2021

Air India Data Breach

REVIEW AND RECOMMENDATIONS

SUMAN KAR

Banbreach

B 251 Lake Gardens | Kolkata 700045
email us : contact@banbreach.com

www.banbreach.com

Experience

1. I am Suman Kar. I am the founder of Banbreach. My business address is B251 Lake Gardens Kolkata 700045. Banbreach is a firm providing network security products, cybersecurity consulting, and training. I have expertise in cybersecurity consulting, digital forensics and incident response, and network security. I have been involved in numerous responsible disclosures that have prevented large-scale data breaches from happening. Some of the organizations I have helped are Medantex (healthcare), California Department of Insurance (insurance), Ports America (shipping), IIM Bangalore (education), ITC Hotels (hospitality), Bharat Diamond Bourse (gems & jewelry), etc. I collaborate with CDC, Jadavpur University, on a MEITY-funded, security assurance and compliance framework development project.

Assignment

2. I have been requested by Internet Freedom Foundation to review and evaluate the Air India data breach incident and subsequent actions taken by the organization and provide concrete recommendations for the organization, as well as regulatory authorities.

Summary of Opinions

3. The Air India data breach poses significant risks to the life and liberty of millions of passengers across the globe. This is a national security issue considering members of India’s judiciary, legislative, and executive are more likely to use Air India than other airlines. In addition, exposure to multiple data privacy regimes increases risks of financial penalties that will be ultimately borne by the Indian taxpayers. Resident, ordinary taxpaying Indian customers of Air India affected by the breach therefore are doubly impacted. I provide broad recommendations in the sections that follow.

Definition

4. Air India has global operations. A working definition of the term “data breach” must be able to accommodate the needs of different data privacy regimes such as CCPA, GDPR, APPI, etc. that Air India may have to comply with. The GDPR provides one such definition:

   > A data breach occurs when the data for which your company/organization is responsible suffers a security incident resulting in a breach of confidentiality, availability or integrity [1].

5. Air India also provides an overview of their IT practices:

   > The Company has an extensive system of internal controls which ensures optimal utilization and protection of resources, IT security, accurate reporting of financial transactions and compliance with applicable laws and regulations as also internal policies and procedures. The internal control system is supplemented by extensive internal audits, regular reviews by management and well documented policies and guidelines to ensure reliability of financial and other records to prepare financial statements and other data [2].

Scale

6. SITA’s 2018 Air Transport Cybersecurity Insights report highlighted that executive and board-level buy-in, and a focus on external threats were must to counter the rising risks of cyberattacks. **Recommendation: Air India should publish actions they have taken based on this (and possibly other) industry research reports.**

7. In 2018, Cathay Pacific, British Airways, Delta Air Lines and Singapore Airlines experienced data breaches involving personal details and payment information of passengers worldwide. **Recommendation: Intra-industry threat intel collaboration, mandated by boards, and overseen by a regulatory agency is vital.**

Scope

8. In 2017, an ethical hacker published vulnerabilities on the e-ticketing platforms of Air India, SpiceJet, and Cleartrip. These vulnerabilities had existed since 2015. **Recommendation: Organizations should not ignore reports by security researchers. Regulators can facilitate setting up a vulnerability disclosure platform, and organizations should pay bug bounties to encourage more researchers to come forward.**

9. In 2018, Air India’s Twitter account were compromised allegedly by Turkish threat actors. These incidents provide attackers an idea of the robustness of controls and are sometimes used as entry-points for larger attacks. **Recommendation: Regulators should pay attention to even minor breaches and publish root-cause analyses.**

10. In 2020, an ethical hacker alerted SpiceJet of a data breach involving 1.2 million customers’ personal information [3]. The researcher reached out to CERT-IN who in turn informed SpiceJet. SpiceJet however did not acknowledge the breach. **Recommendation: CERT-IN should publish a periodic summary of reports received from security researchers. Affected organizations must publish any such breaches irrespective of the perceived damage caused.**

Threat Model

11. There is some consensus in the cybersecurity community that the airlines industry is particularly lucrative for nation-state actors for surveillance of domestic, as well as foreign, persons of interest [4] [5]. **Recommendation: Regulators and industry bodies can collaborate to create playbooks to deal with industry specific threats. Additionally, law enforcement agencies should be roped in to thwart nation-state actors. Transparency in reporting incidents will help build resiliency across the industry.**

12. Air India’s threat profile is significantly different from that of other carriers in India. Air India is the often the first (and sometimes, only) choice for a broad range of VIPs such as judges, PSU executives, politicians, bureaucrats, etc. Personal, financial, and travel data of VIPs are highly sought-after. **Recommendation: Air India should explain the steps taken to address this elevated risk profile. Air India should**

report if they implement CIS controls, opt for certifications such as ISO 27001, and/or a target cybersecurity maturity model level.

13. As organizations become better at plugging security issues, adversaries are increasingly focusing on weakness in supply-chain security. For example, Air India's has 25 code-share agreements, 1 joint venture with STS, Singapore, and various subsidiaries, vendors, partners, etc. **Recommendation: Air India should publish data sharing agreements with other partners in their supply-chain. Air India must highlight any implicit risks that a customer bears through these partners, explicit and implied obligations of partners, reasonableness of precautions, standard of care, and jurisdictional latitude for customers.**

14. In 2010, Air India entered a 10-year agreement with SITA to use their Horizon Passenger Services System in a deal worth $190 million (Rs. 845 crore) at the time [6]. **Recommendation: Air India should disclose findings from pre-deal security due diligence, and mitigation steps taken by SITA, if any. Air India should also explain planned migration plans at the end of the deal period.**

15. In 2018, and 2019, faults in the SITA PSS caused operational disruption and financial losses. In both cases Air India refused to claim compensation from SITA. In 2019, Air India renewed their deal with SITA for another two years [7]. It appears that Air India may be the only major airlines using SITA Horizon PSS at the moment. **Recommendation: Air India must explain their refusal to hold SITA accountable despite repeated failures, and continuing with a system that has not seen market success.**

SITA Breach 2021

16. On March 4, 2021, SITA confirmed an incident they termed "a cyber-attack" that took place on February 24, 2021 involving "certain" passenger data stored on their servers. They also reported taking prompt action to contain the breach and informing "all related organizations" [8]. Affected airlines followed suit in issuing press releases. E.g. Singapore Airlines issued a notice the same day at 9:30PM SGT (GMT+8) on their website [9]. In comparison, Air India's brief, misleadingly titled "Information regarding Passenger Service System" notification came out only on May 19, 2021 [10]. **Recommendation: Data breach notifications must be prompt, and unambiguous. Air India, like their peers, must apologize to their customers for the data breach. Air India must explain the two-week delay as well as the lack of details (that SITA and other affected airlines had already made public) in reporting.**

Post-Breach

17. A successful data breach mitigation starts with communicating with the impacted data subjects and providing them with the means to cope with the impact of the breach, then complying with applicable laws across jurisdictions, and finally, investigating the incident [11]. **Recommendation: Air India must provide financial compensation to all impacted customers. Air India must also explain how and why they decided to follow a process that goes against established norms.**

18. Air India's subsequent breach notification came almost two months later, on May 15, 2021, which raises serious questions [11]. Air India mentions that they were notified of the breach on February 25, 2021 and received a list of affected data subjects on March 25, 2021 and April 5, 2021. **Recommendation: Air India, being possibly the only major airlines using Horizon PSS, needs to explain the efforts they undertook from February 25, 2021 onwards to obtain details about the breach.**

19. Air India's May notification mentions personal data, date of birth, passport information, credit cards data apart from ticketing and loyalty program related data of customers "registered between 26th August 2011 and 3rd February 2021" were compromised. In comparison, SIA reports a much smaller subset of data being breached [9]. **Recommendation: Air India must explain what they mean by registered users, why all users from the past ten years are impacted, and why a richer set of their customers' data was available to the attacker.**

20. On June 7, 2021, Air India issued another notification specifically for Australian customers [12]. This notification contained more details about the breach, and instructions for affected customers. However, this notification mentions that SITA first reported the breach on February 26, 2021. **Recommendation: Air India must explain which date they first received a notification from SITA.**

21. The June notification provides a brief chronology of events which started with billing anomalies experienced by SITA on or around February 8, 2021. SITA advised that their systems were exposed to threat actors from January 20 to February 11, 2021. **Recommendation: Air India must explain why these important details were not released earlier, and to a broader audience. Further, Air India must explain how did data of customers who registered after February 11, 2021 get compromised if the attackers did not have access beyond February 11, 2021 to SITA's systems.**

22. In addition, the June notification reports "the breach involved personal information collected between 26th August 2011 and 20th February 2021." **Recommendation: Air India must explain why the May and June notifications report different last dates of impacted users' registration.**

23. The notification adds that credit card issuers VISA, Mastercard, American Express, Discover/Diners and JCB were impacted. Further, the cardholder's name, credit card number and expiry date. **Recommendation: Air India must provide similar information for non-Australian customers. Air India must provide clarity on whether credit card PIN were part of the compromised data.**

24. The same notification recommends that customers change passwords to their Air India accounts immediately. **Recommendation: Air India must explain why this is necessary, and if other personal information such biometric data (photo) that the website collects** [13] **may have been compromised.**

25. Air India's earliest notification did not comply with the GDPR guidelines of sending out notifications within 72 hours of becoming informed about the breach. If Data Protection Authorities across the world impose penalties on Air India, it will ultimately be borne by the Indian taxpayers. **Recommendation: Air India must explain if there have been compliance failures, and if they foresee any penalties, and what steps they have taken to minimize the financial impact of these failures.**

26. The June notification mentions uncertainty around whether personal information such as gender, and nationality were compromised. **Recommendation: Air India must provide a clear list of such data points including, but not limited to, marital status, visa information, that may be impacted.**

27. None of the three notifications has shed any light on the investigative efforts of Air India. **Recommendation: Air India must explain who is investigating the incident, and progress made in the last three months. Considering the scale of the breach, the Indian regulatory authority can facilitate intel sharing between SITA, Air India, and other impacted airlines, CERTs, and data protection authorities.**

Organizational Impact

28. This breach has significant impact on Air India's security policy considerations. In particular, responsiveness is an area that needs immediate improvement. **Recommendations: Air India should report how their security policies are designed, which stakeholders are involved, and whether the policy is supported by security education, training, and awareness programs.**

29. There is significant reputational damage incurred through a data breach. One way to alleviate this is transparency. **Recommendations: C-level executives must explain the reputational damage they foresee as a fallout from this incident.**

30. Every data breach acts as a signaling mechanism and alters the organization's risk profile. Increased risk attracts more attackers, whereas lowering risk involves instituting organization wider changes in policy, people, and processes. **Recommendations: Air India needs to explain to stakeholders the impact of increased risk on enterprise value.**

31. Governance changes are mandatory to ensure that cyber resilience is implemented as a core strategic goal. **Recommendation: Air India's board needs to institute cybersecurity as a strategic imperative.**

Bibliography

[1] European Commission, " What is a data breach and what do we have to do in case of a data breach?," [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en.

[2] Air India, "MANAGEMENT DISCUSSION & ANALYSIS REPORT," [Online]. Available: https://www.airindia.in/images/pdf/Management-discussion-and-analysis-report.pdf.

[3] M. Singh and Z. Whittaker, "Breach at Indian airline SpiceJet affects 1.2 million passengers," TechCrunch, 01 2020. [Online]. Available: https://techcrunch.com/2020/01/30/spicejet-breach-millions-passengers/?guccounter=1&guce_referrer=aHR0cHM6Ly9nYWRnZXRzLm5kdHYuY29tL2ludGVybmV0L25ld3Mvc3BpY2VqZXQtYnJlYWNoLTEtMi1taWxsaW9uLXBhc3NlbmdlcnMtZGF0YWJhc2UtYnJ1dGUtZm9yY2UtaGFjay1yZXBvcnQtMjE3MjMxN.

[4] S. Hawley, B. Read, C. Brafman-Kittner, N. Fraser, A. Thompson, Y. Rozhansky and S. Yashar, "APT39: An Iranian Cyber Espionage Group Focused on Personal Information," FireEye Threat Research, 29 01 2019. [Online]. Available: https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html.

[5] C. Cimpanu, "A Chinese hacking group is stealing airline passenger details," ZDNet, 20 01 2021. [Online]. Available: https://www.zdnet.com/article/a-chinese-hacking-group-is-stealing-airline-passenger-details/.

[6] H. Correspondent, "Air India in $190-mn deal with SITA," Hindustan Times, 08 04 2010. [Online]. Available: https://www.hindustantimes.com/india/air-india-in-190-mn-deal-with-sita/story-eq7Ux3JKGlk0kJCQ00Z7GN.html.

[7] IANS, "Air India sticks to erring vendor SITA," Business Standard, 19 04 2019. [Online]. Available: https://www.business-standard.com/article/news-ians/air-india-sticks-to-erring-vendor-sita-119043001106_1.html.

[8] SITA, "SITA statement about security incident," 04 03 2021. [Online]. Available: https://www.sita.aero/pressroom/news-releases/sita-statement-about-security-incident/.

[9] Singapore Airlines, "Data incident at SITA affecting some KrisFlyer members," 04 03 2021. [Online]. Available:

https://www.singaporeair.com/en_UK/hr/media-centre/news-alert/?id=kltm93p0.

[10] Air India, "Information regarding Passenger Service System," 19 03 2021. [Online]. Available: https://www.airindia.in/Information-regarding-Passenger-Service-System.htm.

[11] Air India, "Notification to Passengers," 15 05 2021. [Online]. Available: https://www.airindia.in/images/pdf/Data-Breach-Notification.pdf.

[12] Air India, "AIR INDIA NOTIFICATION OF DATA BREACH," 07 06 2021. [Online]. Available: https://www.airindia.in/images/pdf/AIR-INDIA-NOTIFICATION-OF-DATA-BREACH-UPDATE-FOR-AUSTRALIAN-CUSTOMERS.pdf.

[13] Air India, "AIR INDIA CUSTOMER DATA PRIVACY POLICY," 25 05 2018. [Online]. Available: https://www.airindia.in/Images/pdf/Air_India_Customer_Data_Privacy_Policy.pdf.

[14] SITA, "2018 Air Transport Cybersecurity Insights," [Online]. Available: https://www.icao.int/NACC/Documents/Meetings/2018/CSEC/D12b-AirTransportCybersecurityInsights2018-SITA.pdf.