二零一五年七月十七日

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二零一四年七月至今，政府各項資訊保安計劃的最新進展。

背景

2. 資訊及通訊科技、互聯網服務及流動解決方案等技術的創新應用，大大提高了我們的日常生活質素。另一方面，由於科技普及，企業及市民廣泛應用科技，亦增加資訊保安管理的難度。隨着經網上處理的商務及敏感資料愈來愈多，在防禦資訊保安威

脅及網絡攻擊方面，公私營機構及個人的攜手合作尤為重要。

3. 過去一年，政府開展了多項計劃，以針對加強政府資訊系統及其互聯網基礎設施的保安。我們亦與主要的持份者合作，通過分享良好作業模式及指引，加強市民對資訊保安的意識及知識，從而在上網時防禦網上惡意活動及網絡威脅。本文件按以下三個範疇匯報各項計劃的最新進展：

(a) 資訊保安趨勢及挑戰；

(b) 保障資訊保安的主要措施；以及

(c) 資訊保安認知及教育計劃。

資訊保安趨勢及挑戰

日益增加的網絡保安威脅

4. 在二零一四年，網絡罪行數字及相關財務損失都有所增加，顯示網絡保安威脅正不斷上升。根據香港警務處（下稱「警務處」）的資料，二零一四年內共收到 6 778 宗科技罪案報告，較二零一三年的 5 133 宗增加 30%。由此導致的財務損失總額估計由二零

一三年的 9 億元增至二零一四年的 12 億元。這個上升趨勢也在香港電腦保安事故協調中心（下稱「香港協調中心」）收集所得的數據反映出來。在二零一四年，香港協調中心收到 3 443 宗保安事故報告，較二零一三年的 1 694 宗增加超過一倍，當中仿冒詐騙事故由二零一三年的 384 宗上升至二零一四年的 594 宗，增幅為 55%。

5. 在二零一四年十月，有多個香港網站遭受一連串持續的全港性網絡攻擊。攻擊方式包括塗改網頁、入侵網絡及資訊系統，以及針對公私營機構網站的分布式拒絕服務攻擊。部分一按式分布式拒絕服務攻擊工具可經網上取得，即使沒有專門技術的人也可操作使用。其間，有些網站的正常運作受阻，但已在攻擊平息後恢復運作。

6. 現今，黑客除了發動分布式拒絕服務攻擊外，也會發動一些較複雜的網絡攻擊，包括先進的針對性攻擊、數據外泄和宣示黑客主義。去年，國際上也發生了一些矚目事故，例如黑客入侵著名的電影及娛樂企業及國際銀行，導致敏感資料外泄。本地接獲的「勒索軟件」事故數字亦持續上升，該類事故是指有人利用加密軟件把受害者的電腦檔案加密，然後索取贖金以換取解密鑰

匙。這些新興威脅，包括通過仿冒詐騙電子訊息發動的針對性攻擊，對企業及個人均帶來重大的挑戰。

<u>應對挑戰</u>

7. 政府致力採取措施，保障和加強其資訊系統及數據資產的保安。在二零一四至一五年度，政府各政策局及部門（下稱「局和部門」）共推行 114 個與資訊保安相關的項目，投放了 1.39 億元，較二零一三至一四年度推行 122 個項目所投放的 1.14 億元增加 22%。這些項目包括進行保安風險評估及審計、推行保安技術方案，以及提升保安基礎設施。

8. 政府資訊科技總監辦公室（下稱「資科辦」）與各局和部門積極合作防止惡意網絡活動，並加強防禦工作，以保護政府的資訊系統及數據資產。

9. 政府的敏感資料（包括員工的個人資料及僱用詳情）必須保密處理。對於保密資料，政府制定了嚴格的保安要求，供各局和部門遵從。所有保密資料只能在符合政府保安規例的系統上處理，而傳輸資料時亦必須加密。此外，政府也會不時檢討保密資料的保安控制工作，以配合科技發展和應對新興的網絡威脅。

10. 為提高市民的認知，資科辦與香港協調中心及保安服務供應商合作收集保安漏洞的資訊，並向公私營機構適時發布有關惡意網絡活動的警報。在二零一四年，經各種渠道（包括網站、流動應用程式及社交媒體）發布的早期預警及保安警報共有46個。

11. 我們亦協調各持份者（包括互聯網服務供應商、香港互聯網交換中心及香港互聯網註冊管理有限公司），以加強保護重要資訊基礎設施免受網絡攻擊。此外，如有需要，香港協調中心會向市民提供技術建議及協助。

保障資訊保安的主要措施

12. 面對日益增加的保安威脅及網絡攻擊，我們實施了以下措施，以加強政府內部的資訊及網絡保安：

(a) 加強保安控制及技術措施；

(b) 加強管治、風險管理及遵行規定架構；

(c) 進行網絡服務安全檢查及資訊保安事故演習；

(d) 改善電腦保安事故應變機制；以及

(e) 監測和應對網絡威脅及攻擊。

加強保安控制及技術措施

13. 資科辦從各種可靠渠道收集和分析保安情報，為各局和部門提供適時的警報及建議，以應對新興的保安威脅。在二零一四至一五年度，我們發出了 76 次嚴重網絡威脅的保安警報及三份有關資訊保安的催辦便箋，預先提醒各局和部門有關當前或即時的保安威脅，並建議他們在有需要時迅速採取防範及跟進行動。

14. 另外，各局和部門已推行多層保安措施，包括防火牆、入侵偵測及防禦系統和實時監測工具，以抵禦網絡攻擊。一旦政府網絡及網站遭受網絡攻擊，負責進行全日系統監察工作的技術人員會立即採取行動，保護政府電腦及網絡免被入侵。

加強管治、風險管理及遵行規定架構

15. 就政府內部資訊科技的使用，資科辦參照國際標準及業界良好作業模式制定政府資訊科技保安政策，並發出相關指引。有關的保安政策的對上一次檢討於二零一二年完成。因應科技進步衍生的新興保安威脅，我們已就有關政策開展了新一輪的全面檢

討工作，預期於二零一六年年底發布經修訂的資訊科技保安政策及指引。

16. 自二零一一年起，資科辦推出獨立的資訊保安遵行監測及審計機制，以評估各局和部門的遵行情況。在二零一四至一五年度，我們已完成另外八個局和部門的遵行情況審計，並將於二零一六年八月完成對所有局和部門的審計工作。

進行網絡服務安全檢查及資訊保安事故演習

17. 在二零一四年七月至二零一五年三月，資科辦為所有政府網站進行中央協調的保安漏洞掃描，並為 100 個關鍵網上應用系統進行滲透測試。通過這些工作，我們設置了中央電腦設備，並與各局和部門合作，全面檢視和檢討網站及網上應用系統的保安措施。結果顯示各局和部門均已制定有效的保安措施，以保護其網站及網上服務免受網絡攻擊。

18. 資科辦聯同警務處及各局和部門進行網絡保安演習，以加強政府應對網絡保安事故的整體應變能力。有關演習旨在讓各相關保安事故應變小組、政府人員及業務伙伴熟悉現行的保安事故

應變及處理程序。演習後亦會進行檢討和舉行分享會，讓各局和部門的負責人員學習和分享良好作業模式的經驗，務求作出改善。我們將繼續為那些擁有對公眾及香港經濟有重大影響的關鍵應用系統的局和部門安排類似的演習及相關活動。

<u>改善電腦保安事故應變機制</u>

19. 由於網絡攻擊對公共網上服務帶來威脅，資科辦加強了政府的資訊保安事故應變機制，並在二零一五年四月成立香港特區政府電腦保安事故協調中心（下稱「政府協調中心」），積極收集保安威脅資訊，並集中協調政府事故應變工作。政府協調中心也會與香港協調中心、其他區域及全球各地的電腦保安事故應變小組緊密配合，以協調各種威脅的資訊共享及事故應變工作。

20. 在公眾層面，資科辦在二零零五年成立互聯網基建聯絡小組[1]，與互聯網基建持份者緊密聯繫，並致力與業界合作，確保香港的互聯網基建能夠穩健運作。過去一年，我們啓動了保安警報機制四次，以加強監察大型活動的網絡保安和提供支援。我們積

[1]互聯網基建聯絡小組由副政府資訊科技總監(顧問服務及營運)擔任主席，成員包括資科辦、香港協調中心、警務處、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及通訊事務管理局辦公室的代表。

極聯絡各持份者，促進整體在威脅認知及情報共享方面的緊密合作。

21. 在二零一五年一月，警務處成立了網絡安全及科技罪案調查科，負責與本地及國際執法機構共同處理網絡保安事故和進行科技罪案調查。此外，該科會致力加強重要基建持份者、企業、機構及公眾對網絡保安及防止科技罪案的意識。

監測和應對網絡威脅及攻擊

22. 資科辦與香港協調中心緊密合作監察保安威脅，並向公眾發布保安警報。在二零一四年，香港協調中心發出 348 次保安公告和 126 篇保安博錄，適時向公眾提供有關當前保安威脅及保安漏洞的資訊。香港協調中心每季亦出版「香港保安觀察報告」，讓公眾了解保安事故的最新情況，並就相關防禦措施提供建議。通過與全球保安研究組織及機構的緊密合作，香港協調中心加入了全球殭屍網絡殲滅行動，以抵禦網絡攻擊和收集有關位於香港的受影響設備資料。有關工作有助公眾找出和清理隱形的殭屍網絡。

23. 為加強互聯網主要持份者的能力，我們與警務處及香港協調中心攜手合作，在二零一四年十月為互聯網服務供應商、流動網絡營運商及域名註冊服務機構舉辦資訊保安演習。是次演習的主題為「提升對網絡攻擊的應變能力」，通過各種模擬事故場景，測試了參與者在分析事故、識別惡意軟件和追蹤惡意網站方面的能力，同時測試了其事故應變處理的程序。

資訊保安認知及教育計劃

24. 人往往是資訊保安上最薄弱的環節。用戶對資訊保安的認知在應對網絡威脅方面發揮重要的作用。資科辦致力向政府人員及公眾推廣資訊保安認知及教育計劃。

提高政府人員的能力

25. 為確保政府人員在保護其系統及敏感資料方面保持警覺，資科辦在二零一四至一五年度舉辦了下列保安認知研討會及培訓項目：

(a) 為政府資訊科技人員及用戶舉行九個保安研討會及

展示會，以提高他們對保安的認知，並介紹最新的資訊科技保安技術及解決方案。活動內容涵蓋業界良好作業模式、流動技術與網絡安全、數據保護、端點保護及抵禦分布式拒絕服務攻擊的解決方案；

(b) 為部門的資訊科技保安主任舉辦兩個研討會，更新他們對資訊保安的知識，並介紹政府應對網絡保安威脅及採取風險緩解措施的最新方法；以及

(c) 為 800 名政府資訊科技人員安排八個有關網上應用系統保安的專業培訓及分享會。有關活動主要圍繞網站及網上應用系統的常見弱點，並提供實用建議，以便作出相應改善，提升資訊保安水平。

26. 我們將繼續安排相關培訓及分享活動，提高政府人員的能力，確保政府內部的資訊安全。

<u>提高市民對資訊保安的認知</u>

27. 為了提高市民對資訊保安重要性的認知，我們通過各種宣傳渠道，以及與業界合作接觸不同的對象。去年的宣傳計劃主題是「共建安全網絡」及「資訊保安由我做起」。宣傳內容包括網

絡保安發展趨勢、網絡罪行及其預防措施、資訊保安管理的良好作業模式、保護個人資訊和電腦設備的保安提示等。計劃的對象則包括企業（特別是中小型企業）、資訊及通訊科技從業員、教師、學生、學校技術支援人員及市民大眾。有關詳情如下：

(a) 在「共建安全網絡」活動中，我們舉辦了六個研討會，共有超過 500 人參加。這些研討會旨在提高市民對資訊保安的認知，以及推動他們採用保安方面的良好作業模式；

(b) 我們為中小型企業舉辦了保安研討會和設置展覽攤位，以提高他們對網絡罪行的認知，同時讓他們更了解保護資訊系統及數據資產的需要及措施；

(c) 政府高級官員亦參加了 15 個由業界舉辦的保安研討會，與資訊及通訊科技從業員分享新興威脅的趨勢，以及資訊保安管理方面的良好作業模式；

(d) 我們探訪了 10 間學校，協助逾 2 000 名學生提高他們對網絡保安的認知，並為約 600 名教師、學校職員、技術支援人員及學生舉辦資訊保安週及培訓，加強他們在保護數據、系統及網絡方面的知識；

(e) 為了鼓勵市民積極採取保安措施防禦網絡威脅，我們舉辦了以「資訊保安由我做起」為主題的四格漫畫創作比賽。比賽反應熱烈，共收到逾 1 800 份作品，涵蓋資訊保安的不同課題。我們在網站、報章上公布獲獎作品，並將之製成小冊子，分發給公眾及學校；

(f) 在二零一五年一月，我們推出「網絡安全資訊站」專題網站(www.cybersecurity.hk)，旨在為公眾提供實用的提示、建議及有用的工具，以保護他們的電腦設備及網站。通過網站提供的資料，企業及個人可加深認識網絡世界潛在的保安風險，以及防禦網絡攻擊的保安措施；

(g) 為了推廣正確的上網習慣，以保護個人資料及電腦，我們自二零一五年二月起，在本地電視及電台頻道播出新一輯的政府宣傳短片及聲帶；以及

(h) 我們也利用社交媒體，包括 YouTube 及 Twitter 分享網絡保安的良好作業模式，以及推廣即將舉行的保安研討會及活動。

28. 在二零一五年，我們將舉辦「網絡保安、四面八方」圖像

設計比賽。我們會繼續與專業機構合作，加強網絡安全資訊站的內容，提供更多網絡保安的實用建議，並利用各種宣傳渠道，推廣和教育市民認識網絡保安的重要性。

推廣資訊保安標準及良好作業模式

29. 資訊保安標準由國際標準組織制定，訂定應對保安威脅的作業模式及措施。為有效進行保安管理，政府採用了一系列資訊保安的標準，例如國際標準化組織（ISO）／國際電工委員會（IEC）27001 標準，以及應用相關技術。我們鼓勵公私營機構採用這些標準，加強其員工對資訊保安的意識，提升保安工作效率，並更了解持續改善保安措施的需要。

30. 為了進一步加強各持份者對雲端運算服務和保安標準的認知，我們繼續通過工作坊、專家組會議及雲資訊入門網站（www.infocloud.gov.hk）推廣發展和採用雲端運算。在二零一五年四月，我們參考 ISO 發布的最新標準，發表了「資訊保安管理系統 ISO/IEC 27000 標準系列概論」，以推動香港更廣泛採用資訊保安標準。

加強本地及國際層面的合作

31. 政府與私營機構需要在網絡保安事宜上建立緊密的合作關係。就此，我們舉辦了資訊分享會，與本地業界共同探討企業面對的保安問題，收集業界所知個別事故和威脅的資訊，同時分享採取防禦措施的經驗。在二零一四年十二月，我們聯同重要資訊基礎設施持份者，以及電訊、互聯網服務及數據中心行業持份者，舉行了兩次圓桌會議。有關會議匯集了與會者就應對保安挑戰及潛在威脅所提出的真知灼見及實用建議。我們會繼續與本地業界保持緊密合作。

32. 為了促進政府與國際保安專家的合作，以分享資訊保安的經驗，並增進對新興網絡威脅、保安漏洞及合適風險緩解技術的知識，資科辦通過積極參與全球保安事故協調中心組織，以及負責國家／地區電腦保安事務的電腦保安事故緊急應變小組年會，與其他政府及國際機構保持緊密聯繫。會議討論內容圍繞國際標準的發展、全球資訊及通訊科技保安政策，以及有關網絡罪行的項目及研究。

總結

33. 我們會繼續保持警惕和注意當前的資訊保安威脅，採取各項措施，保護政府資訊系統及數據資產，並提高市民的認知，維護本地網絡環境的安全。

商務及經濟發展局

政府資訊科技總監辦公室

二零一五年七月