二零一二年七月十日

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

本文件匯報自二零一一年六月十三日至今，政府的各項資訊保安計劃。

背景

2. 新興科技和互聯網用戶的行為改變，令全球的資訊保安趨勢繼續不斷演變，並引起了新的資訊保安問題。政府繼續致力提升其網絡保安防護能力，並協助市民保護他們的電腦系統及資料。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；以及
(c) 公眾的資訊保安。

全球的資訊保安趨勢

3. 新興科技的廣泛應用對資訊保安造成影響。舉例來說，用戶通常着重的，是流動裝置所具備的嶄新功能，以及使用社交網絡與朋友聯繫所帶來的方便，但對於保安及私隱，卻未必同樣重視。這往往讓電腦罪犯有機可乘，利用保

安漏洞進行非法活動。另一個趨勢是，機構使用流動解決方案及雲端服務，把更多業務資料數據傳送及儲存至機構以外地方，故保安實體界限正逐漸消失。換言之，機構的資訊系統保安不再只是裝設防火牆及採取周邊防護措施。

4. 根據一間保安供應商公布的數據，在二零一一年偵測到的網絡攻擊次數是二零一零年的兩倍[1]。至於全球的仿冒詐騙攻擊[2]，二零一一年錄得的次數較二零一零年增加了37%[3]。惡意應用程式經流動平台入侵的宗數，則由二零一一年六月的 400 宗，大幅增加約 40 倍，至二零一二年二月逾 15 000 宗[4]。香港與世界其他地方一樣，一直面對着各種網上威脅。根據香港警務處(下稱“警務處”)資料顯示，二零一一年該處接獲 2 206 宗電腦罪行的舉報，與對上一年比較，增幅為 34.3%[5]。

政府的資訊保安措施

5. 政府資訊科技總監辦公室(下稱“辦公室”)十分重視政府內部的資訊保安。我們繼續致力提高政府員工對資訊保安的認知、建議技術工具及解決方案以保護政府資訊系統及資料、推行機制以監管保安規定的遵行，以及檢討現行的保安規例、政策及指引。有關詳情載於下文。

(a) 員工的資訊保安認知和教育

6. 我們須確保全體員工明白資訊保安措施的重要性，並

[1] http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011
[2] 仿冒詐騙攻擊是一種網上威脅，惡意攻擊者利用欺詐電郵或連結，誤導用戶登入欺詐網站。
[3] http://www.rsa.com/phishing_reports.aspx
[4] http://www.devshed.com/c/a/Smartphone-Development/Juniper-Networks-Android-App-Malware-Increasing-11377/
[5] http://www.police.gov.hk/ppp_tc/11_useful_info/doc/1213/SB-c032.pdf

確保他們肩負起保護政府資料的責任，這一點是非常重要的。辦公室透過各種渠道提高員工對資訊保安的認知。在二零一一至一二年度，我們舉辦了 10 場資訊保安認知研討會[6]，有超過 1 400 名政府員工出席；比較在二零一零至一一年度等同的場數有 1 100 名政府員工出席。我們亦安排了 48 項資訊保安培訓課程(包括由內部及外間機構舉辦的培訓課程)，供約 400 名政府員工參與。此外，我們製作了 20 套動畫短片[7]，並上載至政府的內聯網給員工瀏覽，以協助他們了解基本的資訊保安知識及作業模式。多個局及部門均參考這些由辦公室統籌製作的培訓資料，並將之納入其培訓教材內，以供內部培訓及簡報之用。

7. 辦公室密切留意國際及本地機構[8]所提供的網絡保安資訊，確保與時並進，清楚了解網上攻擊的最新趨勢，以及市場就防禦該等攻擊所推出的解決方案。在二零一一至一二年度，我們向各局及部門發出了六份涉及不同主題的催辦便箋，有關主題包括保護政府網站及應用程式和保護流動裝置，以及就保安漏洞發出 66 次嚴重保安警報。與二零一零至一一年度所發出的 73 次嚴重保安警報相約，警報大多數和作業系統、互聯網瀏覽器、媒體播放等軟件漏洞有關。這些警報有助各局及部門能夠迅速採取措施修補有關的軟件漏洞，有效地保護政府的資訊資產。

8. 透過政府內聯網的資訊科技保安專題網站，我們可與政府員工保持有效溝通。該專題網站載有豐富內容，包括本地及海外資訊保安消息和警報、資訊保安技術和解決方案、保安政策、規例及作業指引，以及其他技術參考資料。在最

[6] 資訊保安研討會涵蓋多個主題，當中包括“流動資訊處理及社交網絡保安”、“網上應用系統保安”及“防禦惡意軟件攻擊”。

[7] 連同二零一零至一一年度製作的 20 套動畫短片，現共有 40 套動畫短片，協助員工了解基本的資訊保安知識及作業模式。

[8] 包括本地及海外負責事故應變的機構（例如美國及香港的電腦保安事故協調中心）和銷售抗禦病毒軟件的大型機構。

近一項調查中，88%的局及部門給予該網站“良”或“優”的評級。

(b) 技術工具及解決方案

9. 政府採用了一套系統化的方法，以“防禦、偵測、應變和復原”作為重點原則，來保護我們的電腦系統、網絡及資訊。各局及部門已採取各種技術保安措施，包括安裝防火牆、抗禦病毒軟件、入侵偵測和防禦系統及其他防禦機制，以監測、偵察和堵截惡意程式碼及可疑的網絡通訊。各局及部門也有使用存取控制和加密工具保護資料，防止資料在未獲授權情況下存取。

10. 辦公室進行市場研究，並把科技新知及可行的技術解決方案上載到政府內聯網，以供各局及部門參考。現時已有超過 90 個涉及不同類別的解決方案，例如入侵偵測和防禦、安全網絡通訊、保安事故管理和虛擬化技術。隨着流動資訊處理的應用日益普及，我們已編製有關參考資料，介紹一些較着重保護資料的解決方案，例如資料加密、端點保護及防止資料遺失的解決方案。我們亦推廣應用公開密碼匙基礎建設和數碼證書，確保通訊和交易可安全穩妥地進行。

(c) 監管保安規定遵行情況

11. 為監管和執行政府內部的資訊保安，資訊保安管理委員會於二零零零年成立，督導保安規管，其核心成員包括保安局及辦公室的代表。此外，為了在行政上支援該委員會，政府成立了資訊保安工作小組[9]，負責制定及頒布資訊保安政策及指引，和監察各局及部門在保安規定的遵行情況。各局及部門均須委任一位部門資訊科技保安主任，負責該局及部

[9] 資訊保安工作小組成員包括來自保安局、辦公室、警務處及政務司司長辦公室的代表。

門的整體資訊保安管理及運作。此外，各局及部門須設立資訊保安事故應變小組，以處理保安事故的滙報及應變，包括在必要時提升警戒級別，並定期進行演習。

12. 由二零一一年一月開始，辦公室強化了保安規定遵行審查機制，以加強監察各局及部門的資訊保安狀況。在二零一一至一二年度，辦公室已完成目標，為 12 個局及部門進行保安規定遵行審計工作。透過有關工作，我們協助各局及部門達至符合基準資訊科技保安政策的規定、找出存在風險的項目及可予改善之處，並建議有關局及部門可採取的跟進行動。在二零一二至一三年度，我們計劃為另外 14 個局及部門進行保安規定遵行審計工作。

13. 根據二零一二年六月完成的年度調查，與去年比較，各局及部門在強化採用保安措施及解決方案打擊各類保安威脅方面，情況普遍有所改善。例如，使用端點保安解決方案以保護用戶電腦及伺服器的比率，由二零一一年的 73%增至二零一二年的 82%；而使用修補程式管理解決方案以助更新保安軟件的比率，由二零一一年的 81%增至二零一二年的 88%。

14. 據觀察所見，在二零一一至一二年度，各局及部門已更優先地推行與保安相關的措施，包括進行保安風險評估和提升其保安基礎設施。在上述年度，與保安相關的項目共有 71 個，估計開支達 3,430 萬元；在二零一零至一一年度，這類項目則有 25 個，開支為 1,840 萬元。

(d) 資訊保安規例、政策及指引檢討

15. 為確保與政府資訊科技保安有關的規例、政策及指引能與時並進，配合科技的進步、本地及全球的資訊保安趨

勢，以及國際及業界作業模式的最新發展，辦公室和保安局在二零一一年十一月開展了一項檢討工作。在檢討期間，我們將政府基準資訊科技保安政策與其他經濟體系[10]的有關政策及國際標準[11]作比較。從比較得出的結果，我們建議多項修訂範疇，包括加強資料保護、在外判的環境下的保安管理，以及涉及新興科技如流動資訊處理和雲端服務的應用。我們會因應這些結果，就嶄新技術的應用推出新的保安規定。我們會在二零一二年年底，向各局及部門公布經修訂的資訊保安規例、政策及指引。

公眾的資訊保安

16. 除了在政府內部推出措施外，辦公室亦與其他機構合辦多項活動，以提高市民對資訊保安的認知，並推廣採用有關的良好作業模式，以及提升處理保安事故的應變能力。有關詳情載於下文。

(a) 資訊保安認知推廣活動

17. 為提高市民對資訊保安的認知，並加強保護個人電腦和資訊科技設備免受網絡攻擊，辦公室、警務處及香港電腦保安事故協調中心(下稱“協調中心”)自二零零五年起每年都就時下相關課題合辦活動。二零一一年活動的主題為流動資訊保安，共舉辦了四場公開研討會，吸引超過 500 人參加。二零一二年活動的主題為「共建網絡安全」，重點是推廣採取保安防護措施抵禦網絡攻擊，活動包括四場公開研討會及一項海報設計比賽。

---

[10] 有關經濟體系包括澳洲、加拿大、日本、英國及美國。

[11] 有關國際標準包括 ISO27001 和 ISO27002（由國際標準化組織公布）和 COBIT（國際信息系統審計協會公布的信息及相關技術控制目標）。

18. 為了喚起更多市民注意，辦公室亦每月製作八組一分鐘的宣傳聲帶，為市民提供資訊保安的實用小提示及良好作業模式[12]。這些宣傳聲帶約每日三次在電台播放。

(b) 推廣採用良好作業模式

19. 辦公室把資訊保安良好作業模式上載到資訊保安專題網站(www.infosec.gov.hk)，並不時予以更新，以供市民參考。我們為中小型企業(下稱“中小企”)編制的《中小型企業資訊保安指南》，在各公共場合派發，亦在專題網站供市民參考和下載。

20. 至於雲端運算方面，除了政府的採用，我們亦鼓勵私營機構(包括中小企)應用。我們已在二零一二年四月成立雲端運算服務和標準專家小組，以協助推動本地應用雲端運算。專家小組的成員來自業界、學術界及政府。鑑於雲端保安的重要性，我們在專家小組之下設立了雲端保安及私隱工作小組和其他兩個工作小組。我們會與本地服務供應商及私營機構，特別是中小企，分享工作小組所編制的資料，以促進更廣泛和安全地應用雲端運算。

(c) 加強網絡保安及應變能力

21. 政府認為電腦事故應變中心是互聯網基礎設施可達至安全可靠的一個重要部分。因此，政府提供撥款，給予由香港生產力促進局管理的協調中心提供電腦事故應變中心服務。自二零零一年至今，協調中心一直擔當中央統籌角色，負責接收有關電腦及網絡保安事故報告及作出應變。一旦發生保安事故，該中心會為本地電腦用戶提供協助，以減

[12] 最近播放的宣傳聲帶主題包括“雲端服務用戶的安全貼士”、“網上社交網絡安全貼士”、“安全使用智能手機”和“數碼證書的實用貼士”。

輕事故對其服務的影響及有關損失，並幫助其業務回復運作。在二零一二年，辦公室提供進一步撥款給予協調中心以擴展中心服務和加強其能力，尤其是密切留意網上的不尋常活動，以偵測潛在威脅、發出警報，以及啟動有關防禦措施。為支援流動資訊保安，協調中心會在二零一二至一三年度起，向市民提供處理智能手機事故的服務。至於海外合作方面，協調中心會與其他地方的電腦保安事故應變小組及全球保安事故協調中心組織[13]保持聯繫，以促進彼此合作及互相協調。

22. 針對網上討論區的欺詐訊息出現上升趨勢，協調中心在二零一一年十一月舉行全港電腦保安事故演習，以提升本地網上討論區負責人的事故應變能力。協調中心、警務處及辦公室，聯同三個本地大型網上討論區，參與了是次演習，成功測試了各參與機構的事故應變程序。

總結

23. 我們現正面對着流動技術、雲端運算及社交網絡應用日增所帶來的新保安挑戰，以及網絡世界嶄新出現的威脅。政府會繼續推行各項資訊保安措施，以保護政府的資訊系統及資料和本港的網絡環境。在資訊及通訊科技界、資訊保安從業員、工商機構、社會大眾及政府的同心協力下，香港在建立安全可靠的電子社羣上，定可站在前列位置。

[13] 全球保安事故協調中心組織是由多個獲信賴的電腦保安事故應變小組組成的國際聯盟，負責合力處理電腦保安事故和推廣事故防禦計劃。該組織匯聚了多類型的保安及事故應變小組，特別是來自政府、商界及學術界的產品保安小組。

徵詢意見

24. 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

二零一二年七月