers** | **Terrorism** | | **Low, depends on the area you are at.** | **high** | **Cost of downtime could leads to hundreds million dollar lose and reputation lose** | **Malicious intent or terrorists** | **Using multiple badge systems and gate for entering server room. Supervising by security guard when entering into server room , also build back up site** | **95%** | **recover** | **Build a redundant backup site , preferring hot site [[4]](#footnote-4)** | **Marriott Inc** | **Future** | **1/5** |
| **6** | **Zero-day attack to the reservation system software, exploit coding logic vulnerability** | | **The software runs the reservation system** | | **Hackers take advantage the vulnerabilities founded in the code and exploit them** | **technological risk** | | **High** | **High** | **These could allow hacker get into the system and persist in there for years. Could leads to billions lose** | **Hacker exploit code vulnerability** | **Hire pen-tester actively test the reservation system and found vulnerability and fix it** | **90%** | **Eradicate** | **Hire forensic firm comes in found what damaged already be down and eradicate them** | **Marriott Inc and its customer** | **active** | **3/5** |
|  |  | |  | |  |  | |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  | |  |  | |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  | |  |  | |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  | |  |  | |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  | |  |  | |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  | |  |  | |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  | |  |  | |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  | |  |  | |  |  |  |  |  |  |  |  |  |  |  |

Likelihood vs Impact Ranking: Rank each out of 5 with the output on the table (example: 5/5 = High Likelihood, High Impact)

# References

1. Gibson S. “Security Now Episode #705”, *Gibson Research Cop.* Accessed at June 1 2019. <https://www.grc.com/sn/sn-705.pdf>

2. “AIR Estimates Marriott Cyber Breach Direct Losses Could Reach $600 Million”, *Insurance Journal*, Dec 2018. <https://www.insurancejournal.com/news/national/2018/12/21/512741.htm>

3. “Marriott Breach – Learn From One of the Largest Breaches in History”, *IT Chapter,* <https://itchapter.com/wp-content/uploads/2019/01/Marriott-Breach-From-Info-Tech-Research-Group-Courtesy-of-IT-Chapter-2019-01-04.pdf>

4. Bhaktavatsalam S., Clark P., “Marriott Hit by Starwood Hack That Ranks Among Biggest Ever”, *Bloomberg,* <https://www.bloomberg.com/news/articles/2018-11-30/marriott-found-unauthorized-starwood-database-access-since-2014-jp3xbq64>

1. “AIR Estimates Marriott Cyber Breach Direct Losses Could Reach $600 Million”, *Insurance Journal*, Dec 2018. <https://www.insurancejournal.com/news/national/2018/12/21/512741.htm> [↑](#footnote-ref-1)
2. Bhaktavatsalam S., Clark P., “Marriott Hit by Starwood Hack That Ranks Among Biggest Ever”, *Bloomberg,* <https://www.bloomberg.com/news/articles/2018-11-30/marriott-found-unauthorized-starwood-database-access-since-2014-jp3xbq64> [↑](#footnote-ref-2)
3. Gibson S. “Security Now Episode #705”, *Gibson Research Cop.* Accessed at June 1 2019. <https://www.grc.com/sn/sn-705.pdf> [↑](#footnote-ref-3)
4. “Marriott Breach – Learn From One of the Largest Breaches in History”, IT Chapter, <https://itchapter.com/wp-content/uploads/2019/01/Marriott-Breach-From-Info-Tech-Research-Group-Courtesy-of-IT-Chapter-2019-01-04.pdf> [↑](#footnote-ref-4)