二零一一年六月十三日

參考文件

立法會資訊科技及廣播事務委員會

資訊保安

目的

本文件告知委員自上次於二零一零年七月十二日匯報至今，政府在推行各項資訊保安改善計劃方面的進展，以及政府的資訊保安狀況有何改變。

背景

2. 政府繼續致力改善各決策局／部門(下稱"局／部門")的保安措施，並爲社會各界提供支援，以助改善其資訊保安狀況。本文件按下列三個主要範疇匯報最新狀況 -

(a) 全球的資訊保安趨勢；

(b) 政府的資訊保安措施及狀況；以及

(c) 公眾的資訊保安。

全球的資訊保安趨勢

3. 我們現今生活在一個市民和商界均非常依重資訊科技及互聯網的環境。儘管資訊科技及互聯網可提高流動性、靈活性及效率，但我們也有需要認識到相應的保安風險及威脅。網絡保安不論對市民、機構或政府來說，都是非常重要的。透過網絡保安措施，市民可保護其私人資料，機構亦可安全地處理業務，而政府則可提供穩妥的公共服務。即使這樣，商業機構與其客戶仍持續關注網絡環境會受到各種威脅，例如電腦病毒及蠕蟲、惡意程式碼、身分盜用及仿冒詐騙攻擊。如果企業的電腦系統和服務沒有足夠的防禦能力保護資料的可用性、完整性和機密性，上述保安威脅可能會損害企業與客戶之間的互信關係。

4. 隨着流動裝置及無線上網日趨普及，現時出現了一些與筆記簿型電腦、消費者裝置(例如平板電腦及智能手機)和便攜式儲存裝置(例如 USB 閃存盤)等流動裝置尤其相關的保安威脅。除了外來黑客攻破機構的保安防線外，員工如沒有妥善處理機構的寶貴或敏感資料，也會對資訊保安構成威脅。社交網絡的出現和普及，可能會進一步增加機構內部資料外泄的風險。事實上，世界各地不時有新聞報道著名機構(包括一些主要服務平台供應商)發生大量資料外泄的事故。

5. 政府的抱負是要維持一個安全的資訊及通訊科技環境，以便香港發展爲領先數碼城市。因此，我們的使命是要堅守政府

的資訊保安政策和相關的作業模式，建立良好的資料保護文化，並向市民推廣資訊保安訊息，推動他們正確地使用資訊科技設施，並採取適當措施保護其電腦資源及資訊資產。政府資訊科技總監辦公室(下稱"辦公室")緊貼全球的資訊及通訊科技發展趨勢，並密切留意可能及實際出現的網絡攻擊，以便爲各局／部門及市民提供意見，讓他們採取所需的保安及防禦措施。

政府的資訊保安措施

6. 辦公室繼續致力提高政府員工對資訊保安的認知，推行技術解決方案以防禦網絡保安威脅，並確保各局／部門推行適當的監管措施和穩健的保安管理系統及作業模式，以保護政府的資訊科技資產、資料和資訊。下文載述我們所採取的各項資訊保安措施，包括增強員工的資訊保安認知和教育，優化技術和程序措施，以及加強審查保安規定遵行情況。

(i) 員工的資訊保安認知和教育

7. 我們持續舉辦有關員工資訊保安認知和教育的活動。提高員工的資訊保安認知和增強這方面的教育，是有助加強各局／部門資訊保安的主要因素。在二零一零至一一年度，辦公室舉辦了 10 場資訊保安認知研討會[1]，超過 1 100 名政府員工出席。我們亦安排了 50 項培訓課程(包括由內部及外間機構舉辦的培訓課

[1] 資訊保安研討會涵蓋多個主題，當中包括"保護敏感資料的機密性、完整性和可用性"、"良好的保安習慣"及"確保可信賴的保安策略"。

程)，供約 500 名政府員工參與。此外，我們已把超過 50 套網上培訓教材、超過 20 項良好作業模式，以及職員通訊季刊所刊載的各類專題文章上載政府內聯網，以便政府員工參考。上述的資源惠及政府各級員工。

8. 由辦公室統籌舉辦的資訊保安研討會及培訓課程，深受各局／部門歡迎[2]。我們透過舉辦這些研討會和培訓課程，向出席員工提供資訊保安知識和技術訣竅，並增強員工保護資料的意識。在二零一一至一二年度，辦公室會因應各局／部門所關注的課題舉辦相關主題的研討會，有關主題包括：處理保密資料、持續業務運作計劃及運作復原計劃、身分管理和接達控制，以及與流動資訊處理、社交網絡及雲端運算有關的保安威脅。員工在接受正式培訓後，可協助所屬的局／部門實施資訊保安措施。目前，超過 180 名在各局／部門工作的人員已取得各項資訊保安專業證書。

(ii) 技術和程序措施

9. 辦公室繼續密切留意與資訊及通訊科技發展趨勢相關的保安風險，並致力發掘可以減低風險的資訊保安解決方案。我們已把資訊保安解決方案的示例上載政府內聯網，供各局／部門參考推行，以保護其資訊科技資產、資料和資訊。各局／部門已根

[2] 根據二零一一年三月至四月進行的一項調查，超過 90%的局／部門同意，由辦公室統籌舉辦的資訊保安培訓課程對屬下員工十分有用，並表示日後會繼續提名員工參加該等培訓課程。

據其業務和運作需要，積極採用各項資訊保安解決方案，例如具備加密功能的便攜式儲存裝置、修補程式管理解決方案、安全遠端接達解決方案等。鑑於流動裝置的使用有所增加，各局／部門採取了多項相關控制措施，例如啓動密碼保護功能、只准使用已獲授權使用的軟件、把傳送或儲存的資料加密等。在推行無線網絡時，各局／部門亦實施了保安控制措施，例如爲接駁點提供保護、採用符合業界最新標準的強化加密算法，以及把內部有線網絡與無線網絡分隔，防止黑客入侵。

10. 一旦發現新的保安漏洞，辦公室便即時發出保安和病毒警報，提醒各局／部門在管理和營運其資訊系統時，必須及時進行軟件修補，以堵塞保安漏洞，以及遵行良好的資訊保安作業模式。例如，在過去六個月，我們發出了超過 30 次保安警報及三份催辦便箋，提醒各局／部門關注各項保安事宜，包括保護流動裝置免受惡意軟件和病毒感染、防範欺詐網站和仿冒詐騙攻擊，以及保護政府資料和資訊系統的措施。我們亦建議各局／部門與其轄下公共機構和規管機構分享有關資訊。

(iii) 遵行保安規定的審查

11. 根據現行的資訊科技保安政策，各局／部門須每兩年進行一次保安風險評估和審計，並須跟進評估和審計所得出的結果及建議。由二零一一年一月開始，我們加強了遵行保安規定的審查機制，要求各局／部門在每次完成保安風險評估和審計後六個

月內，須向辦公室提交評估和審計結果。此舉既可加強監管，同時亦可讓辦公室全面了解各局／部門一般面對的困難，以及他們所採取的相應解決方法。由辦公室統籌進行的抽樣保安審計，亦已於二零一一年四月展開，我們的目標是在二零一一至一二及二零一二至一三兩個年度每年完成 10 至 15 項審計工作。此外，辦公室會定期向各局／部門進行調查，了解其資訊保安計劃、作業模式和工作項目，而在二零一一年三月至四月進行的調查則剛已完成。我們會分析上述機制收集所得的資料，以監察各局／部門遵行保安規定的情況，並會用作制訂長遠的資訊保安計劃。有關審計工作剛已展開，預計於二零一一年下半年逐步得出結果。

政府的資訊保安狀況

12. 從供應商和用戶的角度來看，雲端運算[3]是全球趨勢，對資訊科技行業帶來影響。政府已將採用雲端運算提供中央資訊科技服務，定爲政府資訊科技策略的重點主題。辦公室現正評估這方面所涉及的保安風險，並在充分考慮其可用性、可靠性、完整性、保密性和保障私隱等因素後，以訂出最合適的推行方案。我們將制訂良好作業模式和指引，供各局／部門採用雲端運算時作參考使用。

13. 我們須與時並進，不斷緊貼嶄新的保安威脅、新的業務

[3] 雲端運算是一種運算模式，可方便用戶按需要經網絡接達可共用及配置的電腦資源(例如網絡、伺服器、儲存器、應用程式和服務)。用戶只須投放少量的管理資源，或與服務供應商作適量的配合，便能迅速獲得提供有關的電腦資源。

計劃、新興科技和服務模式，以及互聯網用戶行爲的改變，而這方面的工作甚具挑戰性。在二零一零年七月至二零一一年五月期間，政府資訊保安事故應變辦事處[4]共接獲五宗資料外泄事故報告，而發生事故的宗數有下降趨勢[5]。在這五宗事故中，兩宗涉及遺失USB閃存盤，兩宗涉及文件於網上流傳，餘下一宗則有關電腦程式出錯。至於涉及個人資料的事故，有關的局／部門已向個人資料私隱專員報告，並適當地通知受影響人士。這些事故的詳情載於附件。

公眾的資訊保安

14. 在社區方面，辦公室繼續與業界和專業團體合作舉辦各種活動，以提高公眾對保護電腦資源和資訊資產的認知和知識。在二零一一年，我們繼續與持分者，包括香港警務處(下稱“警務處”)和香港電腦保安事故協調中心(下稱“協調中心”)合作，爲市民舉辦三場公開研討會，並爲業界(包括互聯網服務供應商)舉辦一場研討會。鑑於流動平台所受到的保安威脅有增加趨勢，以及社交網絡日益流行，研討會將專注就流動設備、社交網絡和網上欺詐交易等方面探討相關的保安趨勢和問題。至於爲互聯網服務供應商舉辦的研討會，將設有探討網絡攻擊及緩解措施的環節。

15. 辦公室於一站式資訊保安網站(www.infosec.gov.hk)發

[4] 政府資訊保安事故應變辦事處的成員來自辦公室、保安局及香港警務處。
[5] 在二零零八年七月至二零零九年六月及二零零九年七月至二零一零年六月這兩段每段爲期12個月的期間，政府資訊保安事故應變辦事處分別接獲九宗及八宗資料外泄事故報告。

布本港和海外有關資訊保安的消息，讓市民知悉嶄新出現並可能會影響他們的保安問題。由二零一零年四月開始，我們在香港電台播放全新一輯宣傳聲帶，每月均設有特定主題，爲市民提供資訊保安的實用小提示和良好作業模式(例如保護資料以防外泄、安全使用社交網絡及流動保安)。我們亦透過上述資訊保安網站，與市民分享政府員工培訓課程所使用的錄像和動畫資源，以提高他們的資訊保安認知。在二零一零年“全城電腦清潔日”活動[6]中，我們舉辦了標誌設計比賽，反應非常踴躍，共有 280 名參賽者。有關獎項已於二零一零年十一月頒發。

16. 爲了測試本港互聯網基建持分者在重大事故期間的協調情況，協調中心在二零一零年十月統籌進行了第二次資訊保安事故應變演習，讓有關各方參與[7]。透過參與該次演習，有關機構汲取了應付緊急情況的經驗，而協調中心亦可根據所獲得的有用意見，改善重大事故期間的協調工作，並加強各持分者之間的溝通。

總結和未來路向

17. 現今的網絡保安威脅層出不窮，涉及流動裝置及服務、社交網絡、身分盜用等。政府會繼續致力提高社會各界對資訊保安的認知和警覺性，並密切留意網絡保安威脅，以及確保各局／

[6] “全城電腦清潔日”是辦公室、協調中心及警務處每年合辦的資訊保安認知推廣活動。
[7] 參與演習的機構包括辦公室、警務處、香港互聯網供應商協會、香港互聯網交換中心、香港互聯網註冊管理有限公司和 DotAsia Organisation 等。

部門推行適當的監管措施和穩健的保安管理系統及作業模式。鑑於資訊保安是一項須持續進行的工作，我們會繼續採取各項保安措施，以保護政府的資訊科技資產、資料和資訊。

徵詢意見

18. 請委員察悉本文件的內容。

商務及經濟發展局

政府資訊科技總監辦公室

二零一一年六月

附件

二零一零年七月至二零一一年五月

政府資料外泄事故摘要

項目	事故日期	局／部門	事故摘要和跟進措施
1	二零一零年七月	政府資訊科技總監辦公室	聖公會聖匠堂社區中心一名職員遺失一個 USB 閃存盤，內載有共 4 413 名中心活動參與者的個人資料。該中心獲政府資訊科技總監辦公室委託在九龍城區推行“做個智 Net 的”互聯網教育活動。 中心已知會個人資料私隱專員，並已通知所有受影響人士。
2	二零一零年十一月	勞工處	勞工處互動就業服務網站的電郵通知程式，將載有 220 名登記用戶敏感資料的電郵發送給非預定收件者。該處證實沒有資料在事故期間曾被人修改。 勞工處已知會個人資料私隱專員，並已通知所有受影響人士。該處其後已找出並糾正該程式錯誤。
3	二零一一年二月	警務處	網上流傳三份據稱屬於警務處的文件，一份爲早前外泄且載有個人資料的口供，另一份則爲已上載至警務處網站的非保密文件，餘下一份文件載述已過時的警察槍械使用規則。 事件並無涉及新的受影響人士的個人資料。

項目	事故日期	局／部門	事故摘要和跟進措施
4	二零一一年四月	警務處	網上流傳四份據稱屬於警務處的文件。該處仍就事件進行調查，以確定外泄源頭。當中一份相信是一名市民就申請警務督察職位事宜所草擬的文件，並非由警務處外泄。其餘三份相信是經由私人電腦內置 FOXY 軟件外泄的文件。 事件涉及 17 名人士(包括 15 名警務人員和兩名市民)的個人資料。警務處已知會個人資料私隱專員，並已通知所有受影響人士。
5	二零一一年五月	社會福利署	一名職員遺失一個私人擁有的 USB 閃存盤，內載有兩名人士的個人資料，包括姓名和身份證號碼。 社會福利署已知會個人資料私隱專員，並已通知所有受影響人士。