二零一四年七月二十二日

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

本文件向委員匯報自二零一三年七月至今，政府各項資訊保安計劃的最新進展。

背景

2. 在過去一年，隨着互聯網和流動裝置在企業營商以及日常生活中廣泛應用，資訊保安威脅和網絡攻擊不論在種類或頻率方面，都有上升的趨勢。香港警務處（下稱「警務處」）在二零一三年共收到 5 133 宗科技罪案報告，較二零一二年的 3 015 宗，增加超過 70%，當中「未獲授權而取用電腦」的數字增加了 90%。

3. 根據香港電腦保安事故協調中心（下稱「協調中心」）所發表的「香港保安觀察報告」顯示，在過去四個季度保安事故的數字呈上升趨勢。在二零一四年首季，保安事故總數超過 15 000 宗，當中釣魚網站攻擊有 2 039 宗，而網頁塗改攻擊有 3 490 宗，分別大幅上升了 154% 和 97%[1]，由此可見網絡威脅在規模或精密程度方面都在不斷增長。

面對挑戰

4. 在各種新興網絡威脅下，傳統的資訊保安角色和職責愈趨複雜，企業和個人單靠保護自己的資訊系統並不足夠，他們需要掌握新技術，以防禦互聯網或流動網絡上的攻擊和惡意活動。政府非常重視資訊和網絡保安。

5. 在政府內部，政府資訊科技總監辦公室（下稱「資科辦」）致力－

- 保護政府的資訊系統和數據資產；
- 審核所有政府決策局和部門(下稱「各局及部門」)在保安規定方面的遵行情況；以及

[1] https://www.hkcert.org/my_url/zh/blog/14052101?nid=219283

- 檢討電腦保安事故應變機制和推廣網絡保安的認知及教育。

6. 在公眾層面，我們亦致力－

- 與本地及海外持份者合作，加強保安情報的收集和通報；
- 推廣資訊和網絡保安的認知及教育；以及
- 促進公私營機構合作，以保障網絡安全。

保護政府的資訊系統

7. 政府的資訊系統會按其服務性質和風險水平受到適當及足夠的保安措施所保護。我們已採用的保安措施包括入侵偵測及防禦系統、存取控制系統、防火牆及抗禦病毒方案，用以監測、偵察和堵截政府電腦系統和網絡上可疑的網絡通訊。政府的雲端基礎設施和數據中心均全面遵從政府的保安規定，受到安全穩妥的保護，所有數據亦利用加密技術加以保護。這些裝置在操作管理及保安控制的品質保證方面亦獲得國際標準認證，包括國際標準化組織（ISO）／國際電工委員會（IEC）20000－資訊科技服務管理，以及

ISO/IEC 27001－資訊安全管理系統的認證。

8. 為確保現行的資訊保安措施足以妥善應付新挑戰，政府網站已定期進行保安風險評估。除了由個別局及部門定期進行的風險評估外，資科辦正計劃特別為所有公開的政府網站進行安全掃描，以確定各網站的保安風險及確保其防禦能力。我們也會為政府的資訊保安從業員安排進階的網絡保安培訓，並向系統管理人員提供複修課程，提升各局及部門整體的網絡保安能力和增進政府人員的知識及技能，以應付新興網絡威脅所帶來的挑戰。

審核資訊保安方面的遵行情況

9. 保安風險管理是政府對保障資訊安全所採取的重要程序，旨在積極找出保安風險，並採取適當的保安措施以減低相關風險。在二零一三至一四年度，政府共投放了 1.144 億元進行 122 個與資訊保安相關的項目，與二零一二至一三年度投放 6,580 萬元進行 85 個項目比較有顯著增加。這些項目包括進行保安風險評估和審核、推行技術解決方案加強保安控制，以及對現有的保安基礎設施進行升級。

10. 自二零一一年一月起，資科辦展開一個專項計劃，評估各局及部門在政府保安政策和規定方面的遵行情況。截至二零一四年六月，我們已就 42 個局及部門的重要系統完成遵行情況審核，結果顯示這些局及部門均已遵從政府的資訊保安政策和規定，同時亦從評估的過程中，讓他們明白到持續優化保安管理系統對應付新興保安威脅十分重要。我們在未來兩年會繼續為餘下的局及部門進行遵行情況審核。

收集和通報保安警報及警告

11. 政府、企業和公眾等相關持份者是網絡世界的主要參與者，因此必須了解有關風險和學習不同的技能，以期保護各自的資訊系統和敏感數據。

12. 政府會持續加強資訊安全網入門網站（www.infosec.gov.hk）的內容，協助公眾有效地獲取與資訊保安相關的資訊和資源，以及查閱預防網上罪行的措施和良好作業模式。我們亦透過電子郵件及「香港政府通知你」流動應用程式，發布保安警報和警告。

13. 在政府內部，我們致力監察保安威脅和科技趨勢發展，以便制定適當的保護措施，保護政府的資訊科技系統及資訊資產。在二零一三至一四年度，資科辦向政府用戶發出了 63 次嚴重保安警報及四份有關資訊保安的催辦便箋，提醒各用戶有關當前或即時的保安威脅，並建議他們妥善跟進。我們亦修訂了政府的事故應變機制，加強對事故各階段的應變管理，並要求各局及部門嚴格遵從保安事故應變的規定，按緩急優次分配資源處理已知的保安事件，以及採取適當的補救措施。

14. 在公眾層面，協調中心專責協調本地企業及個人就電腦保安事故作出回應。協調中心與世界各地的電腦保安事故應變小組合作，發布保安警報及警告，並提供有關保安威脅預防措施的建議。在二零一三至一四年度，協調中心共發出了 443 次保安公告和 103 篇保安博錄，較二零一二至一三年度發出 439 次保安公告及 78 篇保安博錄有所增加。近期為「心臟出血」漏洞和電子灣（eBay）帳戶密碼事件所發布的保安忠告，亦協助本地企業及個人迅速採取補救行動。協調中心自二零一三年第四季開始每季出版「香港保安觀察報

告」，讓公眾了解保安事件的最新趨勢及需要關注的地方，並就相關預防措施提供建議。

電腦保安事故應變機制

15. 為更順暢和有效地通報區內已知的事故，我們已修訂資科辦、警務處、協調中心及本地持份者之間的電腦保安事故應變通訊機制，以加強各方在收集網絡威脅情報、通報威脅評估及處理事故應變方面的角色和工作流程。經修訂的機制有助促進各方緊密合作，以便能適時和有效地協調和防禦網絡威脅。

16. 因應網絡威脅的上升趨勢，以及針對政府資訊系統和資訊資產的攻擊可能為公眾所帶來的影響，由資科辦、保安局及警務處代表組成的政府專責小組已開始檢討政府現行的電腦保安事故應變及處理的管理架構，以加強網絡保安的能力。該專責小組會參照其他政府的良好作業模式，並建議改善措施，加強政府對處理電腦保安事故的應變能力。

17. 網絡威脅無分疆界，因此我們必須建立國際合作關

係，以具成效及效率的方式分享資訊。資科辦一直積極參與國際資訊保安活動，並與相關機構（包括亞太經濟合作組織和全球保安事故協調中心組織（FIRST））合作，在國際及地區層面與有關專家建立工作聯繫，以掌握有關資訊保安威脅和防禦措施的最新消息和趨勢。此外，我們也與協調中心合作，參與由亞太區電腦保安事故協調組織（APCERT）所舉辦的活動，並適時向市民發布相關的保安資訊。

18. 我們現正聯同協調中心研究其他經濟體系的電腦保安事故應變小組的組織功能和能力，以優化香港在類似範疇的功能，包括可能需要在現行機制加入保安範疇的分析、特定界別的參與、網絡威脅的偵察和採取較為積極主動的運作模式，以應付網絡世界的新興威脅。

資訊保安認知及教育

19. 人為因素往往被視作資訊保安最薄弱的環節。資科辦致力增進市民對抵禦網絡威脅的知識。就此，用戶對資訊保安的意識及知識發揮重要作用，我們在這方面的計劃涵蓋政府內部和公眾兩個層面的工作。

政府員工

20. 資科辦為政府員工定期舉辦研討會和培訓課程，讓他們掌握資訊保安的最新發展和提升他們的能力，以便更妥善履行職責。

21. 自二零一三年十一月開始，我們聯同資訊科技保安業界舉辦了一系列的資訊科技保安解決方案展示會，讓各局及部門了解最新的保安技術和解決方案，並提高他們對保護系統和數據的認識。這些展示會結合演講環節和示範攤位，為各局及部門提供專門的資訊保安解決方案和服務，以處理特定的保安事宜，例如端點設備保安、流動保安、加密的解決方案等。我們將繼續舉辦專題資訊保安解決方案展示會，協助各局及部門持續改進其推行保安措施的安排。

22. 為資訊保安支援人員安排培訓，對各局及部門執行保安職務有莫大幫助。在過去一年，我們為超過 400 名政府資訊科技保安從業員安排逾 60 項有關資訊保安的進階培訓課程。截至二零一四年六月，在各局及部門工作的相關人員已

取得超過 230 張國際認可的資訊科技安全專業證書[2]。

23. 除此之外，在二零一三至一四年度，我們特別為各局及部門的資訊保安人員舉辦兩場專題研討會。研討會的目的是確保有關人員能充分了解自己的職務和職責、更新他們對資訊和網絡保安威脅及相關緩解措施的知識，並向他們重申保護網絡上的政府資訊系統和數據資產的重要性。我們將繼續定期舉辦進階的保安培訓，並提供有關政府資訊科技保安政策的最新資訊。

24. 我們將進一步加強政府資訊科技專業人員防範網上應用系統攻擊的技能和能力。對於參與網上應用系統入侵測試的政府內部保安專業人員，我們會提供在職培訓，以提升他們在網絡保安方面的能力。

公眾層面

25. 為提高市民對資訊保安的認知，資科辦自二零零五年起聯同警務處及協調中心合辦全年推廣活動。在二零一三

[2] 資訊安全專業證書包括由國際資訊系統保安認證協會(ISC)[2] 所頒發的資訊系統安全師專業認證(CISSP)，以及由國際電腦稽核協會(ISACA)所頒發的電腦稽核師專業認證(CISA)等。

年，活動的主題為「防禦針對性攻擊」，我們舉辦了四場公開研討會，以提高公眾對針對性攻擊風險的認識。為了把訊息推廣至年青的一代，我們舉辦了以「做個精明網民」為主題的短片創作比賽，藉此提高市民對資訊安全的認知和推動他們採用良好作業模式。是次比賽反應熱烈，得獎作品不僅展現參加者的創意和熱誠，並彰顯了用以保護電腦設備免受保安威脅的良好作業模式。

26. 在未來一年，資科辦會繼續透過不同宣傳渠道，為普羅大眾舉辦有關資訊科技保安的專題教育及推廣計劃。我們竭力確保資訊科技從業員和用戶能更了解潛在的保安風險及緩減風險的方法。我們亦會進一步為公眾提供檢測電腦設備漏洞的指引，以及防範網絡風險的實用措施。由二零一四年六月至九月，我們會舉辦以「資訊保安由我做起」為主題的四格漫畫創作比賽。

27. 我們會繼續在學校推行提高認知的推廣活動。未來一年，在資訊科技教育策略推動下，預期學校將更廣泛應用資訊科技和無線網絡。我們會進一步與專業機構合作，為學校的技術支援人員提供培訓及工作坊，讓他們更有效地管理學

校的電腦系統、網絡及數據，以防範這些設施遭受網絡攻擊。

保障網絡安全

保護重要資訊基礎設施

28. 由於重要基礎設施的操作管理和控制日益依賴資訊科技，如出現技術故障或網絡攻擊，均會對這些設施的保安及復原能力構成威脅。因此，警務處於二零一二年成立網絡安全中心，以加強保護香港的重要基礎設施，並提升本港遭受網絡攻擊時的復原能力。警務處計劃擴展現時科技罪案組的角色和職責，在二零一四年稍後時間成立新的網絡安全及科技罪案調查科，以期加強警務處在保護重要基礎設施的資訊系統安全方面的能力，以及應對各種新興科技罪案的挑戰。警務處成立這個新調查科將有助提升香港對網絡攻擊和保安事故的應變及復原能力。

29. 我們明白公私營機構合作對保護重要基礎設施十分重要。資科辦於二零零五年成立互聯網基建聯絡小組[3]，作為

[3] 互聯網基建聯絡小組成員包括香港互聯網交換中心、香港互聯網註冊管理有限公司、香港互聯網供應商協會、協調中心、通訊事務管理局辦公室、警務處和資科辦的代表。

政府和重要資訊基礎設施持份者的合作平台，以分享、交流和合作應對本港的保安事故，以及就區內舉辦影響重大的大型活動時協力維護本港互聯網基礎設施的穩定性、安全性、可用性和復原能力。

30. 自二零零九年起，資科辦聯同警務處和協調中心，與主要的互聯網持份者每年聯合進行網絡保安演習。二零一三年演習的主題是「應付針對性攻擊」，參與者包括固定及流動網絡供應商、域名註冊服務機構，以及一些政府部門。是次演習成功測試了參與各方的事故應變程序。我們將於今年稍後時間再次舉辦網絡保安演習。

採用國際保安標準和良好作業模式

31. 為了防禦潛在的網絡攻擊和網絡罪行，制定全面的資訊保安管理機制對所有機構都尤為重要。

32. 在政府內部，我們參照國際保安標準和業界良好作業模式制定政府資訊科技保安政策及指引，有助各局及部門採用國際資訊保安管理系統和遵從政府保安政策的規定。為緊貼資訊科技步伐和應對不斷變化的保安威脅，我們定期檢討

政府的資訊保安規定。我們將於二零一五年年中展開下一輪檢討工作，以檢視最新的保安環境，並就這些保安規定建議所需的修訂。

33. 在公眾層面，我們鼓勵企業採用國際資訊保安標準和良好作業模式，以保護他們的資訊系統和數據資產。在二零一四年四月，我們在香港主辦了國際標準化組織和國際電工委員會（ISO/IEC）第一聯合技術委員會／第 27 分技術委員會（下稱「SC 27」）會議，以推廣本地資訊科技業界更廣泛採用國際標準和良好作業模式。由 SC 27 所擬定和管理的 ISO/IEC 27001 標準系列，是一套獲全球認可的資訊保安管理系統標準。是次會議有超過 300 名來自逾 30 個經濟體系的海外和本地保安專家和專業人員出席。此外，在會議舉行期間舉辦的業界活動亦吸引了大約 400 人參加，包括超過 200 名本地參加者。是次活動成功提高本港企業的保安意識，促進企業在資訊保安方面更廣泛採用國際標準。我們會繼續舉辦推廣活動，鼓勵本地企業採用資訊保安標準，以加強本港在資訊保安方面的整體能力。

與業界合作

34. 在二零一三年八月，資科辦主辦了一場圓桌會議，就香港在防範網絡威脅的能力和準備程度方面，向本地資訊保安專業人員、企業用戶及學術界的精英徵求專業意見。是次會議討論和探討如何加強本港在資訊保安管理、網絡威脅偵察和監測、保安事故應變、人才發展、跨行業合作等方面的資訊保安能力。

35. 在今年四月的 2014 國際 IT 匯期間，我們舉辦了三項資訊保安業界活動，為海外及本地的資訊科技保安專業人員及資訊科技從業員提供平台，讓他們分享知識及交流經驗。三項活動共有超過 350 人參加。

36. 雲端服務在世界各地日趨普遍。然而，準用戶（特別是中小型企業）由於缺乏相關專業知識，在物色和採購合適雲端服務時可能會遇到困難。今年四月，我們在雲資訊入門網站（www.infocloud.gov.hk）發布了雲端服務評估工具及認證計劃的清單，協助雲端服務供應商確定他們所提供的雲端服務的保安能力。準用戶在選擇雲端服務時可參考相關供應商透過這些工具和計劃提供的資訊。我們亦與廣東省的雲計

算專家合作，發展雲安全管理計劃，三個本地雲端服務供應商已應邀參與計劃，於二零一四年內進行試點測試。

總結

37. 我們已準備就緒，應對不斷變化和層出不窮的網絡威脅所帶來的新挑戰。除了沿用保護資訊科技系統和資訊資產的既定防禦機制外，我們正積極在政府內部、商界及公眾層面加強資訊保安的能力。我們會繼續保護政府的資訊系統和數據，並與業界及相關持份者合作，為香港提供更安全的電腦網絡。

商務及經濟發展局

政府資訊科技總監辦公室

二零一四年七月