資料外洩事故
調查報告

根據香港法例第 486 章《個人資料(私隱)條例》
第 48(2) 條發表

國泰航空有限公司

及

港龍航空有限公司

未獲授權取覽或查閱乘客個人資料

（中文譯本）
（本報告以英文撰寫。如中文譯本與英文報告有歧異，
概以英文為準）

報告編號：R19 – 15281(c)
發表日期：2019 年 6 月 6 日

國泰航空有限公司
及
港龍航空有限公司

資料外洩事故
未獲授權取覽或查閱乘客個人資料

香港法例第 486 章《個人資料（私隱）條例》（**《私隱條例》**）第 48(2)條訂明，「[香港個人資料私隱]*專員在完成一項調查後，如認為如此行事是符合公眾利益的，可－*

(a) *發表列明以下事項的報告－*

(i) *該項調查的結果；*

(ii) *由該項調查引致的、專員認為是適合作出的關乎促進有關資料使用者所屬的某類別的資料使用者遵守本條例條文（尤其是各保障資料原則）的任何建議；及*

(iii) *由該項調查引致的、專員認為適合作出的任何其他評論；及*

(b) *以他認為合適的方式發表該報告。*」

現根據《私隱條例》第 48(2)條履行所賦予的權力和責任，發表本調查報告。

黃繼兒
香港個人資料私隱專員
2019 年 6 月 6 日

目錄

資料外洩事故
調查報告

（根據香港法例第 486 章《個人資料（私隱）條例》第 48(2) 條發表）

國泰航空有限公司
及
港龍航空有限公司

未獲授權取覽或查閱乘客個人資料

摘要

背景及調查

香港個人資料私隱專員（**專員**）在 2018 年 10 月 24 日接獲國泰航空有限公司代表其本身及港龍航空有限公司（統稱「**國泰**」）透過其法律代表，就有關國泰發現約有 940 萬名乘客的個人資料曾被未獲授權而取覽或查閱一事作出的資料外洩事故通報後，於 2018 年 11 月 5 日對事件展開調查。（第 1 至 4 段）

由於是次資料外洩事故（**該事件**）的相關事實及情況的準確性及敏感度對整個調查結果的影響甚為重要，專員謹慎行事以確保其調查及調查結果是根據準確事實而作出，並確保所披露的事實不能用作損害國泰的資訊系統安全、航班運作及商業機密。（第 9 段）

該事件的事實取自國泰的供認及陳述、資料外洩事故通報、國泰的公告及新聞稿、國泰於立法會聯席會議中所陳述的事宜，以及對專員在調查的偵訊所作出的回覆。（第 10 - 48 段）

國泰於 2018 年 3 月 13 日首次在系統中發現可疑活動跡象，因而發現該事件。（第 11 段）

受影響的資料當事人均屬國泰的乘客，當中包括亞洲萬里通和馬可孛羅會的會員和國泰的註冊用戶（**受影響乘客**）來自超過 260 個國家／司法管轄區／地區共約 940 萬名乘客。（第 17 - 18 段）

涉及的個人資料主要包括受影響乘客的姓名、航班編號及日期、稱謂、電郵地址、會員號碼、地址及電話號碼等。（第 19 - 20 段）

國泰的保安管理及系統，以及已採取的相關補救措施均已被審視。（第 21 - 48 段）

涉及的法律事宜集中在資料保安及資料保留，相關的規定載列於香港法例第 486 章《個人資料（私隱）條例》（**《私隱條例》**）附表 1 的保障資料第 2 及第 4 原則。（第 49 - 66 段）

觀點，調查所得及違例事項

<u>向專員作出資料外洩事故通報</u>

目前《私隱條例》沒有規定資料使用者須向專員及資料當事人（就該事件，即為受影響乘客）通報資料外洩事故，亦沒有規定資料使用者在指定時間內通報。因此，專員認為國泰沒有違反《私隱條例》的規定。（第 69 段）

<u>通知受影響乘客</u>

國泰即使沒有違反任何《私隱條例》的法定要求，當初亦應能在發現可疑活動時立即通知受影響乘客，並建議他們提前採取適當的步驟，以符合他們的合理期望。（第 70-71 段）

資料保安

國泰未能識辨一個廣為人知及可被加以利用的保安漏洞，亦未能識辨利用該漏洞的行為，同時沒有採取合理地切實可行的步驟在建立該伺服器時進行適當的部署。（第 72-81 段）

國泰只為該伺服器每年進行一次漏洞掃描，就有效保障國泰資訊系統以面對不斷變化的數碼威脅的做法屬流於表面及過份鬆懈。（第 82 段）

國泰沒有採取合理地切實可行的步驟，避免該伺服器的管理員控制台埠曝露於互聯網，因此導致為攻擊者開啟一個入口。（第 83-85 段）

國泰應對涉及存取國泰資訊系統內個人資料的所有遙距使用者實施有效的多重身份認證。（第 86-90 段）

國泰在沒有採取有效的保安管控措施下，不應為了方便遷移數據中心而建立未經加密的數據庫備份檔案，因而導致受影響乘客的個人資料曝露予攻擊者。（第 91-92 段）

國泰應建立有效的個人資料庫存以涵蓋所有載有個人資料的系統。（第 93-94 段）

國泰對風險的警覺性低，在 2017 年的保安事故發生後沒有採取合理地切實可行的步驟減低國泰資訊系統被植入惡意軟件及被入侵的風險。（第 95 段）

沒有足夠證據顯示資訊科技部的架構重組是導致該事件的原因。（第 96 段）

鑑於所有涉及個人資料保安的相關情況，專員認為國泰在漏洞管理、採用有效的技術保安措施，以及資料管治方面，沒有採取所有合理地切實可行的步驟，以保障受影響乘客的個人資料免受未獲授權的取覽或查閱，違反了《私隱條例》附表 1 的保障資料第 4(1)原則。（第 97 段）

資料保留

專員認為國泰在沒有合理原因的情況下，沒有採取所有合理地切實可行的步驟，確保受影響乘客的香港身份證號碼的保留時間不超過達致已廢除的核實身份的目的，違反了《私隱條例》附表 1 的保障資料第 2(2)原則。（第 98 段）

執法行動

專員根據《私隱條例》第 50(1)條所賦予的權力，向國泰送達執行通知，指示國泰糾正以及防止有關違反再發生。（第 99-100 段）

I. 引言

1. 2018 年 10 月 24 日晚上約 11 時，香港個人資料私隱專員（**專員**）接獲國泰航空有限公司（**國泰航空**）及其「*全資附屬公司*」港龍航空有限公司（**國泰港龍**）（以下統稱「**國泰**」）透過其法律代表，就國泰發現約有 940 萬名國泰乘客的個人資料曾被未獲授權取覽或查閱一事（**該事件**）作出的資料外洩事故通報。

2. 同日，國泰航空就該事件發佈一則標題為「內幕消息　資料外洩事件」的上市公司公告[1]（**該公告**）及一則標題為「國泰航空公佈涉及乘客資料的資料安全事件」的新聞稿[2]（**該新聞稿**）。

3. 專員隨即於 2018 年 10 月 25 日主動展開循規審查，並聯絡國泰跟進該事件[3]。專員亦建議國泰盡快通知受影響乘客（**受影響乘客**），及即時採取並闡釋有關的補救措施。

4. 2018 年 11 月 5 日，專員在收到國泰於循規審查所提供的資料後，有合理理由相信國泰可能涉及違反香港法例第 486 章《個人資料（私隱）條例》（**《私隱條例》**）規定的情況，遂依據《私隱條例》第 38(b)條[4] 就該事件向國泰展開循規調查[5]。

---

1 http://www3.hkexnews.hk/listedco/listconews/SEHK/2018/1024/LTN20181024758_C.pdf

2 https://news.cathaypacific.com/**國泰航空公佈涉及乘客資料的資料安全事件**

3 見 2018 年 10 月 25 日標題為「私隱專員非常關注國泰航空公司外洩客戶個人資料事件」的新聞稿 (https://www.pcpd.org.hk/tc_chi/news_events/media_statements/press_20181025.html)。

4 《私隱條例》第 38(b)條訂明：「*凡專員有合理理由相信有符合以下說明的作為或行為—(i)已經或正在(視屬何情況而定)由資料使用者作出或從事的；(ii)關乎個人資料的；及(iii)可能屬違反本條例下的規定的，則…專員可就有關的資料使用者進行調查，以確定該段所提述的作為或行為是否屬違反本條例下的規定。*」

5 見 2018 年 11 月 5 日標題為「國泰航空有限公司外洩客戶個人資料事件　私隱專員公署公正執法」的新聞稿 (https://www.pcpd.org.hk/tc_chi/news_events/media_statements/press_20181105.html)。

立法會會議

5. 2018 年 11 月 14 日，香港特別行政區立法會政制事務委員會、保安事務委員會和資訊科技及廣播事務委員會就該事件舉行聯席會議（**聯席會議**）。

6. 國泰在向聯席會議提交的書面文件[6] 中交代該事件，內容如下：—

「*香港特別行政區立法會（"立法會"）要求國泰航空有限公司（"國泰"）出席在二零一八年十一月十四日(星期三)舉行的政制事務委員會、資訊科技及廣播事務委員會及保安事務委員會的聯席會議。立法會並要求國泰在二零一八年十一月十二日正午前向聯席會議提交一份書面文件。書面文件的內容如下：*

國泰航空公司於二零一八年十月二十四日向香港私隱專員公署及香港證券交易所通告本公司有部分資訊系統遭未獲授權者入侵及部份客戶資料被取覽，我們同時亦就此事向香港警務處報案。隨後本公司亦馬上向其他有關監管機構通告這事，亦同時通知受影響的香港及世界各地乘客。

在詳細闡述事件的經過及交代已經採取的行動之前，國泰希望就是次事件向公眾表達深切的遺憾，及向受影響的乘客誠懇致歉。國泰重視與香港市民的關係，並致力自我改善，希望繼續獲得乘客的信心和信任。

在調查是次事件的過程中，我們首要考慮的重點是為受影響顧客提供準確及完整的整套相關資訊，並為我們受影響的乘客提供協助。國泰深明及尊重所有個人資料都需要受到保護，我們亦了解個人資料對每位客人都十分重要。國泰亦會嚴肅處理乘客因此次事件而產生的憂慮。在調查中的每一刻，我們都希望能夠更盡早提供有關此次事件的

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

資訊，但是由於調查工作艱巨複雜，較預期需時，故未能早日完成，就此鄭重向公眾致歉。

事件發生的情況說明

精密的網絡罪犯入侵國泰的系統使國泰及受影響的乘客都成為受害者。在發現可疑活動後，國泰即時聘請一家有國際領導地位的專家協助展開全面調查，以確定事件發生的情況及受影響資料的範疇。在調查的最初期，國泰已確認其航班運作及安全系統並沒有受到影響，飛行安全亦從未受到影響。國泰就此次事件的調查是專注於以下三個目標: (i) 調查、控制及補救; (ii) 確認那些資料曾被取覽及是否可以被黑客閱讀; 以及(iii) 確定每一位受影響乘客的個人資料類別及通知。調查結果達到這三個調查目標後，我們便馬上通知受影響的乘客及有關當局。

受影響的乘客及被取覽的資料

這次受到影響的乘客包括馬可孛羅會及亞洲萬里通會員，亦包括曾經乘坐國泰或國泰港龍航班的非會員乘客。根據我們的調查，全球大約有九百四十萬乘客受到是次事件的影響。

受到取覽的個人資料包括乘客姓名、國籍、出生日期、電話號碼、電郵地址、通信地址、旅行證件/護照號碼、身份証號碼、飛行常客計劃的會員號碼、顧客服務備註及過往的飛行記錄資料。每位受影響的乘客被不當取覽的資料都有所不同。據我們的分析顯示，大部份受影響的乘客他們被取覽的資料僅限於乘客姓名及電話號碼，或乘客姓名及電郵地址。

我們的調查亦顯示，我們處理付款資料的系統是具有適當的遮蓋功能，信用卡資料是受到保護的。是次事件中，並沒有一套完整的信用卡資料曾被取覽。但是有一小部分的信用卡號碼因為被錯誤輸入於並

非儲存信用卡資料的欄位曾被取覽，這類信用卡絕大部分是已過期的。

在調查中我們確認並沒有任何一位乘客及常客的資料被整套取覽，亦沒有任何乘客密碼外洩。

在調查的過程中，國泰聘請了一家網絡安全專家機構搜尋暗網及其他網站。根據至今的搜尋，我們沒有證據顯示任何被竊取的資料曾在這些網站上出現。我們亦會繼續進行這類搜尋。

給予乘客的協助

國泰深明全面及準確地了解每位受影響乘客被取覽的個人資料範圍及具體細節至為重要。 這樣才能確保在通知他們的時候，我們所提供的資料是整套、完備及具意義的。

國泰就事件在通知全球乘客上亦制定了一套全面的全球通知計劃，我們透過電郵及郵寄發送個人通知信件給每一位受影響的乘客，並在信件中清楚列明每位乘客所被取覽的資料類別。而就無法個別通知的乘客，我們亦於專屬網站 infosecurity.cathaypacific.com 上發佈了一份概括的通知。

除了個人化的通知，國泰亦設立了不同客戶服務渠道協助受是次事件影響的乘客，包括建立免費專屬顧客查詢熱線及專屬電郵地址 (infosecurity@cathaypacific.com)，讓乘客可查詢有關事件的的事宜。

以下的統計數據列出受影響乘客使用上述客戶服務渠道的情況：

客戶服務渠道	*截至二零一八年十一月十二日凌晨*
網站	*181,700 次網頁瀏覽*

通過顧客查詢熱線的查詢	*收到 5,031 個電話查詢*
通過網站的查詢	*收到 19,005 則查詢*
infosecurity@cathaypacific.com	
收到的電郵	*收到 5,622 封電郵*

國泰亦繼續向受影響乘客提供一個免費的身份監察服務 - IdentityWorks。此項服務由一家名為 Experian 的公司在不同地區(包括香港)提供。截至二零一八年十一月十二日凌晨，共有 50,271 位乘客登記使用該服務。

Experian 與許多世界各地行業領先公司、金融機構及政府機關都有合作。而我們的研究亦顯示他們在網絡(包括暗網)上搜索被未獲授權使用的個人資料方面的能力對受影響的乘客尤其寶貴。乘客可自由選擇是否使用該服務，而每位乘客在這項服務上可選擇他們希望受監察的個人資料類別。Experian 於二零一五年曾發生網絡安全事件，但 Experian 的個人信貸資料庫並沒有被取覽。該公司為持續努力改善安全，已實施全球網絡安全計劃，透過實施識別、保護、及偵測規格，進一步增強其安全性並提高應對網絡安全威脅的標準。Experian 持續達到全球保障資料及私隱的準測。

國泰資訊技術安全

國泰了解資訊技術安全至關重要。過去三年，我們投放了超過十億港元於資訊基建及資訊網絡安全上。國泰的資訊技術安全的任務是由一隊專家團隊負責，該團隊並沒有受到二零一七年的架構重組影響。他們負責監管及保障資訊技術安全的工作，並有行業領先的專家輔助及提供專業知識 。 我們深明隨著黑客手段愈趨精密和複雜，我們應對網絡安全威脅的反應亦需因時制宜，資訊技術保安的規劃上亦要不斷改良演變，包括強化壯大我們的資訊技術安全團隊以應付急速變化環境所帶來的挑戰。

為何調查時間這麼冗長？

我們對事件的調查及應對是分為三個階段 ，這三個階段是順序進行的，執行時間上亦時有重疊。這三個階段是 - (i) 調查、控制及補救; (ii) 確認那些資料曾被取覽及是否可以被黑客閱讀; 以及(iii) 確定每一位受影響乘客的個人資料類別及通知。

第一階段於二零一八年三月展開。當時國泰首次在系統中發現可疑活動跡象，我們馬上採取行動了解事件並堵截該等活動，並聘請了一家在行業上有領導地位的國際知名全球網路安全公司協助，調查事件情況及阻止事件繼續深化。在這調查階段，我們的系統仍然不斷地受到更多攻擊，其中三月、四月及五月尤為強烈。持續不斷的攻擊驅使我們把內部及外部的資訊技術安全資源集中放在控制及防範上。即使我們往後被成功攻擊的次數有所下降，但我們仍顧慮到系統會有可能受到新的攻擊，不敢鬆懈。

此後，持續的攻擊的範疇亦不斷擴大，使到我們在了解可能被取覽的資料範圍上，添加了不少挑戰，亦令到在第二階段的工作更冗長及複雜。

在第二階段，我們面對的兩大問題為：那些乘客資料被取覽或洩漏；以及，由於受影響的資料庫只是被局部取覽，該等資料是否可在國泰的資訊系統外被重建為可閱讀的格式，從而被黑客使用。要在這些問題上得出答案實在是十分困難及耗時，最終我們只可以在八月中旬才能找到答案。

在第三階段期間，我們工作的重點轉移至確認每一位受影響乘客被取覽資料的類別。我們希望給予每一位受影響乘客一個單一、準確及具意義的通知，而不是提供一個流於空泛且不具體的告示。直到十月二十四日，國泰才能完成確認每位受影響乘客所被取覽的個人資料。與

此同時，國泰亦為在回應乘客的查詢上作出了有效的安排 (詳見以上「給予我們乘客的協助」)。二零一八年十月二十四日，我們開始了向有關部門通佈的工作，我們亦在二零一八年十月二十五日開始通知受影響的乘客。

總括而言，國泰是次受到的攻擊既精密而且先進，受到影響的範疇涉及數個複雜的系統，調查涉及大量高度技術性的工作，在分析上耗時。而將被竊取的資料在進行確認、處理、及將該等資料連繫至個別乘客上的過程複雜，因此由首次發現事件到向公眾公佈事件之間的時間上因而延長。

……

最後，國泰重申我們非常重視我們在保護乘客個人資料上的責任，亦從此次事件中吸取了許多教訓。我們藉此再次就是次事件及因其而引起的任何憂慮向我們的乘客深表歉意。

國泰航空有限公司

二零一八年十一月」

7. 國泰主席在聯席會議開始時曾致辭[7]，重點如下：

「*…因為各位議員大多是我們的乘客，令我及在座國泰航空的同事此刻感到特別難受，我必須親自向您和香港大眾就今天討論的黑客入侵事件道歉。因為部分在座人士及香港市民的個人資料可能曾在我們的資訊系統中受到不當取覽或盜取…*

國泰航空和國泰港龍航空深明保障乘客的資料安全至為重要，我們責無旁貸。作為一間香港的航空公司，我們對是次事件影響眾多香港市民深表遺憾…

[7] 全文：https://www.legco.gov.hk/yr18-19/chinese/panels/ca/papers/caitbse20181114cb4-216-3-c.pdf

我希望借這個機會解釋國泰資訊系統的規模及複雜程度。我們在多個層面於香港甚至亞太區內均屬最大的資訊科技用戶。我們的系統包括 13 億個會被備份的文件、470 個資料庫、4,500 個伺服器、龐大的網絡、約 600 個應用程式，我們每日收發的電郵高達 450 萬封。值得留意的是，我們每個月亦封鎖及截退約16,000 個包含病毒的外部電郵。

這些事實並非藉口，而是希望讓各位能了解我們系統的複雜性。正因系統如此複雜，令我們未能適時實踐我們的初衷 — 為每一位受影響的乘客就其資料洩漏的情況提供真實，準確及個人化的說明…」

8. 截至本報告的發佈日期為止，專員就該事件共接獲 143 宗投訴及 176 宗查詢[8]。

[8] 投訴人及查詢者主要就其個人資料保安和通報的及時性表達不滿。

II. 該事件的相關事實及情況

9. 尋找和在下文詳列與該事件的相關事實及情況的準確性及敏感度對整個調查結果的影響至為重要，專員謹慎行事以確保其調查及調查結果是根據準確事實而作出，並確保所披露的事實不能用作損害國泰的資訊系統安全、航班運作及商業機密。

循規調查

10. 本循規調查是根據國泰對該事件的供認及陳述，以及在資料外洩事故通報、該公告、該新聞稿、聯席會議提供的資訊及回覆循規審查的偵訊而作出的。

11. 國泰於 2018 年 3 月 13 日「*首次在系統中發現可疑活動跡象*」，因而發現該事件。在向專員作出通報資料外洩事故前的七個月期間，國泰進行了「*內部調查*」及「*分析*」，採取了相關的補救行動以遏止該事件，並提升其資訊系統（**國泰資訊系統**）的保安。

12. 在循規調查的過程中，專員透過向國泰法律代表作出書面及口頭偵訊及溝通，以獲取及審閱該事件的證據和資訊。

13. 專員共耗五個月的時間以獲取國泰就該事件所提供必需及相關的資訊。在這段期間，國泰提供逾 10 次書面回覆，當中披露逾 2,200 頁的文件。專員亦接受國泰需時以提供所要求的資訊和文件的理由，因此批准所有延期回覆的申請。

14. 專員曾要求索取國泰在內部調查中聘請的網絡保安公司所撰寫的法證調查報告。不過，國泰表示該網絡保安公司是由其法律代表所聘請，並聲稱有關的法證調查報告是受法律專業保密權保護的。

15. 由於與該事件有關的國泰資訊系統規模龐大且複雜，專員遂行使《私隱條例》下的法定權力[9]，就該事件所涉的科技保安事宜尋求獨立專家作第二意見。

通知受影響乘客

16. 在發出該公告及該新聞稿後，國泰自 2018 年 10 月 25 日起，「*透過電郵及郵寄（只限有其聯絡資料的乘客）及透過專屬網站的概括通知*」，通知受影響乘客。國泰表示「*在信件中清楚列明每位乘客所被取覽的資料類別*」。

受影響乘客的類別

17. 國泰承認受影響乘客包括會員和非會員。會員包括亞洲萬里通[10]及馬可孛羅會[11]的會員，以及國泰的註冊用戶[12]；非會員包括曾經乘坐國泰航班的乘客。

18. 國泰的調查顯示，全球約 940 萬名乘客受該事件影響：會員和非會員的受影響乘客的數目分別約為 359 萬和 586 萬。國泰向專員提供一份超過 260 個國家／司法管轄區／地區受影響乘客分類的保密文件。

---

9 《私隱條例》第 43(1)條訂明：「*在符合本條例的規定下，專員可為任何調查的目的而 — (a)自他認為合適的人處獲提供他認為合適的資訊、文件或物品，及作出他認為合適的查訊；及(b)以他認為合適的方式規管本身的程序。*」

10 亞洲萬里通是國泰的獎勵計劃（於 1999 年 2 月推出），由亞洲萬里通有限公司營運及管理。會員可透過在不同旅遊及消閒範疇的日常消費賺取里數，包括航空、酒店、飲食、金融服務、零售和電子科技產品。

11 馬可孛羅會是國泰的飛行常客計劃，由國泰營運。馬可孛羅會旨為根據飛行常客的會籍級別提供不同禮遇，包括預辦登機手續、優先登機、額外行李限額及享用機場貴賓室。所有馬可孛羅會會員會自動成為亞洲萬里通會員。

12 註冊用戶指在國泰開立帳戶以享用國泰網上服務（包括網上預訂及預辦登機）的乘客。這項計劃於 2016 年 2 月推出，由國泰營運和管理。

受影響的個人資料

19. 國泰首先是在資料外洩事故通報及聯席會議中列出受該事件影響的個人資料的類別，專員其後再與國泰確認有關情況。現載列如下：

受影響的個人資料的類別	佔受影響乘客總數的百分比約數
(i) 姓名	100%
(ii) 航班編號及日期	61%
(iii) 稱謂	56%
(iv) 電郵地址	53%
(v) 會員號碼	38%
(vi) 地址	24%
(vii) 電話號碼	19%
(viii) 國籍	12%
(ix) 護照號碼	9%
(x) 出生日期	8%
(xi) 身份證號碼[13]	6%
(xii) 信用卡號碼[14]	0.004%
(xiii) 顧客服務備註[15]	不適用

表 1 – 受影響的個人資料的類別和佔受影響乘客總數的百分比約數

[13] 包括香港身份證號碼 (~243,000)、其他身份證號碼 (~310,000)，及其他旅遊證件號碼 (~52,000)，例如中國居民往來港澳通行證、因公往來港澳通行證、台灣居民來往大陸通行證、港澳居民來往內地通行證，及內地居民出入境證件。

[14] 國泰表示有 430 個信用卡號碼曾被取覽或查閱，而當中大部分（403 個號碼）已逾期。

[15] 國泰表示「顧客服務備註」包含在受影響系統內自由文本字段中的非結構化資料。不過，基於有關數據庫檔案的性質，有關資料是不能用以識別乘客身份的，國泰在公告中納入這項是純屬「*出於謹慎*」。

20. 由於外洩的資料是提取自多個數據庫的部分摘錄，而非單一數據庫的全部資料，因此國泰表示沒有乘客的個人資料被整套取覽或查閱。國泰亦表示沒有密碼外洩。專員對這些事實沒有爭議。

國泰的資訊保安

21. 國泰向專員提供其資訊科技部 2013 至 2018 年的組織架構作審閱[16]。

22. 在聯席會議中，國泰提供的書面文件表示：

> 「*國泰了解資訊技術安全至關重要。過去三年，我們投放了超過十億港元於資訊基建及資訊網絡安全上。國泰的資訊技術安全的任務是由一隊專家團隊負責，該團隊並沒有受到二零一七年的架構重組影響。他們負責監管及保障資訊技術安全的工作，並有行業領先的專家輔助及提供專業知識。我們深明隨著黑客手段愈趨精密和複雜，我們應對網絡安全威脅的反應亦需因時制宜，資訊技術保安的規劃上亦要不斷改良演變，包括強化壯大我們的資訊技術安全團隊以應付急速變化環境所帶來的挑戰。*」[17]

23. 國泰航空為國泰港龍管理及提供資訊管理服務[18]，而「*國泰港龍乘客的個人資料是儲存於*〔國泰資訊系統內〕」。專員審閱了國泰航空與國泰港龍之間的相關服務協議，並對這些事實沒有爭議。

24. 國泰主席在聯席會議的致辭中簡述國泰資訊系統的規模及複雜性：

---

[16] 為保障可能被用作損害國泰資訊系統安全的敏感資料，資訊科技部組織架構的詳情被略去。

[17] https://www.legco.gov.hk/yr18-19/chinese/panels/ca/papers/caitbse20181114cb2-222-2-c.pdf, 第 3 頁。

[18] 資訊管理服務包括應用程式牌照及維護、應用程式外判支援服務、應用程式支援資源、基建硬件、基建外判服務、基建軟件牌照及維護、資訊科技諮詢服務，以及網絡和電訊服務。

「*…我們在多個層面於香港甚至亞太區內均屬最大的資訊科技用戶。我們的系統包括 13 億個會被備份的文件、470 個資料庫、4,500 個伺服器、龐大的網絡、約 600 個應用程式，我們每日收發的電郵高達 450 萬封。值得留意的是，我們每個月亦封鎖及截退約 16,000 個包含病毒的外部電郵。*」[19]

受影響系統

25. 國泰表示，截至 2017 年 12 月，國泰資訊系統中逾 120 個系統載有個人資料，當中有四個系統受該事件影響（**受影響系統**）[20]，專員對此沒有爭議。

(i) 〔系統 A〕是一個客戶忠誠系統，用作「*處理和記錄會員的會籍資料*」。在該事件中，〔系統 A〕的一個數據庫受影響。

(ii) 〔系統 B〕是「*一個用作支援網上應用程式的共享後端數據庫*」。在該事件中，〔系統 B〕的一個數據庫受影響。國泰表示正將「〔系統 B〕*由一個數據中心遷移至新的數據中心*」，而〔系統 B〕的數據庫備份檔案（在該事件中被取覽或查閱）是「*儲存於生產伺服器(production server)以便遷移*」。

(iii) 〔系統 C〕是「*一個編纂報告的工具*」，而編纂哪項報告則視乎「*需滙出報告的數據庫*」。在該事件中，攻擊者透過〔系統 C〕取覽或查閱國泰顧客資訊系統（**客資系統**）內的個人資料。

(iv) 〔系統 D〕是「*一個暫時性的數據庫，讓亞洲萬里通會員換領非機票獎賞*」。〔系統 D〕的一個數據庫在該事件中受影響。

[19] 見註解 7

[20] 為保障可能被用作損害國泰資訊系統安全的敏感資料，受影響系統的詳情被略去。

26. 國泰表示它「*擁有及營運這四個系統*」。所有受影響系統是「*互斥及…互無關係的*」。

27. 國泰亦表示「*在維護〔受影響系統〕方面涉及第三方供應商*」，但沒有因此將個人資料轉移予服務供應商。專員審閱了國泰與第三方服務供應商之間的相關服務協議後，對國泰所提供的資料沒有爭議。

保安措施

28. 在循規調查的過程中，專員審視了國泰為保障國泰資訊系統內的乘客個人資料而採取的機構性和技術性保安措施，包括運作保安、網絡保安和存取控制。

29. 本報告略去敏感的保安措施，以保障國泰資訊系統免受進一步攻擊。

30. 國泰備有一套資訊科技政策，有關政策已上載至其內聯網。

國泰資訊系統的重要活動

31. 根據國泰在資料外洩事故通報中承認的事實及在循規調查中提供的回覆，國泰資訊系統在該事件中的重要活動如下：

日期/時段	**事件**
2014 年 10 月 15 日	在該事件發生後展開的內部調查揭示的「*國泰資訊系統遭未獲授權取覽的最早日期*」。「*攻擊者在〔系統 C 〕裝入鍵盤側錄惡意程式*」，以搜集帳戶憑證資料。
2016－2018 年	遷移數據中心的過程。
2017 年 5 月 7 日	國泰發現一宗國泰資訊系統被未獲授權的取覽或查閱事件，當中的最早入侵日期為 2016 年 9 月 7 日。根據國泰

	的說法，是次事件未有導致資料外洩。
2017 年 8 月	推出個人資料庫存計劃。
2018 年 3 月 13 日	國泰首次在其網絡偵測到一宗與暴力攻擊有關的可疑活動，而該攻擊導致約 500 名職員用戶被強制登出其帳戶，因而發現該事件。
2018 年 3 月 14 日	國泰展開其內部調查（網絡保安公司自 2018 年 3 月 22 日獲聘並協助調查）。
2018 年 3 月 31 日	「*偵測到透過〔系統 C 〕向〔客資系統〕作出查詢的攻擊活動*」。
2018 年 4 月 4 日	國泰「*發現存放於伺服器內的〔系統 B〕的數據庫備份檔案，並可能成為攻擊者的目標*」。
2018 年 5 月 4 日	「*攻擊者遙距進入國泰的網絡環境，並竊取〔系統 A〕的部分數據庫備份檔案*」。
2018 年 5 月 6 日	「*再發現涉及〔系統 C 〕的惡意軟件*」。
2018 年 5 月 7 日	國泰「*確認其部分載有乘客資料的資訊系統曾被未獲授權取覽*」。
2018 年 5 月 8 日	「*攻擊者進入〔系統 D 網站〕的管理員平台取覽顧客的換領和交易資料，並匯出數據庫備份*」。
2018 年 8 月 28 日	「*遏止及攔截了一次試圖攻擊，沒有任何資料被取覽*」。

表 2 – 國泰資訊系統的重要活動

指出的肇事原因

32. 國泰表示，其內部調查鑑定「*未獲授權取覽是該事件的直接起因*」，並懷疑有關的取覽或查閱行為是由「*兩組明顯的攻擊者*」進行的。

第一組攻擊

33. 國泰表示「*最早的證據顯示涉嫌的第一組攻擊活動發生於 2014 年 10 月 15 日*」，當中發現〔系統 C〕被裝入一個鍵盤側錄惡意程式[21]，以搜集取帳戶憑證資料。然而，國泰未能鑑定最初入侵國泰資訊系統的路徑。

透過虛擬私有網絡以有效的帳戶憑證資料進入國泰資訊系統

34. 攻擊者利用所偷取的有效帳戶憑證資料，透過虛擬私有網絡（繞過虛擬私有網絡的限制）進入國泰資訊系統，並取覽或查閱當中的個人資料。另一方面，攻擊者在國泰的網絡中橫向移動[22]，進一步放置竊取憑證資料的工具以提取系統的領域憑證資料。攻擊活動於 2018 年 3 月 22 日停止。

第二組攻擊

(1) *初期入侵*

35. 攻擊者利用一個連接互聯網的伺服器（**該伺服器**）的漏洞（**該漏洞**）使其可略過認證並獲取管理權限。該漏洞亦讓攻擊者能夠、而攻擊者亦確實在國泰資訊系統內橫向移動，並裝入惡意軟件和竊取憑證資料的工具。在事發時（即未獲授權取覽或查閱發生時），存在於國泰的該伺服

[21] 鍵盤側錄惡意程式是一程式，用作擷取輸入裝置的活動。攻擊者會利用鍵盤側錄惡意程式去擷取輸入到電腦系統的個人資料。

[22] 橫向移動是網絡攻擊者所用的一種技術，在網絡內逐漸移動以搜尋其目標（例如：數據）。

器的該漏洞自 2007 年已在互聯網內被廣泛公佈[23]。國泰表示「*最早的證據顯示涉嫌的第二組攻擊發生於 2017 年 8 月 10 日*」。

36. 該伺服器於 2017 年 3 月建立時的應用程式屬 3.0 版本。國泰表示未能提升該應用程式至最新版本的原因是因為它與一個空中巴士手冊應用程式[24]不兼容，因此國泰選擇使用該應用程式的一個較早期的版本。

37. 國泰聲稱在 2017 年 3 月正式使用該伺服器前，曾進行漏洞掃描以作為運作驗收測試的一部分，但沒有發現該漏洞。國泰聲稱它在選擇及繼續使用 3.0 版本時，並無察覺到該漏洞。

38. 國泰進一步聲稱因為「*沒有公開可獲取的病毒識別碼*」，在該伺服器所安裝的抗惡意程式和端點保護應用程式均未能偵測到相關的惡意軟件及工具。

(2) *暴力攻擊*

39. 2018 年 3 月 13 日，國泰在其網絡首次偵測到一宗與暴力攻擊[25]有關的可疑活動，而該攻擊導致約 500 名職員用戶被強制登出其帳戶，因而發現該事件。在察覺有關的可疑活動後，國泰在網絡保安公司的協助下展開內部調查。

40. 國泰承認它「*未能確定在這次攻擊中是否有帳戶遭入侵*」。

(3) *透過虛擬私有網絡以有效的帳戶憑證資料進入國泰資訊系統*

41. 攻擊者利用所偷取的帳戶憑證資料，透過虛擬私有網絡進入國泰資訊系統。最後所知的攻擊活動發生於 2018 年 5 月 11 日。

---

[23] 該漏洞存在於該伺服器的應用程式 3.0 版本。

[24] 空中巴士手冊應用程式載有記錄空中巴士起飛和機隊表現數據的手冊及發送內容至使用者的平板電腦。

[25] 暴力攻擊是嘗試所有可能性以破解加密或認證系統的技術。

帳戶憑證資料

42. 國泰承認共有 41 個有效的帳戶憑證資料被竊，並用作為透過虛擬私有網絡進入其網絡。被竊的帳戶憑證資料涉及不同類型的帳戶，包括管理員、使用者、網絡及服務帳戶。攻擊者透過在國泰資訊系統內植入不同的惡意軟件及工具，進一步搜集憑證資料，以便在國泰資訊系統內橫向移動。

資料保留

43. 國泰備有相關政策和指引，規定資料不應保留超過達致收集目的所需的時間。

會員的個人資料

44. 根據國泰的資料保留常規，如會員連續七年被標示為「*不活躍*」[26]，國泰便會刪除其個人資料。

非會員的個人資料

45. 非會員的個人資料會由完成交易日期起計保留七年。

46. 如受影響乘客（會員及非會員）使用〔系統 B〕內的網絡應用程式，其部分資料亦可能存在於〔系統 B〕。國泰表示，〔系統 B〕是一個含有多個列表的數據庫，不同的網絡應用程式從相關的列表中提取所需資料，而資料的保留期間則因應各應用程式而有所不同。

[26] 國泰在回覆循規調查過程中的提問時解釋，當註冊用戶要求終止其帳戶，或被發現擁有重複帳戶，便會被標示為「*不活躍*」。例如，馬可孛羅會會員在下述情況會被標示為「*不活躍*」：如果(a) 會員要求終止其馬可孛羅會及／或亞洲萬里通會籍；(b) 會員被發現擁有馬可孛羅會（自動成為亞洲萬里通會員）的重複會籍； (c) 會員在連續 12 個月內未能保持最低級別的最低旅遊要求及沒有繳付會費；亞洲萬里通會員在下述情況會被標示為「*不活躍*」：(a) 會員要求終止其亞洲萬里通及／或馬可孛羅會會籍； (b) 會員被發現擁有重複會籍；或 (c) 會員在連續 36 個月內沒有累積任何亞洲萬里通積分。

亞洲萬里通會員的個人資料

47. 亞洲萬里通會員的資料（包括基本個人資料，例如姓名和聯絡資料）可能會暫時顯示於〔系統 D〕，以供會員換領非機票類的會員獎賞。有關資料只會在交易時顯示，其後隨即轉移至〔系統 A〕，而該系統的保留時限適用於這類個人資料。

補救措施

48. 國泰聲稱在察覺到該事件後，在網絡保安公司的協助下，已採取一系列的補救行動，遏止該事件和攔截攻擊者[27]。

[27] 為保障可能被用作損害國泰資訊系統安全的敏感資料，補救行動的詳情被略去。

III. 法律事宜及規管框架

《私隱條例》

49. 個人資料私隱是受《私隱條例》保障的。《私隱條例》是以原則為本及科技中立，在制定時曾參考 1980 年經濟合作與發展組織的私隱指引及 1995 年歐盟的資料保障指令。雖然個別行為可能由《私隱條例》明確規管，但其核心條文扼要概述於《私隱條例》附表 1 的六項保障資料原則中。保障資料原則旨在制定框架，規管處理由收集到銷毀個人資料的整個生命周期。在大多數情況下，違反保障資料原則並不構成刑事罪行，但當專員在調查後發出執行通知，指示違規一方糾正該項違反及採取行動以防止該項違反再發生，而違規一方沒有依從執行通知，即屬犯罪。違反保障資料原則亦可成為民事訴訟的基礎，無論專員有否發出執行通知，受屈一方可根據《私隱條例》第 66 條向違規一方申索補償。

規管方法

50. 專員的規管方法是與普通法的法定詮釋一致，尤其是香港法例第 1 章《釋義及通則條例》的規定。該條例第 19 條規定條例「*必須當作有補缺去弊的作用，按其真正用意、涵義及精神，並為了最能確保達致其目的而作出公正、廣泛及靈活的釋疑及釋義*」。終審法院在 *The Medical Council of Hong Kong v David Chow Siu Shek* [2000] 2 HKLRD 674 一案解釋了這個「公正、廣泛及靈活」的方法。

51. 專員亦時刻留意公認的「反荒謬的推定」原則的法定詮釋，正如在 *Bennion on Statutory Interpretation* （第六版，Butterworths）一書中的解釋。

52. 專員作為公平的執法者，除了應用一致的法律詮釋外，亦會恰當地和有必要地考慮實際情況和社會價值的轉變，例如本地及海外司法機關的裁決和觀點、瞬息萬變的環球私隱形勢、演變中的數碼範式和數據驅動經濟、不斷發展的資訊及通訊科技、相關專家的觀點，以及所有持份者、機構和個人的相關期望。

個人資料

53. 根據《私隱條例》第 2(1)條，「*個人資料*」是「*指符合以下說明的任何資料—*

(a) 直接或間接與一名在世的個人有關的；
(b) 從該資料直接或間接地確定有關的個人的身分是切實可行的；及
(c) 該資料的存在形式令予以查閱及處理均是切實可行的。」

資料當事人

54. 上述「*在世的個人*」在法律上亦指《私隱條例》第 2(1) 條的「*資料當事人*」。

資料使用者

55. 《私隱條例》，包括保障資料原則，旨在規管資料使用者的行為及作為。根據《私隱條例》第 2(1)條，資料使用者指「*獨自或聯同其他人或與其他人共同控制該資料的收集、持有、處理或使用的人*」。

資料外洩事故

56. 資料外洩事故一般指資料使用者持有的個人資料懷疑或實際外洩；資料遭受遺失、未獲准許的或意外的查閱、處理、刪除或使用的風險；資料

庫內的個人資料被黑客未獲授權取覽或查閱及轉移；不當棄置含有個人資料的文件等。

資料外洩事故通報

57. 目前，《私隱條例》並沒有強制規定資料使用者必須向專員或相關資料當事人通報資料外洩事故。然而，作為良好的行事方式，專員仍鼓勵資料使用者就資料外洩事故作出通報，並出版了《*資料外洩事故的處理及通報指引*》[28]。

資料保安

58. 該事件主要涉及資料保安，亦正是本循規調查的關鍵所在。

59. 隨著為顧客提供的網上服務不斷增加，加上透過網上服務收集、儲存或傳輸個人資料的情況越見普及，資料使用者有責任確保資訊系統安全，並保障在網上收集、儲存及傳輸的個人資料時免受黑客或非預期的使用者等人士的未獲授權或意外地查閱或刪除。

60. 保障資料第 4(1)原則 — 個人資料的保安訂明：

> 「 *須採取所有切實可行的步驟，以確保由資料使用者持有的個人資料（包括採用不能切實可行地予以查閱或處理的形式的資料）受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響，尤其須考慮—*
>
> *(a) 該資料的種類及如該等事情發生便能做成的損害；*
>
> *(b) 儲存該資料的地點；*
>
> *(c) 儲存該資料的設備所包含（不論是藉自動化方法或其他方法）的保安措施；*

[28] https://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/DataBreachHandling2015_c.pdf

(d) *為確保能查閱該資料的人的良好操守、審慎態度及辦事能力而採取的措施；及*

(e) *為確保在保安良好的情況下傳送該資料而採取的措施。*」

61. 根據《私隱條例》第 2(1)條，「*切實可行*」指「*合理地切實可行*」。

62. 上述保障資料第 4(1)(a)原則所述的「*損害*」測試，需考慮資料使用者就其持有的個人資料而採取的保安措施是否與資料的敏感程度及如被未獲授權或意外的查閱或刪除資料所導致的損害相稱。

63. 此外，保障資料第 4 原則只規管個人資料的儲存或傳輸方式，而非個人資料的使用情況。有關個人資料的使用方式由保障資料第 3 原則所規管。

資料保留

64. 資料使用者在收集個人資料後，須考慮應保留資料多久。因為不必要地或過長地保留個人資料，將無可避免地造成或增加數據安全的風險。

65. 保障資料第 2(2)原則訂明：

「*須採取所有切實可行的步驟，以確保個人資料的保存時間不超過將其保存以貫徹該資料被使用於或會被使用於的目的（包括任何直接有關的目的）所需的時間。*」

66. 保障資料第 2(2) 原則曾於 2012 年修訂，澄清了資料使用者只須採取所有合理地切實可行的步驟以依從這項資料保留原則的要求。迄今該原則被詮釋為資料使用者有絕對責任，確保個人資料不會被保留超過所需的時間。

IV. 觀點，調查結果及違例事項

個人資料；資料當事人；資料使用者；資料外洩事故

67. 根據國泰對該事件的供認及陳述，以及在資料外洩事故通報、該公告、該新聞稿、聯席會議提供的資訊及回覆循規審查及循規調查的偵訊而提供的文件及資料，專員認為下述事宜在該事件的關鍵時間符合《私隱條例》（包括附表）的釋義，並對有關事宜沒有爭議：

(i) 涉及和受影響的資料是個人資料；
(ii) 受影響乘客（會員及非會員）是資料當事人；
(iii) 國泰航空及國泰港龍是資料使用者；及
(iv) 發生了資料外洩事故。

受影響乘客

68. 專員的調查結果顯示在關鍵時間的受影響乘客包括曾經乘坐國泰航班的乘客、亞洲萬里通和馬可孛羅會的會員，以及國泰的註冊用戶。

向專員作出資料外洩事故通報

69. 儘管《私隱條例》沒有規定資料使用者須向專員及資料當事人通報資料外洩事故，亦沒有規定資料使用者須在指定時間內作出通報，但國泰已於 2018 年 10 月 24 日向專員通報該事件，並採取步驟通知資料當事人（就該事件，即為受影響乘客）。專員認為國泰沒有違反《私隱條例》的規定。

通知受影響乘客

70. 《私隱條例》在沒有法定要求國泰須就該事件通知受影響乘客的情況下，專員欣悉國泰在這方面的努力。國泰通知受影響乘客的方式包括公

告、經由電郵或郵寄發送個人通知信件、在專屬顧客網站發佈概括通知、及設立專屬顧客查詢熱線及專屬電郵地址。國泰解釋直至 2018 年 10 月 25 日才作出通知是由於「*國泰深明全面及準確地了解每位受影響乘客被取覽的個人資料範圍及具體細節至為重要。這樣才能確保在通知他們的時候，我們所提供的資料是整套、完備及具意義的*」及「*國泰是次受到的攻擊既精密而且先進，受到影響的範疇涉及數個複雜的系統，調查涉及大量高度技術性的工作，在分析上耗時。而將被竊取的資料在進行確認、處理、及將該等資料連繫至個別乘客上的過程複雜，因此由首次發現事件到向公眾公佈事件之間的時間上因而延長*」[29]。

71. 考慮到國泰首次在系統中發現可疑活動跡象（即發現該事件）七個月後才發出通知以及所提供的原因，專員認為<u>國泰即使並沒有違反任何《私隱條例》的法定要求，當初亦應能在發現可疑活動時立即通知受影響乘客，並建議他們提前採取適當的步驟，以符合他們的合理期望</u>。

資料保安

72. 該事件的主要關注點及所指的肇事原因是不知名的攻擊者繞過或攻破國泰資訊系統的網絡保安及／或利用該系統存在的漏洞進行入侵。專員嚴謹地審視了國泰資訊系統的保安政策及措施。

73. 專員注意到保障資料第 4 原則並沒有要求國泰對個人資料的保安有絕對的責任。

74. 行政上訴委員會[30] 在行政上訴案件第 8/2008 號總結：

「*…資料使用者只須採取所有切實可行的步驟，保障個人資料免受未獲准許的或意外的查閱。資料使用者須採取的步驟對他來說必須是切實可*

[29] 見註解 6

[30] 根據香港法例第 442 章《行政上訴委員會條例》於 1994 年 7 月成立的獨立法定機構。行政上訴委員會會就上訴人因為不服某些行政決定而提出的上訴，進行聆訊並作出裁決。這些上訴必須是在委員會的仲裁範圍內，當中包括《私隱條例》。

*行的。在解釋保障資料第 4 原則和決定資料使用者應採取甚麼步驟以保障個人資料時，尤其須考慮「該資料的種類及能造成的損害」（見保障資料第 4 原則(a)段）。因此專員認為**所採取的步驟必須「與資料的敏感程度和有關資料被意外的或未獲准許的查閱而導致的損害相稱」**是正確的。」*[31]

〔後加粗體以作強調〕

75. 在較近期的案件（行政上訴案件第 70/2016 號 ），行政上訴委員會確定：

「〔《私隱條例》〕*保障資料第 4 原則的法律要求是資料使用者須採取所有合理地切實可行的步驟，以確保資料當事人的個人資料受保障。**所有合理地切實可行的步驟並非要求處理資料當事人個人資料的方法完美或可隔絕風險。所採用的每個系統／步驟可能有些已知或未知的缺點，只要在個案的情況下屬合理地切實可行的步驟，這步驟便不會受到**〔**《私隱條例》**〕**保障資料第 4 原則的質疑。**」*[32]

〔後加粗體以作強調〕

「合理地切實可行」的步驟

76. 鑑於行政上訴委員會的解釋及規管方法，專員理解資料使用者須採取的步驟在不同個案中都不盡相同，亦須考慮一系列因素，包括資料的數量、種類及敏感程度、資料外洩事故可能導致的傷害及損失、企業管治及機構性措施，以及對如國泰這類機構[33]所預期的標準及應合理地具備的技術政策、運作、控制及其他保安措施。此外，資料外洩事故後所採取的步驟（例如：通知相關人士）及未來的行動（例如：保安預防措施）亦在考慮之列。

---

31 https://www.pcpd.org.hk/tc_chi/enforcement/decisions/files/AAB_8_2008.pdf, 第 36 段

32 https://www.pcpd.org.hk/tc_chi/enforcement/decisions/files/AAB_70_2016.pdf, 第 51 段

33 國泰提供定期客貨運服務往來 50 多個國家及超過 200 個地區。

77. 專員亦參考了海外司法管轄區如何應用「*合理地切實可行*」的步驟，以確保個人資料的安全[34]。《通用數據保障條例》第 32 條表明[35]，資料控制者及處理者須實施適當的技術性及機構性措施，以確保有足夠的保安水平以對應相關風險。

78. 專員瞭解網絡攻擊越趨普遍和複雜，而且「*合理地切實可行*」的步驟並非詳盡無遺的，因此專員在循規調查時的評估是採用整體方式來衡量。

(1) *未能識辨該漏洞及利用該漏洞的行為*

79. 國泰表示攻擊者最初成功入侵國泰資訊系統是利用存在於該伺服器的該漏洞。國泰聲稱它在 2017 年 3 月建立該伺服器時，曾進行漏洞掃描，但沒有發現該漏洞。國泰進一步表示，它曾對該伺服器的復原影像再次進行漏洞掃描，但仍然沒有發現該漏洞。

80. 專員發現該漏洞已於 2007 年在互聯網內被廣泛公佈，在關鍵時間並非鮮為人知。專員曾對發佈常見漏洞的相關網站進行研究，所有搜尋結果均輕易地識辨該漏洞。此外，專員發現國泰所使用的漏洞掃描工具已具有偵測該漏洞的病毒識別碼，有關的病毒識別碼已於 2013 年公佈。這反映國泰若然當時有效地利用其漏洞掃描工具的功能是可以及時識辨所有已知的漏洞。

81. 專員認為**國泰未能識辨一個廣為人知及可被加以利用的保安漏洞（即上文第 35 段所指的該漏洞），亦未能識辨利用該漏洞的行為，同時沒有採取合理地切實可行的步驟在建立該伺服器時進行適當的部署**。

---

[34] 包括澳洲資訊專員公署的 “Guide to securing personal information” (https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-securing-personal-information.pdf)，DonateBlood.com.au 資料外洩事故調查報告 (https://www.oaic.gov.au/resources/privacy-law/commissioner-initiated-investigation-reports/donateblood-com-au-data-breach-australian-red-cross-blood-service.pdf)，以及 Federal Trade Commission v AshleyMadison.com (https://www.ftc.gov/enforcement/cases-proceedings/152-3284/ashley-madison)等。

[35] 見 https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en 以取得更多資料。

(2) *進行漏洞掃描相距的時間寬鬆*

82. 國泰在 2017 年 3 月正式使用該伺服器前曾進行漏洞掃描。儘管國泰安排每年進行漏洞掃描工作，但在攻擊者利用該漏洞並入侵國泰資訊系統的期間，國泰並沒有進行有關掃描。專員認為，由於國泰資訊系統的規模龐大，並載有大量敏感的個人資料，而**國泰只為該伺服器每年進行一次漏洞掃描，就有效保障國泰資訊系統以面對不斷變化的數碼威脅的做法屬流於表面及過份鬆懈**。

(3) *將該伺服器的管理員控制台埠曝露於互聯網*

83. 未被偵測的該漏洞讓攻擊者能夠及有機會存取該伺服器的管理員控制台及網絡管理界面。這項問題應可在安裝該伺服器時，透過修改伺服器的配置而解決，令管理員控制台埠只限獲授權人士從內部網絡進入，而不是曝露於互聯網。然而，該伺服器的管理員控制台埠在關鍵時間是可以從互聯網進入，因而為攻擊者開啟一扇大門。

84. 專員認為國泰應根據保安強化原則限制攻擊面，即限制可用於管理和設定該伺服器的管理員控制台埠，使其不能從互聯網直接進入，以有效降低該漏洞被利用的風險。

85. 專員認為**國泰沒有採取合理地切實可行的步驟，避免該伺服器的管理員控制台埠曝露於互聯網，因此導致為攻擊者開啟一個入口**。

(4) *未有提供多重認證予所有遙距使用者*

86. 國泰的內部調查顯示，攻擊者涉嫌透過初次入侵國泰資訊系統，植入惡意軟件及工具，以搜集帳戶憑證資料。他們以偷取得的帳戶憑證資料[36]，假裝合法帳戶並透過虛擬私有網絡進入國泰資訊系統，取覽或查閱系統內的個人資料。

[36] 根據國泰的調查，共有 41 個帳戶憑證資料被盜。

87. 國泰聲稱已採取多重方法，對透過虛擬私有網絡進入國泰資訊系統加以控制[37]。遙距進入國泰資訊系統是需要雙重認證，以避免他人使用偷來的憑證資料。但在該事件發生時，這項管控措施只適用於資訊科技支援小組，而不包括所有遙距使用者。國泰聲稱「*…由於選用的雙重認證方案持續不穩定，又欠缺適當的本地支援作補救措施，全面應用於所有遙距使用者並不切實可行…*」。專員認為國泰應以更正面及主動的態度對待乘客的個人資料私隱。

88. 在循規調查的過程中，沒有證據顯示國泰充分利用其特權身份管理系統，並以多重身份認證作支援，限制和嚴格控制針對國泰資訊系統特權的提升[38]。

89. 專員注意到在該事件後，國泰於 2018 年 7 月決定更改有關的認證方案，並擴展其應用至所有遙距使用者。

90. 在考慮到遙距存取國泰資訊系統的需求非常高，專員認為有限的遙距存取管控措施（即只應用雙重認證予資訊科技支援小組）對保障系統沒有成效，必需要有穩健安全的遙距存取機制。專員認為**國泰應對涉及存取國泰資訊系統內個人資料的所有遙距使用者實施有效的多重身份認證**。

(5) *為方便遷移數據中心而曝露未經加密的數據庫備份檔案*

91. 循規調查顯示，國泰在 2016 至 2018 年期間遷移一個數據中心時，兩個受影響系統（〔系統 A 及 B〕）的生產伺服器內為遷移程序而準備的數據庫備份檔案並沒有加密。國泰解釋，把數據庫備份檔案儲存於生產伺服器是便利遷移程序的最切實可行方法，可以縮減所需的遷移時間[39]，並容許較快的復原和後退時間。

---

[37] 包括雙重認證、 防止或限制未獲授權進入虛擬私有網絡的措施，以及採用存取控制清單和活動目錄，管理透過虛擬私有網絡進入許可的應用程式。

[38] 例如：管理員特權以管理伺服器。

[39] 這包括減少應用程式停機時間以配合國泰的全天候運作、降低對國泰業務運作的影響，及確保符合遷移數據中心的時間表。

92. 專員認為基於所涉個人資料的敏感程度，國泰在建立數據庫備份檔案前應充分評估保安風險及採取恰當的處理資料方式，包括為數據轉移程序選擇適當的數據管理方法、加密靜態的數據庫備份檔案，以及限制所需的資料。這些措施可以有效地減低攻擊者在入侵國泰資訊系統時的損害。專員認為**國泰在沒有採取有效的保安管控措施下，不應為了方便遷移數據中心而建立未經加密的數據庫備份檔案，因而導致受影響乘客的個人資料曝露予攻擊者**。

(6) *欠缺成效的個人資料庫存*

93. 國泰確認在該事件發生之前，並沒有中央個人資料庫存，以記錄儲存於國泰資訊系統內所有乘客的個人資料。國泰於 2017 年 8 月開始個人資料庫存計劃，但國泰聲稱由於所涉系統數目眾多、過程複雜和耗時，因此在該事件發生時該中央個人資料庫存尚未落實。在該事件發生時，缺乏一個個人資料庫存以涵蓋所有載有個人資料的系統，嚴重削弱國泰資料管治的有效性。

94. 專員認為，基於國泰資訊系統規模及所持有的個人資料數量和敏感程度，**國泰應建立有效的個人資料庫存以涵蓋所有載有個人資料的系統**。

(7) *未從過往的保安事故汲取教訓*

95. 根據一個較早前的保安事故報告，國泰曾於 2017 年 5 月於國泰資訊系統發現一宗未獲授權取覽或查閱事件，並採取相應的補救措施作出補救。專員認為，國泰應從之前的事故汲取教訓，透過全面檢視及評估整個網絡的保安風險改善事故管理，包括加強保護整個資訊基建和系統（例如：檢視及更新保安工具的功能、檢視及對高風險的系統和裝置再進行保安測試等），這些措施可以減低發生類似事故的風險。專員認為**國泰對風險的警覺性低，在 2017 年的保安事故發生後沒有採取合理地切實可行的步驟減低國泰資訊系統被植入惡意軟件及入侵的風險**。

(8) *資訊科技部架構重組和縮減人手*

96. 在循規調查的過程中，專員亦審視了國泰資訊科技部的組織架構（為保障國泰的保安而略去有關詳情）。專員認為**沒有足夠證據顯示資訊科技部的架構重組是導致該事件的原因**。

97. 鑑於所有涉及個人資料保安的相關情況，專員認為**國泰在漏洞管理、採用有效的技術保安措施，以及資料管治方面，沒有採取所有合理地切實可行的步驟，以保障受影響乘客的個人資料免受未獲授權的取覽或查閱，違反了《私隱條例》附表 1 的保障資料第 4(1)原則**。

資料保留

不必要地保留亞洲萬里通會員計劃申請者的香港身份證號碼

98. 國泰承認，自亞洲萬里通會員計劃推出以來，共向會員計劃的申請者收集了約 24 萬個香港身份證號碼，用作核實身份之用。這核實身份措施已於 2005 年停止，而申請表（網上及紙張）亦已於當時修訂。然而，這些已收集的身份證號碼卻被保留超過 13 年。**專員認為國泰在沒有合理原因的情況下，沒有採取所有合理地切實可行的步驟，確保受影響乘客的香港身份證號碼的保留時間不超過達致已廢除的核實身份的目的，違反了《私隱條例》附表 1 的保障資料第 2(2)原則**。

V. 執法行動

99. 根據《私隱條例》第 50(1)條，專員在完成一項調查後，認為有關的資料使用者正在或已經違反條例的規定，專員可向該資料使用者送達書面通知，指示該資料使用者糾正該項違反，以及（如適當的話）防止該項違反再發生。

100. 專員認為國泰違反了《私隱條例》附表 1 的保障資料第 4(1) 及 2(2) 原則，因此依據《私隱條例》第 50(1)條向國泰送達執行通知，指示國泰：

(1) 聘請獨立的資料保安專家徹底檢修載有個人資料的系統，務求該些系統沒有已知的惡意軟件及漏洞；

(2) 為所有會存取載有個人資料的國泰資訊系統的遙距使用者實施有效的多重身份認證，並承諾定期檢視遙距存取的權限；

(3) 定期[40]及在伺服器及／或應用程式有重大變更／新開發時，在伺服器及應用程式層面進行有效的漏洞掃描；

(4) 聘請獨立的資料保安專家定期[41]對國泰的網絡的保安進行檢視／測試；

(5) 制定清晰的資料保留政策，訂明每個系統內的乘客資料的保留期限，即不超過將其保存以貫徹該資料被使用於的目的，並承諾實施有效措施以確保有關職員獲明確告知政策內容及政策獲有效執行；

(6) 由執行通知的日期起計六個月內，或立即（如已採取補救措施）提供文件證明，證明已完成上述第 (1)至 (5)項；

(7) 從所有系統徹底銷毀亞洲萬里通會員計劃收集的所有不必要的香港身份證號碼（不論任何形式）；及

[40] 為保障可能被用作損害國泰資訊系統安全的敏感資料，有關的時段詳情被略去。
[41] 同上

(8) 由執行通知的日期起計三個月內，或立即（如已採取補救措施）提供由獨立專業第三方發出的證書，證明已完成上述第(7)項。

VI. 評論

101. 由於資料外洩事故不斷上升且越趨複雜，企業要維持其競爭力，在保障顧客的個人資料安全方面，履行責任之餘，面對的壓力也不斷增加。首要而言，它們必須遵從保障個人資料私隱的法例。

102. 雖然網絡攻擊本身可能屬刑事罪行而受到其他法律規管，與此同時企業在部分情況下亦不能控制這類攻擊，但《私隱條例》的要求是機構須採取合理地切實可行的步驟，確保個人資料的安全，以應付可能出現的資料外洩事故。理所而言，需要採取的步驟則會因應每宗個案的事實和情況而定。

103. 妥善保障顧客的個人資料安全及不可將之保留超過所需期限，這些法定責任毋須再作闡釋；更遑論企業是從資料的擁有者，即顧客的手上收集資料，卻無疑地隨即視之為資產，並設法從中取得利益。

104. 然而，即使個人資料不像其他動產（例如鈔票）或不動產般屬有形的資產，亦不足以免除企業沒有妥善地保護資料及沒有在達致有關目的而不再需要該資料時徹底銷毀資料的責任。顧客（資料當事人）及監管機構合理地期望企業能擁有一個完備、有效及可行、能適切企業的規模與需要、並可全面實施的私隱循規政策和計劃，以落實法例要求。

105. 從歐盟於 2018 年 5 月實施的《通用數據保障條例》的例子中，可以見到良好的數據管理、管治或問責的概念已被很多司法管轄區納入為新的法例和法規。在香港，儘管類似的問責原則仍未立法規管，但香港的企業應在這數據驅動經濟的年代作好準備，採納積極的數據管理作為企業的數碼價值、道德和責任，把法律規定轉化為風險為本、可驗證和執行的企業實務及管控措施，以應對環球就數據私隱規管的轉變。同時，企業亦應落實最新的數碼化及全球化企業模式，並確保其資料保障屬可持續性及可信賴的。

106. 尤為重要的是，不論資料使用者、資料控制者或處理者的規模大小，皆不能低估或輕視資料當事人交託的信任。

107. 自 2014 年以來，專員一直倡議所有機構採納以責任為本的私隱管理系統作為企業管治的一部分。個人資料私隱保障應是董事會會議的常設事項，而不應只交由資訊科技部門或人員負責。對此，專員亦已向不同的公私營機構提供實施私隱管理系統的指引和工具[42]。

108. 專員希望機構能珍惜透過尊重及保障個人資料私隱的權利而從資料當事人及監管機構獲取得來不易的信任。個人資料私隱的權利不單是香港法律所賦予的、亦是公眾所期望的基本人權。專員期許機構能透過尊重及保障個人資料私隱，從而發展出迎合 21 世紀的企業數碼責任，以助培育正確的私隱文化。

－完－

[42] 見，例如：「私隱管理系統 最佳行事方式指引」(2018 年 8 月，第一修訂版) (https://www.pcpd.org.hk/pmp/files/pmp_guide2018.pdf)