Enhancing air transport confidence in data security management

K. Charernnit*

College of Hospitality Industry Management, Suan Sunandha Rajabhat University, U-Thong Nok Rd., Dusit, 10300 Bangkok, Thailand

Abstract. In the modern landscape of air travel, the confidence of passengers in the security of their data is paramount. This study delves into the intricate realm of data security management within the air transport industry which aims to identify areas of improvement and provide recommendations to strengthen data security management within the air transport industry especially low-cost carriers in Thailand. The findings of this research will provide valuable insights into the current state of data security management in the air transport industry. The findings not only shed light on the current state of confidence but also offer insights into potential avenues for enhancing data security measures. As air travel continues to digitize, understanding managing data security is necessary in order to maintain a robust and reliable air transport industry.

1 Introduction

As the world becomes more interconnected and travel demands continue to rise, air transport operators have embraced innovative technologies to address challenges and seize opportunities in many functional areas, such as storage, inventory control, ordering, customer service, development scheduling, and supplier operations, for instance. In accordance with Dudukalov et al. (2021), Mezinova et al. (2022, 2023) the internet of things helps reduce costs and improve services as well as enhancing the customer experience. Recent players in air transport industry are implementing digital innovation like digital sales control, e-procurement, e-payments, and partnerships respectively. However, the advancement of digital service especially mobile devices and their usage have increased the transaction in air transportation industry accordingly, but it also increased tremendously threats on mobile application security and have become a challenge for both passengers and airline operators respectively.

According to Ushakov et al. (2022), the use of emerging technologies, such as artificial intelligence (AI) and the Internet of Things (IoT), in the air transport industry also introduces new cyber-security challenges. While these technologies offer immense potential in improving efficiency and enhancing passenger experience, they also create additional entry points for cyber-attacks. Furthermore, Lohse et al. (2000), in numerous studies analyzing data security management, it has consistently been found that the primary...
reasons customers choose to discontinue their engagement with online businesses are related to privacy concerns and a lack of confidence in their information security as well as trustworthiness.

As Low-cost carriers' (LCCs) have recently shown strong market performance, their high efficiency was measured in terms of passenger load factor, competitive cost reduction, and organizational structure. Since 2017, low-cost carriers have made up nearly a third of the world's air travel market.

Additionally, Salas (2022), it has been projected that from 2020 to 2027 that the global low-cost carriers’ market will be worth more than 254.1 billion US dollars. This steady market value development is mostly due to two important factors as the rising in air passenger traffic amount and low-cost airlines' attempts to improve their efficiency respectively as shown in Figure 1.

Therefore, researcher is interested in investigating approaches to enhance data security management in low-cost airlines and this study will have wider implications for air transport business organizations as a whole, as it will shed light on ways to enhance the adoption of digital services. The study also explores passengers' awareness, concerns, and attitudes towards data privacy. Furthermore, this research will make a substantial impact on the local business community, particularly within an air transport industry in Thailand.

Fig. 1. The Global low-cost carrier market size forecasting from 2020 – 2027 (Source: Adapted from Projected size of the low-cost carrier market worldwide from 2020 to 2027, Salas, 2022).

2 Research Objectives

The objective of this study is to identify areas of improvement and provide recommendations to strengthen data security management within the air transport industry: a case study of low-cost carriers in Thailand.
To achieve the objectives of this study, a comprehensive review of existing literature on data security management in air transport sector will be conducted. This review will examine various frameworks, standards, and best practices that have been implemented to protect passenger data in air transport industry.

3 Research Methodology

The approach of this study aims to identify areas of improvement and provide recommendations to strengthen data security management within the air transport industry especially low-cost carriers in Thailand.

With the goal of examining the confidence of data security management, the present study constructs from various sources. Therefore, this study employing a qualitative interview that will not focus on the individual low-cost carriers in Thailand, but the general picture of low-cost carriers’ data management according to the literature review and a comprehensive analysis of factors such as technological advancements, regulatory frameworks, and communication strategies.

4 Literature Review

4.1 Dealing With Digital Technology & Service Delivery

According to Chevrin et al. (2005), Scupola (2008b), digital-services refer to the services that are generated, offered, and utilized through electronic networks such as the Internet, applications, wireless connections, and mobile devices. This trend highlights the increasing importance of digital platforms and technology in facilitating various transactions and interactions between businesses and consumers. In the globalized world of business, digital-services play a crucial role in effectively managing and nurturing consumer relationships. Furthermore, Hoffman (2003) and Stafford (2003), also provided similar interpretations of e-services that it is an online features and capabilities that are made available to customers for a fee, with the ultimate goal of assisting individuals in problem-solving and fulfilling their requirements. Therefore, in the realm of information technology, e-services refer to the delivery of software functionality between machines, without the need for human involvement. This concept can be seen as an expansion of e-Commerce, according to Stafford's marketing perspective, while technology specialists perceive e-services as online capabilities that can be accessed through the internet.

While Douglas et al. (2003), dividing e-services (electronic-service) into two distinct types: hard and soft e-services, hard e-services focus on delivering goods and services to customers, placing emphasis on timely delivery and response time. On the other hand, soft e-services revolve around website design, data information readiness, and transactions. In the realm of soft e-services, particular attention is given to web content, security, accessibility, and reliability. In conventional practices, Worasuwannarak (2023) the process of producing, providing, or consuming a service typically involves direct interaction between the service provider and the user. This interaction has predominantly been carried out through personal encounters, often in a face-to-face manner. However, with the emergence of e-services, the dynamics of service production, provision, and consumption have shifted to the realm of the Internet and mobile networks.

As pointed out by Hoffman (2003), service marketers who transition from traditional approaches to e-services encounter fewer hurdles and discover a greater potential for generating revenue in this new paradigm. In a study conducted by Hofacker et al. (2007), it was found that there are three distinct categories or prototypes of e-services. These
prototypes include e-services that act as complements to traditional offline services and goods, such as online seat reservations provided by airlines. Additionally, there are e-services that serve as substitutes for existing offline services, like e-newspapers or online auctions. Lastly, there are e-services that stand as unique and entirely new core e-services, such as online computer games or search engines.

In addition, Scupola (2008b) classified characteristic of e-services to four primary features that Firstly, e-services are accessible through the Internet or mobile networks. Secondly, these services can take various forms such as applications, computing resources, services, processes, or information. Thirdly, e-services are utilized by individuals, applications, and businesses alike. Lastly, it is important to note that while some e-services may be offered for free by the government, there are also instances where customers are required to pay a fee to the service provider in order to access and utilize the e-services. There are several well-known applications of e-services that most people are familiar with, including online banking, online retailing (such as amazon.com), online auctions (such as e-bay.com), and online travel booking (such as traveloka.com). In addition to these commonly known e-services, there are also other types available. For example, e-government services offer online access to tax information, while e-Learning provides courses that can be taken online. E-libraries allow users to electronically access journal articles or specific sections of books. Lastly, e-health services offer medical advice and information online (Yee, 2006).

However, Charernnit (2020), studied passenger’s satisfaction levels at the Suvarnabhumi Airport, Thailand, and found out that most passengers rated internet and wireless connectivity service as the highest priority, followed by the efficiency of immigration and airport authority workers and their convenience of connecting to the next airliner. On the other hand, passengers had the lowest degree of satisfaction for the attribute of self-check-in counter because this function does not show how to operate in many languages, causing passengers to consider this service as low level and dissatisfied with the technology.

The majority of passengers still require the assistance of an airline staff member to ask and demonstrate how to utilize the self-check-in service station, which related to Culnan & Armstrong (1999), that the reasons behind privacy concerns or the reluctance to share personal information can be attributed to the presence of intimidating attitudes embedded within specific online transactions. The adoption of digital-services by customers is influenced by various factors, including effort expectancy, social influence, facilitating conditions, outcome expectancy, privacy concerns, trustworthiness, and motivation.

4.2 Data Security Management

Kagalwalla & Churi (2019) emphasized the heightened difficulties associated with ensuring cyber-security in the aviation industry, which have arisen due to the widespread adoption of advanced information and communication technology (ICT) systems such as the Internet of Things (IoT), machine learning, and cloud storage and computing. These emerging technologies, while offering numerous benefits, also come with inherent vulnerabilities that pose significant risks to the security of aviation systems.

According to Lehto (2020), the current trend in cyber-attacks affecting airlines, aircraft manufacturers, and authorities can be attributed to a combination of factors. These factors include the continuous development and evolution of cyber-attack tools and techniques, the growing number of vulnerabilities and exposures in the aviation industry, and the motivation and intent of the attackers themselves. As advancements in technology provide attackers with more sophisticated means to carry out their malicious activities, the aviation sector becomes increasingly susceptible to cyber threats. This poses significant challenges
for airlines, aircraft manufacturers, and authorities as they strive to protect their systems, data, and operations from potential breaches and disruptions caused by cyber-attacks. Consequently, it is necessary for these entities to remain vigilant, proactive, and adaptive in their cybersecurity measures in order to mitigate the risks posed by this ongoing and evolving threat landscape.

According to Monteagudo (2020), the increase in cyber-security threats can be attributed to various factors such as the ongoing digital transformation, greater levels of interconnectedness, segmentation, and complexity. These trends have been further fueled by the recent advancements in the travel industry, which have led to a surge in global connectivity. In essence, Monteagudo, J. (2020) stated that the key findings indicate that the heavy reliance on IT systems for maintaining service quality has made organizations more susceptible to cyber-attacks.

Additionally, the presence of multiple entry and exit points within the industry has created new vulnerabilities that can be exploited by malicious actors. Moreover, the existence of legacy IT systems and the fragmentation of technology further complicate the situation, as these older systems were not originally designed to withstand the threats posed by cyber-crime. In order to address these challenges and enhance cybersecurity, it is imperative for organizations to foster a strong security culture. This entails creating an environment where security is valued and prioritized by all employees. Furthermore, implementing preventive measures and taking proactive steps can prove to be effective solutions. By staying ahead of potential threats and vulnerabilities, organizations can mitigate risks and safeguard their systems and sensitive information.

5 Research Results & Conclusions

Cyber-attacks and vulnerabilities within the air transport sector over the past two decades is terrifying. A notable target within the aviation industry is its Information Technology (IT) infrastructure, with the primary type of attack being malicious hacking aimed at unauthorized access. Defining and implementing proactive measures to safeguard critical aviation infrastructures against cyber incidents is crucial for maintaining customer confidence in a vital service-oriented industry. Enhance understanding of existing and potential future data security management for the air transport industry is essential.

According to Ukwandu (2022), most significant threats arise to steal intellectual property, intelligence and gather information about other sovereign nations' capabilities. The categorization of threats against digital infrastructures and applications within smart airports was conducted by Lykou et al. (2018), these threats can be classified into three main categories as network and communication attacks, malicious software, and tampering with airport smart devices. Additionally, from the literature review, the results appeared that potential harmful attack circumstances, including those involving phishing, social engineering, and abuse of authorization aimed particularly at smart applications. Consequently, Kagalwalla & Churi (2019), a lack of resources, money, and skilled workforce have been identified as an internal threat.

According to Culnan & Armstrong (1999), customers' adoption of digital services is influenced by a variety of elements such as effort expectation, social influence, facilitating conditions, outcome expectation, privacy concerns, trustworthiness, and motivation. These antecedent factors play a significant role in determining whether customers will accept and utilize digital-services. Having a deeper comprehension of the various factors that determine confidence of data security management within the airline industry can offer valuable insights and recommendations for airlines to effectively implement digital services for their customers.
In conclusion, the adoption and use of data security management have become imperative in today's digital landscape. Both individuals and organizations must prioritize the protection of sensitive information to mitigate the risks of unauthorized access, data breaches, and cyber-attacks.

By implementing robust security measures, fostering a culture of accountability, and staying informed about emerging threats, individuals and organizations can safeguard their data and maintain the trust and confidence of their stakeholders.

Therefore, data security management in air transport operators must involve the practices and measures that should put in place to protect sensitive information from unauthorized access, alteration, or destruction. Air transport operators should implement a wide range of strategies, including encryption, access controls, firewalls, and regular system updates regularly. These measures must be designed to ensure the confidentiality, integrity, and availability of data, safeguarding it from potential threats.

6 Recommendation

For organizations, data security management is paramount to protect their operations, reputation, and the trust of their stakeholders. In an era where data breaches and cyber-attacks can have devastating consequences, organizations must take proactive measures to ensure the security of their data. This involves implementing robust security protocols, conducting regular vulnerability assessments, training employees on best practices, and establishing incident response plans to mitigate potential risks. The adoption and implementation of data security management also require a shift in mindset and organizational culture. It is not enough to simply have the technologies and strategies in place; individuals and organizations must prioritize and make data security a fundamental part of their daily operations.

This involves creating a culture of awareness and accountability, where everyone understands the importance of data security and takes responsibility for their actions. In today's technologically advanced world, the adoption and use of data security management has become increasingly crucial for individuals and organizations alike.

As the reliance on digital platforms and data storage systems continues to grow, the risk of unauthorized access, data breaches, and cyber-attacks has become a persistent concern. Individuals are now more reliant than ever on digital platforms and services for various aspects of their lives, including banking, healthcare, communication, and entertainment. With the increasing amount of personal information being shared and stored online, individuals need to prioritize data security management to protect their sensitive data from falling into the wrong hands. This involves implementing strong passwords, enabling two-factor authentication, regularly updating software, and being cautious about sharing personal information online.

Furthermore, as technology continues to evolve, so do the threats and vulnerabilities associated with data security. Individuals and organizations must stay up to date with the latest trends and advancements in cybersecurity to adapt their strategies accordingly. This may involve investing in advanced security technologies, partnering with cybersecurity experts, and participating in ongoing training and education programs.

7 Acknowledgement

Through the collaborative efforts of all teams, the research was completed successfully and the researcher would like to appreciate the help and support from everyone involved in this project, especially, all reviewers that took part along the processes. Moreover, would like to thank Suan Sunandha Rajabhat University, Bangkok, Thailand, for financial support, as well as colleagues in the
College of Hospitality Industry Management, for assistance in many respects, particularly the thoughtful and broader recommendations provided in this research.

References

- College of Hospitality Industry Management, for assistance in many respects, particularly the thoughtful and broader recommendations provided in this research.

- Educational and digital tools as factors of service quality increase in Thailand 4.0 era (the case of Suvarnabhumi Airport, Bangkok) (Last accessed 14.05.2023)

- Some issues for the modelling of interactive e-services from the customer multi-channel interaction perspectives (Last accessed 14.05.2023)

- Industry 4.0 Readiness: The Impact of Digital Transformation on Supply Chain Performance (Last accessed 14.05.2023)

- Towards a research agenda. Journal of Value

- Contributions of Financial Management to the Digital Competitiveness (Last accessed 14.05.2023)

- Big Data for Transport; Springer: Berlin/Heidelberg, Germany, 19

- Proceedings of the 2019 5th International Conference on Computing, Communication, Control And Automation (ICCUBEA), Pune, India, 19

- Control And Automation (ICCUBEA), Pune, India, 19

- Big Data for Transport; Springer: Berlin/Heidelberg, Germany, 19

- Proceedings of the 2019 5th International Conference on Computing, Communication, Control And Automation (ICCUBEA), Pune, India, 19

- Control And Automation (ICCUBEA), Pune, India, 19


