Data Breach Incident Investigation Report

published under Section 48(2) of
the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong

Cathay Pacific Airways Limited

and

Hong Kong Dragon Airlines Limited

Unauthorised access to personal data of passengers

Report Number：R19 - 15281

Date Issued: 6 June 2019

Cathay Pacific Airways Limited

and

Hong Kong Dragon Airlines Limited

Data Breach Incident

Unauthorised access to personal data of passengers

Section 48(2) of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (**Ordinance**) provides that "*the* [Privacy] *Commissioner* [for Personal Data, Hong Kong] *may, after completing an investigation and if he is of the opinion that it is in the public interest to do so, publish a report -*

(a) setting out -

(i) the result of the investigation;

(ii) any recommendations arising from the investigation that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and

(iii) such other comments arising from the investigation as he thinks fit to make; and

(b) in such manner as he thinks fit."

This investigation report is hereby published in discharge of the powers and duties under section 48(2) of the Ordinance.

Stephen Kai-yi WONG
Privacy Commissioner for Personal Data, Hong Kong
6 June 2019

TABLE OF CONTENTS

Data Breach Incident
Investigation Report

(published under Section 48(2) of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong)

Cathay Pacific Airways Limited
and
Hong Kong Dragon Airlines Limited

Unauthorised access to personal data of passengers

Executive Summary

Background and Investigation

Upon the receipt of a data breach notification (**DBN**) lodged by Cathay Pacific Airways Limited on behalf of itself and Hong Kong Dragon Airlines Limited (collectively referred to as **Cathay**) through their legal representative on 24 October 2018 in relation to its discovery of unauthorised access to personal data of approximately 9.4 million passengers of Cathay, the Privacy Commissioner for Personal Data, Hong Kong (**Commissioner**) carried out an investigation on 5 November 2018. (paras. 1-4)

The Commissioner is mindful of the accuracy and sensitivity, and exercises due care and diligence to ensure that he has the accurate facts on which his investigation and findings are based, and that disclosure of these facts could not be potentially exploited or used to compromise Cathay's information systems security, flight operation and business secrets. (para. 9)

The facts of the data breach incident (**Incident**) are obtained and elicited from the admissions and statements made, information provided by Cathay in the DBN; Cathay's announcement and press release, submissions at the joint panel meeting of the Legislative Council of Hong Kong; documents produced and replies to the Commissioner's inquiries during the investigation. (paras. 10-48)

The Incident was discovered when Cathay first detected suspicious activity on its network on 13 March 2018. (para. 11)

The data subjects affected were Cathay's passengers including members of Asia Miles and Marco Polo Club, as well as registered users (**Affected Passengers**), amounting to approximately 9.4 million from over 260 countries/jurisdictions/locations. (paras. 17-18)

The personal data involved consisted mainly of the Affected Passengers' name, flight number and date, title, email address, membership number, address, phone number, etc. (paras. 19-20)

Cathay's security management and systems and the relevant remedial measures taken were also examined (paras. 21-48)

The legal issues involved focused on data security and data retention, and the relevant provisions are respectively set out in Data Protection Principles 4 and 2, Schedule 1 to the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (**Ordinance**). (paras. 49-66)

Views, Findings and Contraventions

Data Breach Notification to the Commissioner

There being no statutory requirements under the Ordinance for a data breach notification, whether to the Commissioner or Affected Passengers and whether within a particular period of time or otherwise, the Commissioner finds that there is no contravention of the Ordinance in this connection. (para. 69)

Notification to Affected Passengers

Cathay, without contravening any statutory requirement under the Ordinance though, could have notified the Affected Passengers of the suspicious activity once detected and advised them of the appropriate steps to take earlier to meet their legitimate expectation. (paras. 70-71)

Data Security

Cathay failed to identify the commonly known exploitable vulnerability and the exploitation, and did not take reasonably practicable steps to accord due deployment of the internet facing server (**Internet Facing Server**). (paras. 72-81)

Cathay's vulnerability scanning exercise for the Internet Facing Server at a yearly interval was too lax in the context of effectively protecting its information systems (**IT System**) against evolving digital threats. (para. 82)

Cathay had not taken reasonably practicable steps not to expose the administrator console port of the Internet Facing Server to the Internet, as a result of which a gateway for attackers was opened. (paras. 83-85)

Cathay should have applied effective multi-factor authentication to all remote access users for accessing its IT System involving personal data. (paras. 86-90)

Cathay should not have produced unencrypted database backup files to facilitate migration of data centre without adopting effective security controls, thus exposing the personal data of the Affected Passengers to attackers. (paras. 91-92)

Cathay should have had an effective personal data inventory to cover all systems containing personal data. (paras. 93-94)

Risk alertness being low, Cathay did not take reasonably practicable steps to reduce the risk of malware infections and intrusions to its IT System after the earlier security incident in 2017. (para. 95)

There is no sufficient evidence to suggest that the Incident could be attributed to Cathay's restructuring of its IT Department. (para. 96)

In all the relevant circumstances of the case in relation to personal data security, the Commissioner finds that Cathay did not take all reasonably practicable steps to protect the Affected Passengers' personal data against unauthorised access in terms of vulnerability management, adoption of effective technical security measures and data governance, contravening DPP 4(1) of Schedule 1 to the Ordinance. (para. 97)

Data Retention

The Commissioner finds that there being no justifiable reasons, Cathay did not take all reasonably practicable steps to ensure that the Hong Kong Identity Card numbers of the Affected Passengers were not kept longer than was necessary for the fulfilment of the defunct verification purpose for which the data was used, contravening DPP 2(2) of Schedule 1 to the Ordinance. (para. 98)

Enforcement Action

The Commissioner exercises his power pursuant to section 50(1) of the Ordinance to serve an Enforcement Notice on Cathay directing Cathay to remedy and prevent any recurrence of the contraventions. (paras. 99-100)

I. Introduction

1. On 24 October 2018, the Privacy Commissioner for Personal Data, Hong Kong (**Commissioner**) received a data breach notification (**DBN**) from Cathay Pacific Airways Limited (**Cathay Pacific**) on behalf of itself and its "*wholly owned subsidiary*" Hong Kong Dragon Airlines Limited (**Cathay Dragon**) (hereinafter collectively referred to as "**Cathay**") through their legal representative at about 11 p.m. in relation to its discovery of unauthorised access to personal data of approximately 9.4 million passengers of Cathay (**Incident**).

2. On the same day, Cathay Pacific made a listed company announcement (**Announcement**) entitled "Inside Information Data Breach"[1] and a press release[2] (**Press Release**) relating to the Incident.

3. The Commissioner immediately initiated a compliance check (**Compliance Check**) and contacted Cathay to follow up the Incident on 25 October 2018[3]. The Commissioner also advised Cathay to notify the affected passengers (**Affected Passengers**) as soon as possible, and take remedial steps with details explained immediately.

4. On 5 November 2018, upon receipt of information provided by Cathay in the Compliance Check, the Commissioner had reasonable grounds to believe that there might be contravention of the requirements under the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (**Ordinance**), and

[1] http://www3.hkexnews.hk/listedco/listconews/sehk/2018/1024/ltn20181024757.pdf

[2] https://news.cathaypacific.com/cathay-pacific-announces-data-security-event-affecting-passenger-data

[3] See media statement of 25 October 2018 entitled, "Privacy Commissioner Expresses Serious Concern over Cathay Pacific Airways Data Breach Incident" (https://www.pcpd.org.hk/english/news_events/media_statements/press_20181025.html).

commenced a compliance investigation (**Compliance Investigation**) against Cathay, pursuant to section 38(b) of the Ordinance[4] in relation to the Incident[5].

The Legislative Council Meeting

5. A joint meeting of the panels of Constitutional Affairs, Security and Information Technology and Broadcasting of the Legislative Council, Hong Kong Special Administrative Region was held on 14 November 2018 (**Joint Panel Meeting**).

6. In the written submission[6], Cathay gave an account of the Incident, which is set out below:-

"*The Legislative Council ("**LegCo**") has requested Cathay Pacific Airways Limited ("**Cathay**") to attend a joint meeting of the Panel on Constitutional Affairs, Panel on Information Technology and Broadcasting and the Panel on Security on Wednesday, 14 November, 2018. The request also invited a written submission for the joint meeting to be provided on or before noon, 12 November 2018. The written submission is set out below.*

On 24 October 2018, Cathay notified the Privacy Commissioner for Personal Data, the Hong Kong Police and the Hong Kong Stock Exchange, and shortly thereafter, other applicable regulators and affected passengers, of

[4] Section 38(b) of the Ordinance provides that "*Where the Commissioner has reasonable grounds to believe that an act or practice - (i) has been done or engaged in, or is being done or engaged in, as the case may be, by a data user; (ii) relates to personal data; and (iii) may be a contravention of a requirement under this Ordinance, then… the Commissioner may carry out an investigation in relation to the relevant data user to ascertain whether the act or practice referred to in that paragraph is a contravention of a requirement under this Ordinance.*"

[5] See media statement of 5 November 2018 entitled, "Cathay Pacific Airways Limited Data Breach Incident PCPD: Fair Enforcement of the Law" (https://www.pcpd.org.hk/english/news_events/media_statements/press_20181105.html).

[6] https://www.legco.gov.hk/yr18-19/english/panels/ca/papers/caitbse20181114cb2-222-2-e.pdf

unauthorised access to certain IT systems of Cathay that affected the personal data of certain passengers in Hong Kong and elsewhere around the world.

Before setting out the details of what happened and what actions have been taken, Cathay wishes to publicly express its great regret over this incident and to extend its sincere apologies to those passengers affected. Cathay attaches great importance to its relationship with the people of Hong Kong and is committed to improving itself so that we can continue to earn their confidence and their trust.

Throughout our investigation of this incident, our foremost objective and primary motivation has been to support our affected passengers by providing accurate and meaningful information to them. Cathay respects the fact that all personal data needs to be protected and is important to the individual and we take our passengers' concerns caused by this incident very seriously. The investigation was complex, longer than what we would have wished and we would have liked to have been able to provide this information sooner.

What happened?

Cathay and our affected passengers are victims of a cybercrime carried out by sophisticated attacker(s). Upon discovery we immediately launched a comprehensive investigation with the help of external experts to determine what occurred and what information was affected. Very early in the investigation, Cathay verified that its operations and flight safety systems were not impacted and flight safety was never compromised. The investigation continued [focusing] *on three objectives: (i) investigation, containment and remediation; (ii) confirming which data had been accessed and whether it could be read by the attacker(s); and (iii) determining the types of personal data that pertain to each affected passenger and notification. Once we met these objectives, we notified affected passengers and relevant authorities.*

Who was affected and what information was accessed?

The affected passengers include members of the Asia Miles programme and the Marco Polo Club, as well as non-member passengers who travelled on Cathay or Cathay Dragon services. Our investigation revealed that approximately 9.4 million passengers globally were affected by this incident.

Types of personal data that were found to be accessed include passenger name, nationality, date of birth, phone number, email address, postal address, travel document and/or passport number, identity card number, frequent flyer membership number, customer service remarks, and/or historical travel information. The combination and number of personal data accessed varied by affected passenger. Our analysis revealed that, for the majority of affected passengers, the data accessed was limited to either passenger name and phone number or passenger name and email.

Our investigation also revealed that, although our systems designed to process payment information appropriately masked credit card details, a very small number of mostly expired credit card numbers were accessed by the attacker(s) because they had been improperly entered into a field not intended for credit card data. In no case was the credit card data complete.

No passenger's travel or loyalty profile was accessed in full, and no passenger passwords were compromised.

During our investigation, Cathay has employed cybersecurity experts to search the dark web and other sites. On the basis of such searches to date, we have found no evidence that any of the stolen data has appeared in these forums. Cathay will continue these searches.

Supporting our passengers

Cathay believes that it was important to fully and accurately understand the scope and specific details of the personal data that had been taken from each affected passenger so as to be able to provide a meaningful, individualised notification to them.

Cathay put in place a comprehensive global notification and customer care plan in the form of individual notification letters via email or post, identifying for each passenger which types of data relating to them had been taken. A more general notice for passengers who could not be contacted individually was placed on the dedicated webpage set up by Cathay at infosecurity.cathaypacific.com.

In addition to the individualised notifications, Cathay set up various customer care channels to assist passengers who were affected by the crime, including establishing a dedicated customer call centre with a toll free number for Hong Kong passengers and a dedicated email address (infosecurity@cathaypacific.com) for passengers to enquire specifically about the data theft.

The statistics below set out the global take up by affected passengers of these customer care channels:

Service channel	***Statistics to midnight 12 November 2018***
Website	*181,700 page views*
Call centre enquiries	*5,031 calls received*
Enquiry mechanism on the Website	*19,005 enquiries received*
Emails received by infosecurity@cathaypacific.com	*5,622 emails received*

Cathay also continues to offer affected passengers the option of enrolling at no-cost in IdentityWorks, an ID monitoring service offered by Experian in countries where it is possible to offer the service, which includes Hong Kong. As at midnight 12 November 2018, approximately 50,271 passengers had enrolled.

Experian works with many leading companies, financial institutions and government agencies around the world and our research indicated that their ability to search the web (including the dark web) for evidence of unauthorized personal data usage is valuable for affected passengers. This service is optional and each passenger can choose which types of personal data they wish to input for monitoring purposes. Experian was involved in a security incident in 2015, but Experian's consumer credit database was not accessed. In Experian's continued efforts to improve security, they embarked on a global cybersecurity initiative to bolster global security and implemented standards to identify, protect, detect and respond to cybersecurity threats. Experian continues to meet all global data protection and security standards.

Cathay IT security

Cathay recognises the critical importance of IT security. Over the past three years, we have spent over HK$1 billion on IT infrastructure and security. Cathay has a dedicated team of IT security specialists who were specifically not impacted in the 2017 organisational re-design. They are responsible for overseeing IT security and their work and expertise is complemented by leading industry experts. Cathay is cognizant that changes in the cybersecurity threat landscape continue to evolve at pace as the sophistication of the attackers improves. Our plans, which include growing our team of IT security specialists, will necessarily evolve in response to this challenging environment.

Why has the investigation taken so long?

Our investigation and response to this incident involved three sequential and overlapping phases: (i) investigation, containment and remediation; (ii) confirming which data had been accessed and whether it could be read by the attacker(s); and (iii) determining the types of personal data that pertain to each affected passenger and notification.

The first phase commenced in March 2018 when Cathay first detected suspicious activity on its network and took immediate action to understand the incident and to contain it. Cathay did this with the assistance of a leading global cybersecurity firm. During this phase of the investigation, Cathay was subject to further attacks which were at their most intense in March, April and May but continued thereafter. These ongoing attacks meant that internal and external IT security resources had to remain focused on containment and prevention. Remediation activities began as part of this effort and continued throughout. Even as the number of successful attacks diminished, we remained concerned that new attacks could be mounted.

These ongoing attacks also expanded the scope of potentially accessed data, making the challenge of understanding it more lengthy and complex in phase two of the investigation.

During the second phase, the two big issues were: which passenger data had been accessed or exfiltrated and, since the affected databases were only partially accessed, whether the data in question could be reconstructed outside Cathay's IT systems in a readable format useable to the attacker(s). Conclusions on these issues proved difficult and time-consuming and were only reached in mid-August.

During the third phase, the emphasis shifted to identifying the compromised data types for each affected passenger. Cathay wanted to be able to give a single, accurate and meaningful notification to each affected passenger, rather than to provide an overly broad and non-specific notice. It was not until 24 October that Cathay had completed the identification of the personal data that pertained to each individual passenger. In parallel, arrangements were made to allow Cathay to respond promptly to passenger enquiries (see Supporting our passengers above). On 24 October 2018, disclosures and notifications began and we commenced notifying the affected passengers from 25 October 2018.

In summary, the nature of this attack involved a number of complex systems that took significant time to analyse. An enormous amount of work was involved in the investigation, which was highly technical. The process by which the stolen data could be identified, processed, and linked to a specific passenger also contributed to the length of time involved between initial discovery and public disclosure.

……

In closing, Cathay would like to apologise again to our passengers for the incident and any concerns that it has caused. We take our responsibilities with respect to our passengers' personal data very seriously and we acknowledge that there many lessons that we can and will learn from this event.

Cathay Pacific Airways Limited
November 2018"

7. The chairman of Cathay also made an opening statement[7] in the Joint Panel Meeting, which is highlighted below:-

"*... The fact that you are my passengers also makes it particularly difficult and painful for me and the Cathay Pacific team to be here today. In this regard, I must personally apologise directly to you and to the people of Hong Kong for the fact that, in this hacking incident we will discuss today, some of your personal data was improperly accessed and or stolen from our computer systems…*

We at Cathay Pacific and Cathay Dragon understand the importance of keeping your data secure and we accept our accountability for that. As we are a Hong Kong airline, we so deeply regret that this incident has impacted so many Hong Kong people…

A very short comment on the size and complexity of our IT systems. We are, along many dimensions, the largest IT users in Hong Kong, and along some dimensions, the largest in the Asia Pacific region. Our systems include 1.3 billion files that we backup, 470 databases, 4,500 servers, an enormous network, about 600 applications and we send and receive some 4.5 million emails per day. Significantly, we also block about 16,000 external emails containing viruses every month.

I offer this information not as an excuse but only to help to set out some context as this complexity ultimately played a significant role in frustrating our attempts to do what we thought was the best thing for our passengers, which was to provide true and accurate information to them on a timely basis…"

[7] Full version: https://www.legco.gov.hk/yr18-19/english/panels/ca/papers/caitbse20181114cb4-216-3-e.pdf

8. Up to the date of publication of this report, the Commissioner has received 143 complaints and 176 enquiries[8] from the public in relation to the Incident.

[8] The complainants and enquirers mainly expressed dissatisfaction about their personal data security and timeliness of notification.

II. Facts and Circumstances relevant to the Incident

9. Finding and setting out the facts and circumstances relevant to the Incident below, the Commissioner is mindful of their accuracy and sensitivity, and exercises due care and diligence to ensure that he has the accurate facts on which his investigation and findings are based, and that disclosure of these facts could not be potentially exploited or used to compromise Cathay's information systems security, flight operation and business secrets.

The Compliance Investigation

10. The Compliance Investigation was based on the admissions and statements made as well as information provided by Cathay in the DBN; Announcement; Press Release; Joint Panel Meeting; documents produced and replies to inquiries raised during the course of the Compliance Check in relation to the Incident.

11. The Incident was discovered when Cathay "*first detected suspicious activity*" on its network on 13 March 2018. During the seven-month period before the DBN was lodged, Cathay had conducted "*internal investigation*" and "*analysis*", and took relevant remedial actions to contain the Incident and enhance the security of its information systems (**IT System**).

12. In the course of the Compliance Investigation, the Commissioner obtained and reviewed evidence and information relating to the Incident through written and verbal inquiries and communications with Cathay through its legal representative.

13. It took the Commissioner five months to acquire the necessary and relevant information relating to the Incident from Cathay. During the period, Cathay provided over 10 written responses with over 2,200 pages of documents disclosed. The Commissioner also accepted that Cathay had justifications for taking time to provide responses to the requested information and documents, and granted all requests for the extension of time to reply.

14. The Commissioner made requests for the forensic investigation report prepared by the cybersecurity firm engaged by Cathay in its internal investigation. However, Cathay submitted that the cybersecurity firm was engaged by its legal representative and claimed that the forensic investigation report was protected by legal professional privilege.

15. Acknowledging also the size and complexity of Cathay's IT System in relation to the Incident, the Commissioner exercised his power under the Ordinance[9] to seek independent expert advice as a second opinion on the technology related security issues involved.

Notification to Affected Passengers

16. After the Announcement and the Press Release and starting from 25 October 2018, Cathay notified all the Affected Passengers "*via email and postal notification (where contact details* [were] *available for the* [passenger]*) and via general and substitute notice on the dedicated website*". Cathay stated that "*all individual notifications contained a list of specific types of personal data accessed which related to the recipient* [passenger]".

[9] Section 43(1) of the Ordinance provides that "*subject to the provisions of this Ordinance, the Commissioner may, for the purposes of any investigation — (a) be furnished with any information, document or thing, from such persons, and make such inquiries, as he thinks fit; and (b) regulate his procedure in such manner as he thinks fit.*"

Categories of Affected Passengers

17. Cathay admitted that Affected Passengers included Member Group and Non-Member Group. Member Group consisted of members of Asia Miles[10] and Marco Polo Club[11] and Registered Users of Cathay[12], while Non-Member Group consisted of passengers who travelled on a Cathay service.

18. Cathay's investigation revealed that approximately 9.4 million passengers globally were affected by the Incident. The number of Affected Passengers of Member Group and Non-Member Group was approximately 3.59 million and 5.86 million respectively. Cathay provided a confidential document on the breakdown of the Affected Passengers from over 260 countries/jurisdictions/locations.

Personal data affected

19. The types of personal data affected in the Incident, which were first listed in the DBN and at the Joint Panel Meeting, which were subsequently confirmed with Cathay, are listed as follows:-

[10] Asia Miles is a rewards programme (launched in February 1999) owned by Cathay and is managed and operated by Asia Miles Limited. Individuals who joined the programme could earn miles by spending daily from a wide range of travel and lifestyle categories including flights, hotels, dining, financial services, retail and technology brands.

[11] Marco Polo Club is a customer loyalty programme owned and operated by Cathay. The purpose of Marco Polo Club is to provide frequent flyers with recognition and a range of travel benefits based on the membership tier, including priority check-in, priority boarding, and additional baggage allowance and lounge access. All Marco Polo Club members are automatically members of Asia Miles.

[12] A Registered User is a passenger who registers an account with Cathay, the registered accounts simplify the booking and check-in process. This programme is operated and managed by Cathay which was launched in February 2016.

Types of personal data affected		Approximate percentage of total number of Affected Passengers
(i)	Name	100%
(ii)	Flight number and date	61%
(iii)	Title	56%
(iv)	Email address	53%
(v)	Membership number	38%
(vi)	Address	24%
(vii)	Phone number	19%
(viii)	Nationality	12%
(ix)	Passport number	9%
(x)	Date of birth	8%
(xi)	Identity card number[13]	6%
(xii)	Credit card number[14]	0.004%
(xiii)	Customer service remarks[15]	Not applicable

Table 1 – Approximate percentage of Affected Passengers by different types of personal data

[13] Including Hong Kong Identity card number (~243,000), other identity card number (~310,000), and other travel permit numbers (~52,000) e.g. Hong Kong Macao Permit for China Resident, Hong Kong Macao Permit for China Resident for Business Purpose, Mainland Travel Permit for Taiwan Resident, Returning Resident Permit for Hong Kong Macao Resident and Travel Permit of Mainland Residents to and from Mainland China.

[14] Cathay stated that 430 credit card numbers had been accessed and the vast majority (403) of which were expired.

[15] Cathay stated that "customer service remarks" consisted of unstructured data contained in the free text fields of the relevant affected systems. However, it was unable to identify passenger in the free text fields due to the nature of the relevant database files but this item was included in its public announcement "*out of an abundance of caution*".

20. Cathay stated that no passenger's profile had been accessed in full because the compromised data consisted of partial extracts of a number of databases rather than any single database in its entirety. It also stated that no passwords were compromised. The Commissioner has no dispute on these facts.

Cathay's IT Security

21. Cathay provided the organisation structure of its IT Department for the period from 2013 to 2018 to the Commissioner for examination.[16]

22. At the Joint Panel Meeting, Cathay provided a written submission stating that:

> " *Cathay recognises the critical importance of IT security. Over the past three years, we have spent over HK$1 billion on IT infrastructure and security. Cathay has a dedicated team of IT security specialists who were specifically not impacted in the 2017 organisational re-design. They are responsible for overseeing IT security and their work and expertise is complemented by leading industry experts. Cathay is cognizant that changes in the cybersecurity threat landscape continue to evolve at pace as the sophistication of the attackers improves. Our plans, which include growing our team of IT security specialists, will necessarily evolve in response to this challenging environment.*"[17]

23. Cathay Pacific managed and provided information management services[18] to Cathay Dragon, and "*personal data of Cathay Dragon passengers resides on* [IT System]". The Commissioner examined the relevant service agreement

[16] For the purpose of protecting sensitive information that attackers could potentially exploit and use to compromise Cathay's security, the details of the organisation structure of the IT Department are redacted.

[17] https://www.legco.gov.hk/yr18-19/english/panels/ca/papers/caitbse20181114cb2-222-2-e.pdf, page 3.

[18] The information management services included application software licenses and maintenance, application support outsourcing services, application support resources, infrastructure hardware, infrastructure outsourcing services, infrastructure software licenses and maintenance, IT consulting services, and network and telecommunications services.

between Cathay Pacific and Cathay Dragon and has no dispute about these facts.

24. In his opening statement at the Joint Panel Meeting, the chairman of Cathay briefly described the size and complexity of Cathay's IT System:-

> "*…We are, along many dimensions, the largest IT users in Hong Kong, and along some dimensions, the largest in the Asia Pacific region. Our systems include 1.3 billion files that we backup, 470 databases, 4,500 servers, an enormous network, about 600 applications and we send and receive some 4.5 million emails per day. Significantly, we also block about 16,000 external emails containing viruses every month.*" [19]

Affected systems

25. The Commissioner has no dispute about information provided by Cathay that there were over 120 systems containing personal data among its IT System as of December 2017, four of which were affected in the Incident (**Affected Systems**)[20]:

(i) [System A] was a customer loyalty system used for "*processing and recording membership of* [passengers] *in the Member Group*". In the Incident, one database of [System A] was affected.

(ii) [System B] was "*a shared back-end database primarily used to support web-based applications*". One database of [System B] was affected in the Incident. Cathay stated that it was "*in the process of migrating* [System B] *from one data centre to a new data centre*", and the database

[19] See footnote 7.

[20] For the purpose of protecting sensitive information that attackers could potentially exploit and use to compromise Cathay's security, the details of the Affected Systems are redacted.

backup files of [System B] (which were accessed in the Incident) were "*saved in the production server to facilitate the migration*".

(iii) [System C] was "*a reporting tool that compiles reports*" depending on "*the database being reported on*". In relation to the Incident, attackers accessed and exfiltrated personal data contained in Cathay's customer information system (**CIS**) via [System C].

(iv) [System D] was "*a transient database which* [allowed] *Asia Miles members to redeem non-air rewards*". One database of [System D] was affected in the Incident.

26. Cathay informed that it "*owns and operates these four systems*". All of the Affected Systems were "*mutually exclusive and…not related to one another*".

27. Cathay also informed that "*third-party vendors are involved in maintaining the* [Affected Systems]", and no personal data had been transferred to the service providers for these purposes. After examining the relevant service agreements between Cathay and the third party service providers, the Commissioner has no dispute on Cathay's information.

Security measures

28. In the course of Compliance Investigation, the Commissioner examined the submission of Cathay's organisational and technical security measures adopted to protect passengers' personal data in the IT System, which included operations security, network security and access control.

29. The sensitive security measures were not published in this report with a view to helping protect Cathay's IT System from further attacks.

30. Cathay had a set of IT policies in place which were uploaded to its internal network.

Notable activities in IT System

31. As admitted in the DBN and revealed by the replies in the course of Compliance Investigation, the notable activities in Cathay's IT System are set out below:

Date / Period	**Events**
15 October 2014	"*The earliest date of unauthorised access to Cathay's information systems*" as revealed by Cathay's internal investigation after the Incident. "*The attacker installed a Malware keylogger on* [System C]" in order to harvest user account credentials.
2016 – 2018	Data centre migration process.
7 May 2017	Cathay discovered an unauthorised access incident to its IT System of which the earliest date of compromise occurred on 7 September 2016. According to Cathay, there was no evidence of data leakage as a result of the unauthorised access.
August 2017	Introduction of personal data inventory project.
13 March 2018	The Incident was discovered when Cathay first detected suspicious activity related to a brute force attack resulting in approximately 500 staff users being locked out of their user accounts.
14 March 2018	Cathay commenced an internal investigation (with the assistance of a cybersecurity firm engaged from 22 March 2018).

31 March 2018	"*Attacker activity was detected in relation to* [System C] *that queries* [CIS]".
4 April 2018	Cathay "*discovered archives had been placed on a server that contained the database backup of* [System B] *and may have been the subject of attacker activity*".
4 May 2018	"*The attacker remotely accessed Cathay's environment and exfiltrated files identified as partial database back-ups for* [System A]".
6 May 2018	"*Additional malware was uncovered relating to* [System C]".
7 May 2018	Cathay "*confirmed that there had been unauthorised access to some of its information systems containing passenger data*".
8 May 2018	"*The attacker accessed the administrator console of* [System D's website] *to view customer redemption and transaction data and export a database back-up*".
28 August 2018	"*An attempted attack was contained and blocked before any data was accessed*".

Table 2 - Notable activities in IT System

Stated cause of the Incident

32. Cathay stated that its internal investigation identified that "*the cause of the Incident was a direct result of* [unauthorised] *access",* which was suspected to be conducted by "*two distinct groups of attackers*".

Group One Attack

33. Cathay stated that "[the] *earliest evidence of activity by what* [was] *suspected as Group One occurred on 15 October 2014*", where it was found that a keylogger malware[21] had been installed on [System C] in order to harvest user account credentials. However, it was unable to identify the path of the initial intrusion to Cathay's IT System at that time.

Accessing the IT System by valid user account credentials via Virtual Private Network (**VPN**)

34. Using the stolen but valid user account credentials, the attackers accessed Cathay's IT System via its VPN (bypassing the VPN restriction) and the personal data contained therein. On the other hand, the attackers moved laterally[22] among the network and further placed credential dumping tools in order to extract domain credentials. The attack activity ended on 22 March 2018.

Group Two Attack

(1) Initial intrusion

35. The attackers exploited vulnerability (**Vulnerability**) of an internet facing server (**Internet Facing Server**) which enabled them to bypass authentication and gain administrative access. The Vulnerability also enabled the attackers to, and the attackers did move laterally in the IT System and install the malware and credential harvesting tools. This Vulnerability, which existed in Cathay's Internet Facing Server at the material time when the unauthorised access

[21] A keylogger malware is a program that captures activities from an input device. An attacker can make use of keylogger malware to capture personal data being input into a computer system.

[22] Lateral movement is a kind of technique cyber attackers use to progressively move through a network in order to search for their targets (e.g. data).

occurred, had been published widely on the Internet since 2007[23]. Cathay stated that "*the earliest evidence of activity by what* [was] *suspected as Group Two occurred on 10 August 2017*".

36. The Internet Facing Server was built with its application version 3.0 in March 2017. Cathay stated that it was unable to upgrade the application version to the latest version because it was incompatible with an airbus fleet manuals application[24] and therefore it opted to use an earlier version of the software application.

37. Cathay claimed that it had run a vulnerability scan on the Internet Facing Server as part of its operational acceptance testing in March 2017 before it went live. However, the scan did not identify the Vulnerability. Cathay claimed that it was not aware of the Vulnerability when it opted and continued to use version 3.0.

38. Cathay further claimed that the anti-malware and endpoint protection application installed on the Internet Facing Server was unable to detect the relevant malware and utilities because "*there were no publicly available signatures*".

(2) *Brute force attack*

39. The Incident was discovered when Cathay "*first detected suspicious activity*" on its network related to a brute force attack[25] on 13 March 2018 "*resulting in approximately 500 staff users being locked out of their user accounts*". Upon

[23] The Vulnerability existed in application version 3.0 of the Internet Facing Server.

[24] The airbus fleet manuals application hosted the manuals and performance data of the airbus fleets and distributed content to users' tablets.

[25] Brute force attack is a technique used to break an encryption or authentication system by trying all possibilities.

becoming aware of this activity, Cathay commenced an internal investigation with the assistance of a cybersecurity firm.

40. Cathay admitted that it was "*unable to determine whether any accounts were compromised as a result of this attack*".

(3) *Accessing the IT System by valid user account credentials via VPN*

41. The attackers made use of the stolen user account credentials and accessed the IT System via VPN. The last known activity of the attack was on 11 May 2018.

User account credentials

42. Cathay admitted that a total of 41 valid user account credentials had been stolen to access its network via VPN. The stolen user account credentials were of different types which included the administrator, user, web and service accounts. By planting various malware and utilities, further credentials were harvested, which enabled the attackers to move laterally within Cathay's IT System.

Data Retention

43. Cathay had the relevant policy and guidelines in place, which provided that the information should not be kept longer than is necessary for the purpose of which it was collected.

Personal data of the Member Group

44. Cathay's retention practice was to purge personal data once a member had been marked as "*inactive*"[26] for seven consecutive years.

Personal data of the Non-Member Group

45. Personal data of non-members would be retained for seven years from the date of the transaction was completed.

46. To the extent that the Affected Passengers (of both Member Group and Non-Member Group) used a web based application sitting on [System B], some of their data might also exist in [System B]. Cathay stated that [System B] was a database with multiple tables, different web-based applications extract data from the relevant tables required for the application, and the retention periods of which varied from application to application.

Personal data of members of Asia Miles

47. An Asia Miles member might have data (including basic profile data such as name and contact details) shown temporarily on [System D], which allowed for the redemption of non-air rewards. The data would only show during the course of a transaction and would subsequently be transferred to [System A], the retention period of which would apply.

[26] In its reply to questions raised in the course of the Compliance Investigation, Cathay explained that a registered user would be marked "*inactive*" when such user requested his/her account be terminated, or duplicate accounts were identified for such user. For example, a Marco Polo Club member would be marked as "*inactive*" if (a) a member requested his/her Marco Polo Club and/or Asia Miles membership be terminated; (b) duplicate Marco Polo Club memberships (and by default Asia Miles memberships) were identified for a member; or (c) a member failed to maintain the minimum travel criteria for the lowest tier during a consecutive 12 month period and failed to pay a renewal fee; an Asia Miles member would be marked as "*inactive*" in one of the following situations: (a) a member requested his/her Asia Miles and/or Marco Polo Club membership be terminated; (b) duplicate memberships were identified for a member; or (c) a member failed to accrue any Asia Miles points during a consecutive 36 month period.

Remedial measures

48. Cathay claimed that, upon becoming aware of the Incident, it had taken a series of remediation activities to contain the Incident and block the attackers with the assistance of the cybersecurity firm engaged.[27]

[27] For the purpose of protecting sensitive information that attackers could potentially exploit and use to compromise Cathay's security, the details of the series of remediation activities are redacted.

III. Legal Issues and Regulatory Framework

The Ordinance

49. The privacy of individuals in relation to personal data is protected under the Ordinance, which is by design principle-based and technology-neutral, having reference to the 1980 OECD Guidelines and 1995 EU Data Protection Directive. Its core provisions are encapsulated in the six data protection principles (**DPP**) set out in Schedule 1 to the Ordinance, although individual acts may be specifically regulated under the Ordinance. The object of the DPP was to create a framework regulating the handling of personal data during the entire life cycle of personal data from collection to destruction. In most cases, contraventions of the DPP do not constitute criminal offences until the contravening party fails to comply with the terms of an enforcement notice issued by the Commissioner after an investigation, directing remedies to be taken and steps to prevent recurrence of the contravention. Contravention of a DPP may also form the basis of a civil suit against the contravening party by the aggrieved party for compensation of damage suffered under section 66 of the Ordinance, whether or not an enforcement notice has been issued.

The Regulatory Approach

50. The Commissioner's regulatory approach is consistent with the general common law rules on statutory interpretation and in particular those laid down by the Interpretation and General Clauses Ordinance, Chapter 1, Laws of Hong Kong. Section 19 of this ordinance provides that an ordinance "*shall be deemed to be remedial and shall receive such fair, large and liberal construction and interpretation as will best ensure the attainment of the object of the* [ordinance] *according to its true intent, meaning and spirit*". This "fair, large and liberal" approach was explained in the Court of Final Appeal case of

The Medical Council of Hong Kong v David Chow Siu Shek [2000] 2 HKLRD 674.

51. The Commissioner is also constantly mindful of the generally recognised principle of "presumption against absurdity" in statutory interpretation as explained in *Bennion on Statutory Interpretation* (sixth edition, Butterworths).

52. As a fair enforcer of the law, the Commissioner, whilst applying a consistent interpretation of the law, may find it proper and necessary to have regard to changes in circumstances and social values, such as rulings and views of local and overseas judicial authorities, the changing global privacy landscape, the evolving digital paradigm and data driven economy, the growing information and communication technologies for development, views of the relevant experts, as well as the associated expectation of all stakeholders, organisations and individuals alike.

Personal Data

53. "*Personal data*", as defined in section 2(1) of the Ordinance, means "*any data* –

(a) relating directly or indirectly to a living individual;

(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and

(c) in a form in which access to or processing of the data is practicable."

Data Subject

54. The "*living individual*" referred to above is also statutorily known as "*data subject*" as defined in section 2(1) of the Ordinance.

Data User

55. The Ordinance, including the DPP, aims to regulate the acts and practices of a data user being, as defined in section 2(1) of the Ordinance, "*a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data*".

Data Breach

56. A data breach generally refers to a suspected or actual breach of data security concerning personal data held by a data user; the exposure of the data to the risk of loss, unauthorised or accidental access, processing, erasure or use; the unauthorised access and transfer of personal data stored in a database by hackers; the improper disposal of documents containing personal data, etc.

Data Breach Notification

57. Currently it is not mandatory under the Ordinance for a data user to notify or report to the Commissioner or the relevant data subjects of a data breach. The Commissioner nevertheless has encouraged it as good practice and issued a "*Guidance on Data Breach Handling and the Giving of Breach Notifications*"[28].

Data Security

58. It is in the context of a data breach that data security is the crux of the Compliance Investigation.

[28] https://www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf

59. With the increasing provision of online services for consumers, coupled with the increasing use of online services to collect, store or transmit personal data, data users are obliged to ensure information system security and the protection of personal data collected, stored and transmitted online from unauthorised or accidental access or removal by, for example, hackers or other unintended users.

60. DPP 4(1) – Security of Personal Data provides as follows:

"*All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure, loss or use having particular regard to –*

(a) the kind of data and harm that could result if any of those things should occur;

(b) the physical location where the data is stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data".

61. "*Practicable*" is defined in section 2(1) of the Ordinance to mean "*reasonably practicable*".

62. The "*harm*" test in DPP 4(1)(a) above calls for the consideration whether the security measures undertaken by the data user with respect to the personal data held were proportionate to the degree of sensitivity of the data and the harm that might result from unauthorised or accidental access to such data.

63. It should also be noted that DPP 4 concerns only the way in which personal data is stored or transmitted but not the way it is used, which is governed by DPP 3.

Data Retention

64. Once personal data is collected, the data user will have to consider, inter alia, how long it should be kept, as unnecessary and excessive period of retention of personal data would inevitably create or increase the risk of data security.

65. DPP 2(2) lays down the principle of data retention which provides that:

"*All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data is or is to be used*".

66. DPP 2(2) was amended in 2012 to clarify that a data user is only required to take all reasonably practicable steps to comply with this data retention principle, which had hitherto been interpreted to impose an absolute duty on the data user to ensure that personal data was not kept longer than is necessary.

IV. Views, Findings and Contraventions

Personal Data; Data Subject; Data User; Data Breach

67. As evidenced in the admissions and statements made as well as information provided by Cathay in the DBN; Announcement; Press Release; Joint Panel Meeting; documents produced and replies to inquiries raised during the course of Compliance Check and Compliance Investigation, there is no dispute and the Commissioner so finds, within the meaning of the Ordinance (including the Schedules) that at the material time of the Incident:

(i) the data involved and affected was personal data;
(ii) the Affected Passengers (Member and Non-Member Groups) were data subjects;
(iii) Cathay Pacific and Cathay Dragon were data users; and
(iv) there was a data breach.

The Affected Passengers

68. The Commissioner finds that at the material time the Affected Passengers included those who travelled on a Cathay service, members of Asia Miles and Marco Polo Club and Registered Users of Cathay.

Data Breach Notification to the Commissioner

69. Notwithstanding that there is no statutory requirement under the Ordinance for a data user to notify the Commissioner and the data subjects of a data breach, and there is no statutory requirement for the data user to so notify within a prescribed period of time, Cathay did lodge a DBN with the Commissioner on 24 October 2018 and take steps to notify the data subjects (i.e. the Affected

Passengers). The Commissioner finds that there is **no contravention of the Ordinance** in this connection.

Notification to Affected Passengers

70. There being no statutory requirement under the Ordinance for Cathay to notify the Affected Passengers of the Incident, the Commissioner appreciates the efforts made by Cathay to have done so. The ways the Affected Passengers were notified included public announcements, individual notification letters via email or post, general notice on a dedicated webpage, a dedicated customer call centre and a dedicated email address. Cathay explained that notification was not made until 25 October 2018 because "*Cathay believes that it was important to fully and accurately understand the scope and specific details of the personal data that had been taken from each affected passenger so as to be able to provide a meaningful, individualised notification to them*" and "*the nature of this attack involved a number of complex systems that took significant time to analyse. An enormous amount of work was involved in the investigation, which was highly technical. The process by which the stolen data could be identified, processed, and linked to a specific passenger also contributed to the length of time involved between initial discovery and public disclosure*".[29]

71. Considering the fact that the notification was not given until seven months after Cathay had discovered the Incident when it first detected suspicious activity on its network and the reasons given for taking such a period of time, the Commissioner takes the view that **Cathay, without contravening any statutory requirement under the Ordinance though, could have notified the Affected Passengers of the suspicious activity once detected and**

[29] See footnote 6.

advised them of the appropriates steps to take earlier to meet their legitimate expectation.

Data Security

72. The primary concern and the stated cause of this Incident are that unknown attackers bypassed or defeated the cybersecurity of Cathay's IT System and/or exploited the vulnerability existing in the IT System. The security policies and measures deployed in the IT System were examined critically.

73. The Commissioner is mindful that, DPP 4 does not impose upon Cathay an absolute duty on the security of personal data.

74. In the Administrative Appeals Board[30] (**AAB**) No. 8/2008, the AAB concluded that:

> *"…The data user is only required to take all practicable steps in the circumstances to protect personal data from unauthorised or accidental access. The steps that a data user is required to take must be practicable for him to take. In construing DPP4 and in determining what steps a data user should take to protect personal data, particular regard need to be given to, inter alia, "the kind of data and the harm that could result" (see para. (a) of DPP4). The Commissioner is accordingly correct in submitting that* ***the steps required to be taken must be "proportionate to the degree of sensitivity of the data and harm that will result from accidental or unauthorized access to such data".***" [31]
>
> [Emphasis added.]

[30] An independent statutory body established under the Administrative Appeals Board Ordinance, Chapter 442, Laws of Hong Kong, in July 1994. AAB will hear and determine appeals against a decision made in respect of an appellant and which falls under its jurisdiction, including the Ordinance.

[31] https://www.pcpd.org.hk/english/enforcement/decisions/files/AAB_8_2008.pdf, at para. 36.

75. In a more recent case (AAB No. 70/2016), the AAB confirmed that:

> "…*The legal requirement under DPP4 of* [Ordinance] *is fulfilled by the data users' taking all reasonably practicable steps to ensure that the data subjects' personal data are protected.* ***All reasonably practicable steps are not intended to be the perfect or watertight risk-proof way of handling data subjects' personal data. Every system/step taken may have some known or unknown shortcomings. Provided it is the reasonably practicable step in all the circumstances of the case, such step is not amenable to any challenge under DPP4 of*** **[Ordinance].**" [32]
>
> [Emphasis added.]

"Reasonably Practicable" Steps

76. Given the meaning as professed by the AAB and the regulatory approach, the Commissioner appreciates that the steps required of a data user may vary from case to case, and a host of factors including the volume, kind and sensitivity of data, the harm and damage that could result from the data breach, corporate governance and organisational measures, and technical policies, operations, controls and other security measures of the reasonable quality and standard expected of an organisation like Cathay[33]. In addition, the steps taken in response to the data breach (e.g. notification to the relevant parties) as well as forward looking steps (e.g. preventive security measures) have also been taken into account.

---

[32] https://www.pcpd.org.hk/english/enforcement/decisions/files/AAB_70_2016.pdf, at para. 51.

[33] Cathay offers scheduled passenger and cargo services to more than 200 destinations in over 50 countries and territories.

77. The Commissioner has also made reference to overseas jurisdictions on the application of "*reasonably practicable*" steps to ensure the security of personal data[34]. Article 32 of the European Union General Data Protection Regulation 2016[35] (**GDPR**) suggests that the data controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

78. Recognising that cyberattacks become common and sophisticated, and the "*reasonably practicable*" steps are by no means exhaustive, the Commissioner adopts the totality approach in the assessment.

(1) *Failure to identify the Vulnerability and Exploitation*

79. Cathay stated that attackers accomplished the initial intrusion to Cathay's IT System by exploiting the Vulnerability of the Internet Facing Server. Cathay claimed that it had conducted vulnerability scan but did not identify the Vulnerability when building the Internet Facing Server in March 2017. Cathay further stated that it had re-run the vulnerability scan against a restored image of the Internet Facing Server but still failed to identify the Vulnerability.

80. The Commissioner finds that the Vulnerability, which had already been published widely on the Internet since 2007, was well known at the material time. Researches were conducted by the Commissioner on the relevant websites publishing common vulnerabilities and all of the results readily identified the Vulnerability. In addition, the vulnerability scanning tool used by Cathay was found to be equipped to detect the Vulnerability with signature

[34] Including the "Guide to securing personal information" of the Office of the Australian Information Commissioner (https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-securing-personal-information.pdf), the investigation report on DonateBlood.com.au data breach (https://www.oaic.gov.au/resources/privacy-law/commissioner-initiated-investigation-reports/donateblood-com-au-data-breach-australian-red-cross-blood-service.pdf), and Federal Trade Commission v AshleyMadison.com (https://www.ftc.gov/enforcement/cases-proceedings/152-3284/ashley-madison), etc.

[35] See https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en for further information.

released in 2013. This implies that the Vulnerability should have been discovered if Cathay had fully utilised the scanning tool to identify all known vulnerabilities in a timely manner.

81. The Commissioner finds that **Cathay failed to identify the commonly known exploitable Vulnerability (as referred to in paragraph 35) and the exploitation, and did not take reasonably practicable steps to accord due deployment of the Internet Facing Server**.

(2) Lax interval of vulnerability scanning exercise

82. Cathay had conducted a vulnerability scan on the Internet Facing Server before it went live in March 2017. Whilst Cathay scheduled annual vulnerability scanning exercise, there was no such scanning during the period when attackers exploited the Vulnerability and gained access to Cathay's IT System. The Commissioner finds that, in view of the enormous size of Cathay's IT System, the volume and sensitivity of the personal data contained therein, **Cathay's vulnerability scanning exercise for the Internet Facing Server at a yearly interval was too lax in the context of effectively protecting its IT System against evolving digital threats**.

(3) Exposing the administrator console port of the Internet Facing Server to the Internet

83. The Vulnerability which had not been detected provided an attacker with the ability and opportunity to access the administrator console and web management interface of the Internet Facing Server. This could have been mitigated by modifying the configuration of the Internet Facing Server at the deployment so that the administrator console port could only be accessed by authorised personnel from the internal network and hence would not be exposed to the Internet. However, the administrator console port of the

Internet Facing Server was left accessible from the Internet at the material time, and thus opening a gateway to attackers.

84. The Commissioner takes the view that the risk of exploiting the Vulnerability should have been mitigated by Cathay when deploying the Internet Facing Server, by following security hardening principles to limit the attack surface, i.e. restricting the administrator console port which could be used to manage and configure the server from being accessible from the Internet.

85. The Commissioner finds that **Cathay had not taken reasonably practicable steps not to expose the administrator console port of the Internet Facing Server to the Internet, as a result of which a gateway for attackers was opened**.

(4) *Lack of multi-factor authentication for all remote access users*

86. As revealed in Cathay's internal investigation, the attackers were suspected to have made use of the initial intrusion to access Cathay's IT System and planted malware and utilities in order to harvest user account credentials. The attackers used the stolen user account credentials[36] to disguise themselves as legitimate entrants and gained access to Cathay's IT System through VPN for accessing personal data stored therein.

87. Cathay claimed to have had multi-layer approach to control the access to Cathay's IT System via VPN[37]. The access required two-factor authentication in order to protect against the use of stolen credentials but this control applied to IT support teams only and not other remote access users of the IT System at the time of the Incident. Cathay claimed that "…*due to ongoing instabilities*

[36] Cathay stated that, according to its investigation, a total of 41 user account credentials had been stolen.

[37] Including two-factor authentication, measures to prevent or restrict unauthorised access to the VPN, and the use of access control list and active directory to manage access to permitted applications via VPN.

with the solution and a lack of suitable local support to remediate, it was not practicable to complete the rollout to all remote users…". The Commissioner considers that this attitude towards passengers' personal data security could have been more positive and proactive.

88. In the course of Compliance Investigation, there is no evidence to suggest that Cathay fully leveraged its privilege identity management system, supported by multi-factor authentication, so as to limit and tightly control elevation of privileges[38] to the IT System.

89. The Commissioner notes that, after the Incident, Cathay expanded the application of authentication and decided to change the solution in July 2018 for all remote users.

90. The high demand of remote access to Cathay's IT System considered, the Commissioner is of the view that the limited access control of remote access (i.e. application of two-factor authentication to IT support teams) was ineffective in protecting the system and a robust secure remote access mechanism was warranted. The Commissioner finds that **Cathay should have applied effective multi-factor authentication to all remote access users for accessing its IT System involving personal data**.

(5) Exposing unencrypted database backup files for facilitating data centre migration

91. The Compliance Investigation revealed that during the data centre migration process from 2016 to 2018, the database backup files in the production server of the two Affected Systems ([Systems A and B]) used for facilitating data centre migration were not encrypted. Cathay explained that saving the database backup files in the production server was the most practicable way to

[38] E.g. administrator privileges to manage servers.

facilitate the migration for reducing the required migration time[39] and enabling faster recovery and fallback time in relation to migration issues.

92. The Commissioner considers that given the sensitivity of personal data involved, Cathay should have adequately evaluated the security risks and adopted the appropriate data handling approaches before producing the database backup files, including applying the right methods of managing data for data migration process, encrypting the database backup files at rest, and limiting the data required, which could have effectively reduced the damage done when attackers intruded Cathay's IT System. The Commissioner finds that **Cathay should not have produced unencrypted database backup files to facilitate migration of data centre without adopting effective security controls, thus exposing the personal data of the Affected Passengers to attackers**.

(6) *Ineffective personal data inventory*

93. Cathay confirmed that prior to the Incident, it had not had a centralised personal data inventory to record all passengers' personal data contained in the IT System. Cathay started the personal data inventory project in August 2017 and claimed that due to the number of systems involved, the process had been complex and time consuming thus the implementation was not put in place at the time of the Incident. The absence of personal data inventory to cover all systems containing personal data at the time of the Incident seriously undermined the effectiveness of Cathay's data governance.

94. The Commissioner finds that, given the scale of Cathay's IT System and the volume and sensitivity of personal data held, **Cathay should have had an**

[39] This included reducing downtime for applications for Cathay's 24/7 operations, minimising the impact to Cathay's business operations and ensuring the data centre migration timeline to be met.

effective personal data inventory to cover all systems containing personal data.

(7) *Lessons from previous security incident not learnt*

95. According to a previous security incident report, Cathay had discovered an unauthorised access incident to its IT System in May 2017 and took consequential remedial measures. The Commissioner is of the view that Cathay should have learnt from the experience of this previous incident and improved its incident management by thoroughly reviewing and evaluating the security risks of the entire network, including strengthening the protection of its entire IT infrastructure and systems (e.g. review and update the function of security tools, review and re-run security testing of systems and devices with high risks etc.), which could reduce the risk of similar incidents. The Commissioner finds that **risk alertness being low, Cathay did not take reasonably practicable steps to reduce the risk of malware infections and intrusions to its IT System after the earlier security incident in 2017**.

(8) *Restructuring and downsizing of IT Department*

96. During the course of Compliance Investigation, the Commissioner also examined the organisation structure of Cathay's IT Department, the details of which are redacted for Cathay's security reasons. The Commissioner finds that there is **no sufficient evidence to suggest that the Incident could be attributed to Cathay's restructuring of its IT Department**.

97. In all the relevant circumstances of the case in relation to personal data security, the Commissioner finds that **Cathay did not take all reasonably practicable steps to protect the Affected Passengers' personal data against unauthorised access in terms of vulnerability management, adoption of**

effective technical security measures and data governance, contravening DPP 4(1) of Schedule 1 to the Ordinance.

Data Retention

Unnecessary retention of Hong Kong Identity (HKID) Card numbers of Asia Miles membership programme subscribers

98. Cathay admitted to have collected approximately 240,000 HKID Card numbers from Asia Miles membership programmes subscribers since inception of the programme, which were used for identity verification purposes. This verification practice was ceased in 2005 and the application forms (both online and paper) have since been revised. Yet these HKID Card numbers were retained for over 13 years. The Commissioner finds that, there being no justifiable reasons, **Cathay did not take all reasonably practicable steps to ensure that the HKID Card numbers of the Affected Passengers were not kept longer than was necessary for the fulfilment of the defunct verification purpose for which the data was used, contravening DPP 2(2) of Schedule 1 to the Ordinance**.

V. Enforcement Action

99. Section 50(1) of the Ordinance provides that in consequence of an investigation, if the Commissioner is of the opinion that the relevant data user is contravening or has contravened a requirement under the Ordinance, he may serve on the data user a notice in writing, directing the data user to remedy and, if appropriate, prevent recurrence of the contraventions.

100. Finding that Cathay contravened DPP 4(1) and DPP 2(2) of Schedule 1 to the Ordinance as aforesaid, the Commissioner exercises his power pursuant to section 50(1) of the Ordinance to serve an **Enforcement Notice** (**EN**) on Cathay directing Cathay to:

(1) Engage an independent data security expert to overhaul the systems containing personal data to the effect that these systems are free from known malware and known vulnerabilities;

(2) Implement effective multi-factor authentication to all remote users for accessing its IT System involving personal data and undertake to conduct regular review of remote access privileges;

(3) Conduct an effective vulnerability scan at server and application levels at an interval [40] and when there are significant changes made/new developments introduced to the servers and/or applications;

(4) Engage an independent data security expert to conduct reviews/tests of the security of Cathay's network at an interval[41];

(5) Devise a clear data retention policy to specify the retention period(s) of passengers' data stored in each and every system, which is no longer than is necessary for the fulfilment of the purpose, and

[40] For the purpose of protecting sensitive information that attackers could potentially exploit and use to compromise Cathay's security, the details of the required interval are redacted.

[41] Ditto

undertake to implement effective measures to ensure that such policy would be elucidated to relevant staff members and effectively executed;

(6) Provide documentary proof within six months from the date of the EN, or forthwith where remedial actions had been taken earlier, showing the completion of items (1) – (5) above;

(7) Completely obliterate all unnecessary HKID Card numbers collected from Asia Miles membership programme in any form from all systems; and

(8) Provide a certificate issued by an independent professional third party within three months from the date of the EN, or forthwith where remedial actions had been taken earlier, certifying the completion of item (7) above.

VI. Comments

101. As data breach incidents continue to rise and become complex, businesses have the added pressure, if not responsibilities, to keep personal data of their customers secure in order to remain competitive in the trade. First and foremost, they must comply with the law that aims to protect the personal data privacy right of individuals.

102. Whilst cyberattacks, which could be criminal of themselves being regulated by other legislative instruments, may in some cases be out of the reach of businesses, the Ordinance requires that reasonably practicable steps be taken to ensure personal data security in the case of a data breach. What these steps are would naturally turn on the facts and circumstances of each case.

103. The statutory duties to keep customers' personal data safely and to keep it no longer than is necessary need no further elaboration, suffice it to say that the data is collected from the customers who arguably own it, and businesses undeniably take it as an asset, deriving somewhat benefits out of it.

104. The fact that personal data is less tangible than other personalty (e.g. bank notes) or realty does not absolve businesses of their failures to keep it safely and to obliterate it when it is no longer necessary for the fulfilment of the purpose for which the data is or is to be used. To give effect to the legal requirements, there is also an expectation of comprehensive, effective and evidenced privacy compliance policies and programmes being put in place, relevant and scalable for the businesses concerned, as well as demonstrable internally and externally. This legitimate expectation comes from both the customers, who are the data subjects, and the regulators.

105. The idea of good data stewardship and governance, or accountability has also been incorporated in the new laws and regulations of many jurisdictions, notably the EU GDPR implemented in May 2018. Notwithstanding that similar principle of accountability is yet to be provided for in the law of Hong Kong, businesses in Hong Kong should be well poised to adopt proactive data management as corporate digital values, ethics and responsibilities in this era

of data driven economy, translating legal requirements into risk-based, verifiable and enforceable corporate practices and controls, to address regulatory changes worldwide; enable updated business models, digitalisation, globalisation and ensure data protection, sustainability and trust.

106. In particular, the trust of data subjects cannot be underrated or taken less than seriously by data users, controllers or processers, be they big or small.

107. Since 2014, the Commissioner has advocated the accountability-based Privacy Management Programme (PMP) for all organisations as part of their corporate governance. Data privacy protection should be a standing issue in the board room and not left to the hands of the IT department or personnel alone. Organisations, public and private alike, have also been provided with PMP implementation guidelines and tools[42].

108. The Commissioner is hopeful that organisations will cherish the hard-earned trust from the data subjects and the regulator by respecting and protecting the individual's personal data privacy right, which is a fundamental human right in Hong Kong, as required by the law and as expected of them, thereby developing a corporate digital responsibility fit for the 21st century with a view to helping cultivate the right privacy culture.

— End —

[42] See, for example, Privacy Management Programme: A Best Practice Guide, first revision, August 2018 (https://www.pcpd.org.hk/pmp/files/pmp_guide2018.pdf)