OPEN ACCESS
Computer Science & IT Research Journal
P-ISSN: 2709-0043, E-ISSN: 2709-0051
Volume 3, Issue 3, P.66-73, December 2022
DOI: 10.51594/csitrj.v3i3.426
Fair East Publishers
Journal Homepage: www.fepbl.com/index.php/csitrj

ENSURING CYBER SECURITY IN AIRLINES TO PREVENT DATA BREACH

Leo Tong[1] & Ming Kwan[2]

[1]Director, Capital Delight Inc.,
Hong Kong, China

[2]Associate Director, Capital Delight Inc.,
Hong Kong, China

*Corresponding Author: Leo Tong
Corresponding Author Email: leo.tong@capitaldelight.com
Article Received: 01-12-22 **Accepted:** 16-12-22 **Published:** 25-12-22

ABSTRACT

Using the data breach issues that happened in Cathay Pacific Airways (CX) and British Airways (BA) as case studies, the aim of this study is to focus on analyzing cyber security against data breach that affects airlines passengers' privacy and induces greater financial losses for airlines. The objective is to investigate the possible leakages in airlines' cyber security and explore how to strengthen cyber security in airlines. Based on the results, preventative, detective, and reactive measures were revealed which contribute to strengthening cyber security for the airlines.
Keywords: Cyber Security, Data Breach, Airlines.

INTRODUCTION

Cyber security has become a threatening issue in airlines. According to a survey conducted by PwC's Global Airline CEO Survey (2015), 85 percent of airline CEOs view cyber security as a significant risk, reflecting the sensitive nature of flight systems and passenger data. In this study, we analyze the preventive, detective, and reactive measures and discuss actionable steps that airline executives can take to prepare for the ever changing and challenging cyber threats.

The financial impact alone is staggering. The cost of data breaches globally could reach $2 trillion by 2019 (ND Net, 2019). Another study estimates that 2014 cybercrime losses cost businesses about $400 billion annually (CRN magazine, 2014). Unavoidably, cyber threats have grown in scope, intensity, and complexity. Consider the expanded use of cloud and mobile devices. Mobile devices create more entry points for hackers by dispersing data. The cloud, where data is aggregated, makes data more accessible, and new vulnerabilities have emerged. The situation is getting tougher and more challenging. To mitigate the threats, companies will need to reassess all facets of their business and establish internal protocols to effectively manage them. Furthermore, as businesses aggregate and analyze more data on customers and processes, the data becomes increasingly valuable and a more attractive target for hackers. This double-edged sword applies to technology as well. While improved technology allows businesses to better understand and target their customers, advances in technology also provide hackers with more sophisticated technology with which to perpetrate attacks.

According to our survey, 85 percent of airline CEOs expressed concern about this risk versus 61 percent of CEOs in other industries, a difference of 24 percentage points (PwC, 2015). Airlines are concerned with the theft of sensitive customer or company data. But an added threat for airlines is that technology is being used to improve the connectivity of flight operations systems with ground crews and air traffic systems. While this enhanced communication and integration is essential to the improvement of financial and operational performance (PwC, 2014).

Overall, security procedures to date have been effective, safely integrating the many technological advances introduced to aircraft and airlines. Yet the industry continues to see major technological advances that contribute to the complexity of protecting data and assets. Two of these are tablet-based electronic flight bags (EFBs) and the installation of in-flight entertainment and Wi-Fi connectivity systems (IFEC). EFBs are particularly popular with pilots as they have taken the place of heavy binders that pilots used to carry onboard. However, another survey revealed that many airlines do not have a targeted plan in place to safeguard the security of EFBs (CSCSS, 2015). On-board IFEC systems are proliferating as they are physically segregated from cockpit systems. Nevertheless, these systems increase the number of connections, vendors, and technologies involved, which in turn expose a higher chances of hacking opportunities.

The threats posed by EFBs and IFECs need to be managed holistically, with airlines closely cooperating with other carriers, hardware and software providers, aircraft OEMs, and other industry stakeholders. Another potential cyber issue for the airline industry is the Federal Aviation Administration's (FAA) modernization of air traffic control, notably the Next Generation Air Transportation System or NextGen. The current system is 40 years old and relies on radar, which

provides limited connectivity. NextGen seeks to improve network efficiency by using a global positioning system (GPS) that is software based and connected to the Internet. However, implementing a system with Internet connectivity brings greater threats to security (GCN, 2015).

As real-time aircraft connectivity continues to evolve, providing accurate and safe information were paramount to optimize airline operations and the customer experience (PwC, 2014). It not only increases the number of opportunities for attacks, but it also potentially makes them more damaging. The industry is making significant investments and taking important steps to address cybersecurity, calling for increased oversight from boards of directors as well as third-party providers. The FAA has "convened a private meeting" to examine the security of aircraft systems,8 which at the very least is an acknowledgement of the need for industry-wide approaches and standards. Tony Tyler, the head of the International Air Transport Association, or IATA has stated that regulators must work with airlines to develop a global security system that adopts "an end-to-end risk-based approach" (IATA, 2013).

IATA's position is that the industry can effectively deal with most attacks by focusing efforts on prioritizing and allocating resources to protect the airlines' most valuable assets. Regardless of how a cyber security strategy is formulated, the airline's board must support the strategy and ensure that it is coordinated across all departments in the organization (MRO Network, 2015). A cyber security strategy includes methods to prevent, detect, and react to attacks as well as a mechanism for capturing learnings. Feedback collected at each stage should be incorporated into the overall security program to make attacks more difficult to execute successfully. While prevention methods are not foolproof, an airline's first security goal is to try and stop attacks from occurring, both on the ground and in the air. Once an attack occurs, airlines must detect the attack as quickly as possible and isolate the intrusion. And then airlines must react quickly and efficiently to minimize the damage and reduce the risk of future incidents. As we have seen in many industries, this involves extensive analysis of the potential vulnerabilities across an organization's internal operations, supply chain, and strategic partner network.

Prevention

The first line of defense is to prevent attacks that can corrupt or destroy data and interrupt operations. Key elements of attack prevention that include:

- The critical role of boards of directors
- A proactive approach that includes knowledge of global threats—current and prospective, people and places
- Expanding and formalizing industry standards
- Dealing with risks from supply chain, parts, and third-party vendors

Detection

Even with the best prevention systems, determined hackers will get through. It is essential to detect and isolate these attempts before they spread and do more damage. The key elements of a detection system include:

- Monitoring network and IT systems
- Protecting customer and operational data

• Understanding and dealing with insider threats

Reaction

Since no system is foolproof, airlines must develop a methodology for responding quickly to an attack to limit reputational damage. And they need to use all details of the attack to enhance prevention. A good reaction plan includes:

• Notifying customers and other stakeholders as soon as possible and managing press stories
• Collecting forensic data to identify security weaknesses
• Minimizing damage caused by security breaches
• Closing the loop by using new information to improve prevention methods

Introduction

The setting for the present study was the data breach cases of Cathay Pacific Airways and British Airways that have revealed the weaknesses of cyber security. Different kinds of cyber threats were explored in this research. The objective of this study is to investigate the possible leakages in airline's cyber security and explore how to strengthen cyber security in airlines. CX flags data breach affecting 9.4 million passengers. Personal data includes names of passengers, their nationalities, dates of birth, telephone numbers, email and physical addresses, passport numbers, identity card numbers and historical travel information had been accessed in 2018 (Monnappa, 2018). Another data breach case happened in BA where the credit card details of 380,000 customers were stolen in the most serious attack on its website and app. The disruption caused by the attack was unprecedented in more than 20 years that BA had operated online. BA said the attackers had not broken the airline's encryption but did not explain exactly how they had obtained the customer information (Sandle, 2018). This study urges the importance for all airlines and governments to engage in cyber security and to implement greater preventive and protective measures to cope with potential data breaches.

LITERATURE REVIEW

As airlines website has large volumes of card transactions so it is a target for hackers. Though the increasing use of data and technology brings new cyber threats, cyber-attacks are often viewed in isolation and seen purely in IT terms not linked to operational processes (IATA, 2018a). Thus, cyber security is paramount because airline competitiveness depends on safety and security that must be extended to cyberspace (Magliulo, 2016). Every organization will be hacked, so the management must get ready to plan and implement preventative and protective measures to cope with the cyber threats. A more comprehensive approach should be adopted as cyber-attacks move from preventing the availability of systems to threatening the integrity of data within those systems. Also, risk assessments should be carried out in advance and screening technologies will be more discrete and decentralized, happening at gates or along corridors rather than in a central location (IATA, 2018b).

Table 1
Definitions of Terms

Cyberspace	the complex of all interconnected ICT hardware and software infrastructure which covers internet, data, and mobile devices (Magliulo, 2016).
Cyber threats	related to the malicious conducts that can be exercised in, throughout or against cyberspace. (Magliulo, 2016).
Cybercrime	all malicious activities with a criminal intent carried out in cyberspace, such as internet fraud, identity theft and stealing of data or intellectual property (Magliulo, 2016).
Cyber espionage	under acquisition of data, not necessarily of commercial value (Magliulo, 2016).
Cyber terrorism:	exploitations of system's vulnerability with political aims (Magliulo, 2016).
Cyber warfare:	actions performed with the purpose of achieving a military advantage (Magliulo, 2016).

METHODOLOGY

The author conducted in-depth semi-structured interviews with cyber security experts to fully analyze preventive and protective measures to cope with potential data breach issues in airlines. Research on cyber security contributions has traditionally employed a variety of deductive processes, testing a plethora of hypotheses and pre-determined theories. Cyber security researchers have typically approached the problem from a positive perspective, utilizing quantitative research techniques such as surveys and questionnaires, and processing data with the help of statistical data analysis tools. While mostly deductive in nature, such research tools tend to measure a set of predetermined hypotheses, searching for answers to the "what" questions and not allowing for any additional factors to enter the researcher's process of reasoning (Yin, 1994). Experts in cyber security have been shown to demonstrate a multitude of contributions and it is likely that their expertise, opinions, judgments, and experiences of cyber security issues differ. To gain a degree of context depth, which is not possible to achieve simply by analyzing quantitative data, a qualitative research approach has been chosen as a more appropriate research strategy. Qualitative research is considered to be "concerned with understanding things rather than with measuring them" (Gordon & Langmaid, 1988, p. 2), whereby the "subjectivity and the authenticity of human experience" (Silverman, 2010, p. 138) allows the researcher to gain an insight into the different meanings, perceptions, opinions, expertise of research subjects (Holloway et al., 2010; Veal, 2006). The research has used purposive sampling because of its capacity to obtain useful informative and rich data from respondents who are cyber security experts. The extensive professional knowledge and experiences of these respondents formed a basis for opinions which made their comments valid, reliable, and trustworthy. This prompted the researcher to make a subjective selection of the sampling units to obtain a representative sample of the research population (Sekaran, 2003). In the current study interviewing would be discontinued once 'saturation' was reached. At this point, no further insights would be forthcoming from the interviews (Myers, 2013).

RESULTS

Profile of Respondents

- Assessor of the Hong Kong ICT Awards

- Member of FinTech Committee of the Hong Kong Innovative Technology Development Association (HKITDA),
- Certification Board Member of Hong Kong Institute for IT Professional Certification (HKITPC)
- Member of the FinTech Special Interest Group of HKCS
- Member of Hong Kong Computer Society (HKCS).

Findings

CX and BA were relying on out-of-date defenses. They lack effective Information Security Management Systems (ISMS) to detect and protect staff, customers, transaction processes, technology, and assets. Both internal and external IT security resources failed to combat and prevent the cyber-attack.

Recommendations to Airlines

- To set up effective information security management systems (ISMS) to protect both staff, customers, processes, technology, and assets.
- To review the cyber security preventative and monitoring systems regularly.
- To nurture and strengthen safety and security values to improve cyber resilience and achieve the necessary balance between operational efficiency and high standard and performance of cyber-security.
- To build more collaborative relationships with governments and regulators to update the cyber security issues.
- To communicate with and coordinate between different departments to anticipate cyber-attacks and more effectively mitigate cyber-risks.
- To set clear standards for effective product and procedure designs for ensuring thorough processing procedures such as implementing facial recognition in all cyber security procedures.

Recommendations to Credit Card Companies:

- To alert anyone with unusual activity on his credit cards especially for those online transactions.

Recommendations to Governments:

- To set strict data regulations that companies must inform regulators of a cyber-attack within 48 hours.
- To develop cyber security and data protection guidelines for the private sectors for ensuring cyber security.
- To make sure those international and national cyber threats monitoring instruments are ready.

DISCUSSION AND CONCLUSION

Discussion and Implications

CX and BA were revealed to have the fragile of personal data protection and the causes of cyber threats. The attempted phishing occurred in CX. Phishing is a cybercrime in which a target or targets are contacted by email, telephone, or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. CX was previously believed to be unauthorized access to 9.4 million passengers' personal data was in fact a sustained three-month-long cyber-attack (Bright, 2018). The findings of this study have significant implications for airline management. Based on the results of this research, practical advice is recommended to enhance cyber security in airlines.

Conclusion

The objective of this search is to investigate the possible leakages in the airline's cyber security. Based on the results, insights were revealed which contribute to strengthening cyber security in airlines. The aim of such an episode is to arouse all individuals, business sectors and governments to engage in cyber security and to invest more resources on greater preventive and protective measures in enhancing cyber security in airlines.

Limitation of this Study and Suggestions for Future Study

Like all research, this study has several limitations which the author attributes to the relative weakness of interviews to present valid, reliable, and trustworthy empirical evidence. Consequently, it is recognized that the results of this study present a snapshot of thoughts and opinions from cyber security experts, at a particular point in time. Future research should explore cyber security in other hospitality sectors such as hotels, and online travel agents.

References

Bright, C. (2018, November 13). Cathay Pacific's data breach update, *Business Travelers*. Retrieved from https://www.businesstraveller.com/business-travel/2018/11/13/cathay-pacifics-data-breach-update/

Cobanoglu, C., & Demicco, F. J. (2007). To be secure or not to be: Isn't this the question? A critical look at hotel's network security. *International Journal of Hospitality & Tourism Administration*, *8*(1), 43-59.

CRN Magazine. (2014, June 9). The Total Global Cost Of Cybercrime? $400 Billion A Year And Growing, Retrieved from http://www.crn.com/news/security/300073063/the-total-global-cost-of-cybercrime-400-billion-a-year-and-growing.html

CSCSS, Airlines and Hacking, (2015, August 14). Retrieved from http://cscss.org/CS1/index.php/2015/08/14/216/

GCN (2015, April 27). Cyber risks inherent in NextGen transition, GAO warns, Retrieved from https://gcn.com/articles/2015/04/27/faa-nextgen-cybersecurity.aspx

Gordon, W., & Langmaid, R. (1998). *Qualitative Market Research: A Practitioner's and Buyer's Guide*, Gower, Aldershot.

Holloway, I., Brown, L., & Shipway, R. (2007). Meaning not measurement: using ethnography to bring a deeper understanding to the participant experience of festivals and events, *International Journal of Event and Festival Management, 1*(1),74-85.

IATA (2018, October 1 a). Spreading a cybersecurity culture, Retrieved from https://www.airlines.iata.org/news/spreading-a-cybersecurity-culture

IATA (2018, October 1 b). AVSEC World Day: The future of aviation security. Retrieved from https://www.airlines.iata.org/news/avsec-world-day-the-future-of-aviation-security

Magliulo, A. (2016). Cyber Security and Tourism Competitiveness. *European Journal of Tourism, Hospitality and Recreation, 7*(2), 128-134.

Monnappa, C. (2018, October 24). Cathay Pacific flags data breach affecting 9.4 million passengers, *Reuters*. Retrieved from https://www.reuters.com/article/us-cathay-pacific-cyber/cathay-pacific-flags-data-breach-affecting-9-4-million-passengers-dUSKCN1MY26L

MRO Network, (2015, September 28). *Cyberattacks and the aviation sector: how can airlines best prepare?* Retrieved from http://www.mro-network.com/guest_blog/2015/09/28/cyberattacks-andaviation-sector-how-can-airlines-best-prepare

Myers, M. (2013). *Qualitative Research in Business & Management* (2nd ed.). London: Sage Publications.

Olding, A., & Turner, P. (2007). Cyber vulnerabilities and the tourism industry: developing a conceptual framework. *ACIS 2007 Proceedings*, 116.

PwC. (2015). Global airline CEO survey, Getting clear of the clouds: Will the upward trajectory continue? Retrieved from http://www.pwc.com/us/en/industrial-products/publications/assets/pwc_2015_global_airline_ceo_survey.pdf

PwC. (2014). Tailwinds: 2014 airline industry trends - The connected airline. Retrieved from http://www.pwc.com/us/en/industrial-products/publications/assets/pwc-tailwindsthe-connected-airline.pdf

Sandle, P. (2018, September 7). BA apologizes after 380,000 customers hit in cyber-attack, *Reuters*, Retrieved from https://www.reuters.com/article/us-iag-cybercrime-british-airways/ba-apologizes-after-380000-customers-hit-in-cyber-attack-idUSKCN1LM2P6

Sekaran, U. (2003). *Research methods for business: a skill building approach*. New York: John Wiley & Sons.

Silversman, J.R. (2004). Professional Event Coordination, John Wiley & Sons Inc., New Jersey.

Ugwoke, F. N., Okafor, K. C., & Chijindu, V. C. (2015, November). Security QoS profiling against cyber terrorism in airport network systems. *In 2015 International Conference on Cyberspace*, Abuja, 241-251.

Veal, A.J. (1994). *Research Methods for Leisure and Tourism: A Practical Guide* (3rd Ed.), Pearson Education, Harlow.

Yin, R.K. (1994). *Case Study Research: Design and Methods* (2nd Ed.), Sage, Thousand Oaks, CA.

ZDNet (2015, May 12). Data breaches to cost global economy $2 trillion by 2019, Retrieved from www.zdnet.com/article/data-breaches-to-cost-2-trillion-by-2019/