國泰航空公司

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
二零一八年十一月十四日(星期三) 聯席會議

國泰航空有限公司對二零一八年十一月五日信件中問題的回應

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、保安事務委員會的聯席會議。立法會亦要求國泰在二零一八年十一月十二日正午前書面回應莫乃光議員所準備的問題。書面回應內容如下：

一、 國泰表示於三月發現其資訊系統出現可疑活動後，五月確認乘客個人資料外洩，請告知（i）當初三月時是如何得知系統出現可疑活動，監察系統是以甚麼方式偵測可疑或入侵活動；（ii）可疑活動出現的時間以及資料庫/系統是否遭受持續攻擊，如是，受到攻擊的持續時間為何；（iii）及後五月又如何確認若干乘客個人資料外洩的詳情？

於二零一八年三月，國泰首次在系統中發現與攻擊相關的可疑活動跡象。最初期，我們唯一掌握到的證據是該等可疑活動對使用帳戶的暴力攻擊。在此階段，國泰進行初步評估，並在初步分析之後，聘請了一家在國際領導地位的網路安全公司協助，展開全面調查。國泰針對當時已知的可疑活動馬上採取堵截，並展開內部調查。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。於五月初，鑑識證據確認資料曾被未經授權取覽及/或洩露。此乃事件的第一階段。

在第二階段，我們的工作繼續專注於被取覽的乘客資料上。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。

二、 早前，國泰給每一位受影響的乘客發出個人化的電郵，內容描述每一位乘客被不當取閱過的資料。請問國泰是否肯定，電郵描述以外的乘客資料沒有被不當取閱？

就每一位我們已經發送電郵的受影響乘客，我們已經確認其被取覽的所有個人資料類別。因此，發送給每一位受影響乘客的電郵應已包含該乘客被取覽的所有個人資料類別。

三、 是否國泰所有資料庫均有查詢日誌功能（特別是今次受影響並管有乘客資料的資料庫/系統）？

國泰所有資料庫及資料庫伺服器均在運作系統及資料庫的層面上配備了日誌功能。

四、 如國泰的資料庫/系統（包括今次受影響的資料庫/系統）有查詢日誌功能，是否有透過該功能調查有關駭客取閱乘客資料的詳情、乘客資料外洩的內容，以及國泰透過查詢日誌功能收集相關資料的時間；

國泰用了所有可用的日誌之資料協助是次調查，包括人手審查日誌及即時反應分析。日誌審查及即時反應分析對調查及確定黑客活動是重要的一環。

五、 被入侵的資料庫/系統有否發現惡意軟件、木馬軟件、惡意載荷（Payload），如有，該等軟件的功能特徵為何？

我們發現黑客所用的是一些惡意軟件和功能程序。該些惡意軟件和功能程序在能力上有所不同，例如可以給予黑客在環境中進行偵察及在網絡環境下移動的能力。惡意軟件的識別碼是前所未知的，因此它們並沒能被國泰最新的防毒系統偵測得到。

六、 國泰有否訂立任何限制第三方服務供應商存取或連接資料庫/系統的政策？如有，詳情為何？

國泰是有制定限制第三方在國泰系統上的連接及存取的政策。

七、 國泰有否恆常進行進階持續性攻擊 (Advanced persistent threat) 之偵測和監察？

國泰設有偵測和監察的機制。自二零一八年三月，國泰亦實施了一個進階端點偵測和應對系統。

八、 國泰有否新措施防止類似事件再次發生，如有，請交代詳情。

由我們的調查開始至今，我們已採取補救措施，這些補救措施仍然繼續採用。當中有些措施為短期的，是為了保護我們的防線及阻止黑客進入。有些措施是較長期及策略性的。我們封鎖 IP 位址，關閉一些伺服器，不時改變保護功能, 例如改變防火牆及對部分不尋常活動設定警報。我們在整個網絡環境內設立進階威脅偵測系統。在調查過程中，我們亦同時發展多項的策略性行動,這些行動亦馬上實施。這些行動包括擴展網絡分割及進一步改善網絡安全。事實上我們一向都由健全的安全程序及安全防護。然而，是次黑客使用了前所未見的惡意程式, 對網絡系統的攻擊十分複雜。

國泰航空有限公司

二零一八年十一月