**Arghadeep Lahiri  
Security Fundamentals**

**Executive Summary:**With big data, comes big responsibilities to companies for safeguarding customer data and protect them to avoid data violation regulation and legal implications. One such industry which often gets affected by frequent cyber-attack is Holiday and Tourism industry, as they are predominantly reliant on digital platforms for online booking and customer data retention, making this sector a prime target for cybersecurity attack. High volume of customer data and financial information makes it a lucrative attack source for hackers, leading to ransomware attack, financial disruption and unethical use of customer information.  
**1. Air India   
2. MGM Resorts and Caesar Entertainment**

**Question 1:  
Company name: Air India - Data breach in the early 2021:**  
 **What the incident was about:**  
Airline industries are always at the verge of supply chain attacks by the notorious group from China, named APT41 and one such incident occurred with Air India in February 2021. The announcement was made public in May 2021 as an effect of attack on SITA. But the actual attack was planted in December 2020(Team, 2021).The incident was orchestrated to use vulnerabilities in SITA’s framework and exploit them to gain root access to Airline’s databases (Team, 2021).  
***N.B****:* ***SITA*** *stands for Société Internationale de Télécommunications Aéronautiques is a global IT and telecommunications solutions for airline industries.(* www.sita.aero, n.d.)

**The data compromise:**  
As per reports from research paper from **ebsco.com**(Ebsco.com, 2025) and **securing.io***(*Team, 2021*)*, approximately 10 years(August 11,2011 – February 3, 2021) data of 4.5 million users data was exfiltrated and leaked to dark web, by the Chinese State sponsored threat actor group APT,APT41.  
It is believed Name of passengers, Contact details (email addresses, phone numbers), Passport and ticket information, Frequent Flyers data(Star Alliance and Air India loyalty program details), Credit Card details(but CVV data was not stored), were exposed to the dark web (TechCrunch, n.d.)

**Impact/Consequences of the data breach:**  
The data breach, puts a grave question on Air India’s customer trust. It is also brought to light that this incident had an adverse effect on **Identity Theft**, **Phising Scams** and possible **Financial Frauds** using the stolen credit card details (CNBCTV18, 2021).Additionally, it also damaged the reputation of Air India’s customer data security practices.

**The Attack Vector:**It is known that a series of supply chain attacks is common for airline industries as 90% of the industry use SITA and it has certain vulnerabilities that can be exploited easily. The Chinese threat actor APT41 is out in the wild since 2012 October and are popularly known as Bronze Atlas, Red Kelpie, Wicked Panda, Blackfly, Winnti, or Barium (www.secureworks.comhttp, n.d.). According to APT’s research, the cobalt strike payload was planted in the systems in December 2020, by using a Cobal Strike beacon(Cobalt Strike Research and Development, n.d.) to compromise the network and spreading the payload across the network in 24 hours, and in February 2021, the beacons started communicating with the hacker’s Command and Control centre, after gaining substantial user credentials, providing them continuous access to Air India’s network. 20 devices were compromised, and one device was used to communicate back the C2C server.

According to researcher Rostovcev(CNBCTV18, 2021), this campaign was codenamed “ColunmTK”, where, after securing a successful connection to APT41’s C2C server, **NTLM hashes** and **plaintext passwords** from the local machines were dumped using [**Mimikatz**](https://medium.com/@redfanatic7/detailed-mimikatz-guide-87176fd526c0) and [**Hashdump**](https://www.utc.edu/sites/default/files/2021-04/4660-lab6.pdf) password cracking tools, following privilege escalation using [BadPotato](https://github.com/BeichenDream/BadPotato) Malware.

Few **IoC’s** that were significant in the attack are listed below (Team, 2021):

|  |  |
| --- | --- |
| 20aebf6e20c46b6bfe44f2828adf3b91  b6b06a95cfeeeeOefe8bc0cd54eac71d  83249cff833182b3299cbd4aac539c9a  143278845a3f5276a1dd5860e7488313  559b7150d936fffe 728092b160c14d28  9337952aa3beOdacfc12898df3180f02  212784cf25fOadfaf9ba46db41c373d5  d414c7ede5a9d6d30e6d3fe547e27484  83e6da9cd8ccf9b0c04f00416b091076 | 7b501402c843034cd79151257aca189e  69f5c5f67850acdb373ddd106adce48c  b071a62d2dd745743c6de5f115d633b1  019122b1d783646f99c73a3c399cc334  f61dbac694d34c96830f184658610261  fc208a4d04c085edcealec5f402057f9  5528bb928e02926179fca52dd388b1f0  b8ecab09b7bfb42b9ace3666edf867a7  c4be6b466807540a22f62ffa6829540f  a00ab8ac0f11c3fcd5c557729afcbf89 |

Using this website one can verify threat score of the above hashes [ioc.locker - Threat Intelligence Toolkit](https://ioc.locker/threats)

Below is a diagram explaining the MITRE ATT&CK Framework of the attack:

A red and white rectangular box

AI-generated content may be incorrect.**(** Team, 2021)

**Detailed timeline Diagram**

**A blue and purple timeline with text

AI-generated content may be incorrect.**

Source: (The Hacker News, no date)

**Company name: MGM Resorts and Caesar Entertainment – Data Breach In September 2023**In September 2023, **MGM Resorts**, one of the largest casino and hospitality operators worldwide, suffered a significant cyberattack that crippled its operations for nearly two weeks (Gomez, 2023). As hotel companies rely heavily upon the internet and a number of digitized technologies for booking, customer support, and marketing, they remain incredibly vulnerable to cyberattacks(Bischoff, Garlington and Erdem, 2025).

**What the incident was about:**Scattered Spider group A.K.A Muddled Libra used Multifactor Authentication Fatigue Attacks (numerous authentication requests) to gain access to MGM Resort network (Ebsco.com, 2025), exfiltrating customer data (Name, Driving License details, Date of Birth, Contact information). This group targeted ignorant employees, harvesting their credentials followed by sending MFA prompts to several people, until one of them mistakenly approves the request. Once access to their systems is gained, various parts of customer infrastructure were disrupted. “This group is primarily formed by operatives from United States and United Kingdom, and they demand ransoms in tens of millions of dollars, obviously in cryptocurrency wallet.” (Russo et al., 2024) and in this case demand for ransom went to $30 Million dollar which was paid by Caesar’s International on a simultaneous hack (Sanchez, 2025b)  
  
**The data compromise:**Confidential data (Customer name, Employer details, Credit Card details, Driving License details) were obtained by the attackers. It additionally rendered the MGM app, booking app, room keys and casino slots unfunctional and customers were unable to use any facilities in the hotel for a wider timeframe, putting MGM’s trust and reputation at stake (Sanchez, 2025).

**Impact of the data breach/ Consequences:**The Cyber incident disrupted operation ability to book rooms and services for guests. Additionally, the casino machines became inoperable, incurring a huge financial loss to the industry amounting to $100 million in the in-3rd Quarter 2023. Investigative bodies - Forensic Bureau of Investigation alongside, Nevada Gaming Control Board was involved ensuring MGM’s compliance with the mandatory Cyber incident laws. Apart from face loss, several plaintiffs filed action class suits claiming MGM’s security measures were inadequate. While some are settled confidentially, in 2025 still few cases remain active (Sanchez, 2025b). It also incurred additional capital investment, towards their cybersecurity wellbeing (Endpoint Security, Cloud Security and Employee training). News media stipulated that MGM’s losses during this period amounted to between $4.2 and $8.4 million per day (ISS Insights, 2023). MGM’s stock (NYSE:MGMNYSE: MGMNYSE:MGM) saw an immediate reaction when news of the hack broke. Shares dropped about 4.1% in two trading days, closing at $41.99 on September 12, 2023, down from $43.79 on September 8(Sanchez, 2025b)

**The Attack Vector:**It is believed the Scattered Spider group, harvested employee credentials using social engineering attacks, specifically targeting IT helpdesk employees. They used Vishing to impersonate officials into tricking people to reveal credentials thus gaining access to their systems. It is speculative; however it is believed that this group has then used zero day attacks by exploiting unknown vulnerabilities in their system to escalate privilege to further orchestrate a ransomware attack (Ebsco.com, 2025). It is possible the attackers, exploited misconfigured Active Directory (AD) permissions or unpatched software to move laterally across the MGM’s network. After gaining access, **BlackCat** ransomware was deployed which is known to use **RUST** programming language for advanced encryption techniques, encrypting critical file systems and rendering them inaccessible. **ALPHV/BlackCat** uses double extortion technique to exfiltrate data initially before encrypting them (Madnick, 2023). It is not publicly disclosed which vulnerabilities were exploited; however, this kind of attacks generally targets the exposed APIs in cloud environment to deliver the ransomware payload and use AES-256 encryption algorithm to encrypt the data, with the capacity of evading security softwares and sandboxed tools. It likely used Domain generated Algorithms for command and control(C2C) communications (Nicho et al., 2023).

**Detailed timeline Diagram:**A screenshot of a web page

AI-generated content may be incorrect.

Source: (Waltermire, 2023)

**Question 2:**

The CNSS Model also known as the McCumber cube often offers a structured approach in addressing modern Cybersecurity threat by offering the intersection a multi dimension balancing the different aspects of data security.

Selecting the intersections as follows:  
**Air India**

1. **Storage + Confidentiality + Technology**  
   Protecting stored customer data using technology, thus maintaining confidentiality.

In case of Air India, 4.5 million user’s data was breached. Had the company implemented strong encryption measures like AES-256, the leaked information would be still unreadable, without a decryption key. Other suggestion involves usage of Multifactor authentication measures, segmentation of stored data in more secure servers(offline DMZ server)

1. **Transmission + Integrity + Policies**

Maintaining data accuracy, when it is transit, through efficient polices.

In case of Air India attack, the communication between SITA server and Air India was unencrypted. Implementing the use of SSL/TLS for the data transfer, would have avoided data alteration. Securing data transfers by the means of periodic security audits and using recognized licensed third-party tools, would ensure data accuracy is maintained.

1. **Processing + Availability + Human Factors**

Maintaining authorised access to data during processing through human related approaches.

In case of Air India, lack of human awareness while handling emails and other sensitive data is prevalent. Thus, employee training to recognize phishing emails and social engineering attack should be incorporated. Additionally, revoking employee access to sensitive by setting up proper Access Control List is a must add on. Nevertheless, a business disaster recovery plan should be in place to maintain continuity of business after a cyber-attack incident.

1. **Storage + Integrity + Policies**Stringent policies in order to maintain the integrity of data stored at rest.

Attackers, easily accessed and potentially altered customer data, leading to data theft. Implementing regular backups of data and later restoring it after a cybersecurity attack will avoid this situation. Using third party monitoring tools to detect unauthorized data alteration could be effective in detecting and blocking the attempt immediately. Implementing syslog server to keep track of access, system and application logs, is a must add on.

**MGM Resort:**

1. **Confidentiality + Processing + Technology**

Maintaining data confidentiality which it is being processed.

The attackers might have used zero-day vulnerabilities, to exploit the IT systems, gaining unauthorised access to sensitive information. Using data obfuscation technique, thus making the data unreadable while it is being processed, this situation can be averted. Updating and patching important applications necessary for business, will reduce the surface area of attack

1. **Availability + Processing + Human Factors**

This intersection talks about the human centric approach taken to ensure data is available when needed. In this incident, proper human training to recognize phishing email and vishing calls would be key factor to reduce the social engineering attack surface, thus ensure the data under process is not intercepted by third party intruders. Conducting regular drills and training staff on incident response is a key factor.

1. **Integrity + Storage + Technology**

Maintaining the data accuracy, using updated technology, while the data is stored.

In the MGM 2023 attack, the attackers probably targeted their infrastructure, consisting of databases, and critical systems, by escalating privileges, encrypting and locking critical data stored at rest. The security flaws in the systems (missing application and security updates), could have possibly made the systems an easy prey for the attackers, thus patching systems regularly and segmenting the stored data to a separate serve with access control policy is a must.

1. **Availability + Processing + Policies**

This intersection explains maintaining system access while the data is still being processed.

In the MGM 2023 attack, there were reports of system outages and operation failure in casino services, potentially leading to a ransomware dropper. Developing organised and clear guidelines to report and respond to such attack, would ensure, it is nipped in the bud. Implementing incremental backups and load balancing concept would ensure data is available, even if stolen and could be restored easily from a previous version, thus always maintaining almost 100% availability.

**Questions 3:**Key Security Roles that must exist in this industry sector to avoid further cyberattacks and data breaches:

**Air India**

1. **Chief Information Security Officer(CISO):**  
   Heading the overall cybersecurity infrastructure and manage key security roles to develop policies complying with data regulatory bodies like GPDR, Indian IT Act. Administer Incident Response and Data Recovery process.
2. **Data Protection Officer(DPO):**  
   Act as a point of contact for data regulatory bodies and customers and exercise strict data regulation policies.
3. **Security Operations Center team (SOC):**  
   Conduct regular vulnerability assessments. Use a third-party Security Information and Event Management tool for threat discovery and remediation. Analyze and respond to threat events promptly.
4. **Network Security Engineer:**  
   Deploy and monitor security tools like Intrusions Detection System (IDS), Intrusion Prevention System (IPS).Monitor network for unknown network traffic from outside the organization. Secure the communication channels using encryptions or VPN.

**MGM Resorts**

1. **Chief Information Security Officer(CISO):**  
   Head the CyberSecurity infrastructure of MGM and identify key roles and responsibilities. Ensure company is complying with regulatory bodies (**HIPAA, PCI-DSS**)
2. **Threat Analyst:**   
   Day to day assessment on new threat landscape in the hospitality industry. If new zero day suspect is identified report to the SOC team with analysis.
3. **Security Operations Center team(SOC)**:  
   Oversee MGM’s infrastructure to identify any intruder alert. Act immediately to stop an incident and assist Incident Response team to mitigate the risks. Perform Forensic analysis of any suspected cyber threat event.
4. **Governance, Risk and Compliance Manager(GRC)**:  
   Ensure MGM complies with data regulations related to CyberSecurity.Perform Risk Management, on regular interval, to ensure Confidentiality, Integrity and Availability.

**References:**

1. Google Books. (2023). *Cybersecurity for Decision Makers*. [online] Available at: https://books.google.ie/books?hl=en&lr=&id=bKIIEQAAQBAJ&oi=fnd&pg=PA71&ots=XzVV1p-Nik&sig=qzgAm3QrjYQBY3MDxfHKvKj8qRQ&redir\_esc=y#v=onepage&q&f=false [Accessed 21 Feb. 2025].
2. ‌ Air India (2024). *About Us | Global Airline. Indian Heart | Air India*. [online] www.airindia.com. Available at: https://www.airindia.com/in/en/about-us.html.
3. ‌ Team, S. (2021). *Back-to-Back Air India Attacks Indicating More than Just a Data Breach? - Securin*. [online] Securin -. Available at: https://www.securin.io/articles/back-to-back-air-india-attacks-indicating-more-than-just-a-data-breach/?\_gl=1.
4. ‌ *www.sita.aero. (n.d.). About us. [online] Available at: https://www.sita.aero/about-us/.*
5. *‌* *Ebsco.com. (2025). NCI Single Sign On. [online] Available at: https://research.ebsco.com/c/x47ol5/viewer/html/t32hi3xvcn [Accessed 19 Feb. 2025].*
6. *‌* *TechCrunch. (n.d.). Air India passenger data breach reveals SITA hack worse than first thought. [online] Available at: https://techcrunch.com/2021/05/23/air-india-passenger-data-breach-reveals-sita-hack-worse-than-first-thought/.*
7. *‌* *CNBCTV18. (2021). China backed APT41 behind SITA and Air India cyber attacks. [online] Available at: https://www.cnbctv18.com/aviation/china-backed-apt41-behind-sita-and-air-india-cyber-attacks-9634641.htm.*
8. *‌* *www.secureworks.comhttp. (n.d.). BRONZE ATLAS | Secureworks. [online] Available at: https://www.secureworks.com/research/threat-profiles/bronze-atlas.*
9. *‌* *Cobalt Strike Research and Development. (n.d.). home. [online] Available at: https://www.cobaltstrike.com/.*
10. *‌* *Cyberkid, V.A. (2024). Detailed mimikatz guide - Vasileiadis A. (Cyberkid) - Medium. [online] Medium. Available at: https://medium.com/@redfanatic7/detailed-mimikatz-guide-87176fd526c0 [Accessed 21 Feb. 2025].*
11. *‌* *Dumping Windows Password Hashes Using Metasploit. (n.d.). Available at: https://www.utc.edu/sites/default/files/2021-04/4660-lab6.pdf.*
12. *‌* *BeichenDream (2020). GitHub - BeichenDream/BadPotato: Windows 权限提升 BadPotato. [online] GitHub. Available at: https://github.com/BeichenDream/BadPotato [Accessed 21 Feb. 2025].*
13. *‌The Hacker News (no date) Chinese Hackers Believed to be Behind Second Cyberattack on Air India. https://thehackernews.com/2021/06/chinese-hackers-believed-to-be-behind.html.*
14. *Gomez, F. (2023). The 2023 Cyberattack on the MGM Resort Explained. [online] Inszone Insurance. Available at: https://inszoneinsurance.com/blog/cyberattack-mgm-resort-explained.*
15. Bischoff, J., Garlington, J., & Erdem, M. (2025). What happens in Vegas no longer stays in Vegas—Cybersecurity attacks on Las Vegas integrated resorts. Journal of Hospitality & Tourism Cases. https://doi.org/10.1177/21649987251314898
16. *Ebsco.com. (2025). NCI Single Sign On. [online] Available at: https://research.ebsco.com/c/x47ol5/viewer/pdf/cdq2j5jpjz?auth-callid=61d77c22-5fb4-9e16-addc-89f5eef231c5 [Accessed 21 Feb. 2025].*
17. *Russo, K., Dever, A., & Elsad, A. (2024b, March 8). Threat Group Assessment: Muddled Libra (Updated). Unit 42. https://unit42.paloaltonetworks.com/muddled-libra/*
18. *Sanchez, D. (2025a, January 13). Business Insurance | Personal Insurance | Inszone Insurance. Inszone Insurance. https://inszoneinsurance.com/blog/cyberattack-mgm-resort-explained*
19. *Madnick, S. E., Ph. D. (2023). The continued threat to personal data: key factors behind the 2023 increase (By Apple). https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf*
20. *Nicho, M., Yadav, R., & Singh, D. (2023). Analyzing WhisperGate and BlackCat Malware: Methodology and Threat Perspective. International Journal of Advanced Computer Science and Applications, 14(4).* [*https://doi.org/10.14569/ijacsa.2023.0140456*](https://doi.org/10.14569/ijacsa.2023.0140456)
21. *Waltermire, B. (2023b, September 15). MGM Resorts Cyberattack: A detailed timeline and the role of cyber insurance. https://www.linkedin.com/pulse/mgm-resorts-cyberattack-detailed-timeline-role-cyber-brian-waltermire/*