2016 年 12 月 12 日
討論文件

立法會資訊科技及廣播事務委員會

資訊保安的最新情況

目的

本文件向委員匯報政府各項資訊保安計劃的進展及發展。

背景

2. 香港是全球最自由的經濟體，擁有先進的資訊及通訊科技基礎設施。隨着智能手機、流動裝置及雲端服務的蓬勃發展和廣泛應用，香港社會在經濟發展、創業營商及日常生活上越來越倚賴資訊及流動通訊科技。正因爲資訊科技發展日新月異，智能裝置愈趨普及，資訊保安及網絡攻擊所帶來的威脅亦為企業及其他互聯網用戶帶來影響，例如可能被黑客盜取有價值的資訊或破壞電腦系統的正常運作。因此，所有持份者（包括政府、企業及個人）均須了解網絡環境的風險，學習有關知識，並採取適當措施保護其資訊資產和電腦系統。

3. 本文件就以下主要範疇匯報有關資訊保安的最新發展：

(a) 資訊及網絡安全的形勢；
(b) 政府如何應對網絡安全威脅的措施；
(c) 社會如何應對網絡安全威脅的措施；以及
(d) 公眾認知及人力資源發展。

資訊及網絡安全的形勢

4. 香港電腦保安事故協調中心（下稱「香港協調中心」）在2016年1月至10月期間共收到5 146宗保安事故報告，較2015年全年的4 928宗增加接近4%。同時，根據香港警務處（下稱「警務處」）的統計數字，警方在2016年首三季共收到4 537宗科技罪案報告，雖然數字較2015年首三季的5 333宗略為減少，但預計的財務損失金額已超越去年全年的18億元至大約19億元。有關科技罪案和保安事故的分項數字載於附件。雖然黑客入侵／網頁塗改、仿冒詐騙、殭屍網絡和分散式阻斷服務攻擊事故的數字呈下降趨勢，但本地勒索軟件的事故則顯著上升，2016年首十個月的相關事故報告為278宗，是去年全年51宗的五倍，顯示惡意軟件的活動相對活躍。上述情況反映出網絡威脅的方式不斷變化，故此，風險的評估和應對方式也必須隨之改變。

5. 大數據、雲端運算、人工智能、流動裝置與物聯網等科技不斷進步，使全球的網絡威脅方式變得更加層出不窮。根據多份資訊及網絡保安業界最近發表的報告[1]，惡意軟件在2016年於全球各地迅速蔓延，其數量和種類急劇增加，而功能和複雜性亦不斷提高。全球的網絡威脅形勢與香港的情況亦很相似，當中勒索軟件的事故報告在過去一年大幅上升，保護電腦數據成為資訊保安的焦點。作為一個資訊發達的城市，香港亦無可避免受到威脅，而個人、企業，以至政府都可能成為攻擊目標。

6. 有見及此，政府、企業及個人都必須做好準備，以應付突如其來的網絡攻擊，同時要加強保安策略，以便更有效應對挑戰。除了加強及定期更新資訊保安防護系統外，個人的資訊保安意識和知識，以及專業的資訊保安團隊都在資訊保安防禦戰中發揮重要的作用。網絡黑客可以從世界上任何地方影響數以百萬計的用戶，因此我們需要加強國際合作，分享情報及

---

[1] "2016 Midyear Security Roundup", Trend Micro Inc.
"Special Report: Ransomware and Businesses 2016", Symantec Corporation.
"H1 2016 Global and Regional Trends of the 'Most Wanted' Malware", Check Point Software Technologies Ltd.

協調對可疑活動的調查工作，識別新興的威脅趨勢及網絡攻擊。政府非常注重不斷變化的網絡威脅，會繼續採取各種措施增強政府的網絡安全，下文各段詳細介紹有關工作。

政府如何應對網絡安全威脅的措施

7. 政府一直密切注視網絡攻擊的趨勢及有關的保安威脅。政府內部已採用多層保安措施抵擋網絡安全威脅。通過收集由網絡安全業界及各地電腦保安事故緊急應變小組發出的網絡威脅訊息，政府資訊科技總監辦公室（下稱「資科辦」）會適時向各決策局和部門（下稱「局和部門」）發出保安警報及催辦便箋，並協助政府資訊科技管理人員及各局和部門的資訊保安事故應變小組，作出緊急應變及加強防範措施。資科辦亦通過定期舉辦研討會和培訓，加強各級人員對相關網絡攻擊的認知，提升資訊保安技能，以增強各局和部門預防網絡攻擊的能力。

政府內部應對惡意軟件的措施

8. 在2016年1月至10月，資科辦向各局和部門共發出了72次嚴重保安警報及16份有關加強資訊保安措施的催辦便箋，其中包括兩份針對勒索軟件的資訊保安指引，促請各局和部門採取有效和迅速的應對措施，並提醒所有員工不要開啟可疑電郵及其附件和連結，以防止電腦遭受感染。資科辦亦提醒各局和部門利用抗惡意程式軟件，定期掃描電腦系統及備份電腦資料，並將其離線保存。

風險評估及審核

9. 面對日益增加及愈趨複雜的網絡安全威脅，資科辦會定期檢討相關保安規定。我們參照最新版的ISO 27001國際標準及業界良好作業模式，檢討《政府資訊科技保安政策及指引》，包括加強儲存敏感資料的保密要求、提升部門應對資訊保安事故的領導水平、檢討資訊保安技術及偵測新興網絡攻擊的能力，以應對不同類型的資訊保安威脅及網絡攻擊。

10. 為評估各局和部門就《政府資訊科技保安政策及指引》的遵行情況，自2011年起，資科辦為所有局和部門進行獨立的資訊保安「遵行監測」及審計，並在評估過程中，協助有關部門持續改善保安管理系統，以應對新興保安威脅。我們將會在2016年年底開展新一輪保安「遵行審計」。此外，資科辦亦提供軟件及設備，讓各局和部門定期為其網站掃描保安漏洞，以便及早發現潛在風險，並適時採取相應預防措施。

事故應變及保安演習

11. 政府已制定一套電腦保安事故應變機制及相關措施，並舉辦定期演習。在2016年4月至10月期間，資科辦與警務處合作為政府部門進行網絡安全演習，以加強政府應對網絡安全事故的整體應變能力。

數據保護

12. 針對數據泄漏的風險，政府已訂立嚴格的資料保安要求及應對措施，包括在儲存和傳送敏感數據及文件時，必須以業界最高標準進行加密，確保政府數據資產得到適當保護。資科辦亦就使用外置儲存裝置傳送政府文件制定實務指引及保安要求，並協助各局和部門採用適當技術加密政府數據。

13. 為了應對日趨精密及複雜的網絡安全威脅，資科辦已要求各局和部門加強在數據方面的保護，並構建系統加強政府在監測、偵察及堵截資料外泄的能力，監控網絡中的可疑流量，進行分析並在有需要時進行堵截。

國際及區域合作

14. 政府電腦保安事故協調中心透過加入國際性的「電腦緊急事故應變小組統籌中心」、「全球保安事故協調中心組織」及「亞太區電腦保安事故協調組織」，與負責其他地區的電腦保安事故緊急應變小組保持緊密聯繫，適時分享保安威脅、漏洞和保安事故的資訊，並積極參與各組織所舉辦的技術交流活動，包括將在明年3 月舉行的亞太區電腦保安事故協調演習。

15. 我們亦定期參與國際標準化組織資訊科技安全技術標準分會ISO/IEC JTC1/SC27的會議，跟進與資訊安全相關技術和標準的最新發展。

建立大數據分析平台

16. 為應對不斷增加的網絡安全威脅，資科辦亦計劃逐步加強監察網絡威脅和分享相關資訊的能力，利用大數據分析技術，構建一個網絡風險資訊共享的平台。這個平台收集和分析網絡威脅資訊及數據，檢測可能發生的事故，為各局和部門提供更針對性的網絡威脅預警訊息，並會推動與業界、企業和香港協調中心共享網絡風險資訊，提醒所有持份者（包括政府、企業及個人）及早防範，合力鞏固香港的網絡安全。

員工培訓

17. 提升員工資訊保安意識和知識有利提升政府整體的資訊保安水平，以及保護政府的資訊系統及數據資產，減低受網絡攻擊的風險。2016 年，我們為政府資訊科技人員及電腦用戶舉行了合共12 場研討會、工作坊和解決方案展示會，以提高他們對最新保安漏洞的認知及更新他們對資訊保安技術的知識。其中四場活動是針對勒索軟件的威脅，藉以增強員工在這方面的保護能力。

社會如何應對網絡安全威脅的措施

18. 資科辦與香港協調中心及業界一直保持緊密聯繫，通過不同渠道，包括網站、報章、電子傳媒、流動應用程式、公開活動及專題演講，分享有關保安威脅及漏洞的資訊，並提供保安建議，保護市民的資訊系統及數據資產。

支援中小型企業（下稱「中小企」）

19. 近年來，愈來愈多中小企利用電子商務及支付平台拓展業務。但企業的網站如果沒有足夠保安措施，有可能會被入侵或被黑客利用作釣魚網站及寄存惡意軟件。有見及此，香港協調中心於2016 年年初聯同多個本地商會，包括中華廠商聯合會、香港工業總會、香港總商會和香港中小型企業聯合會與香港生產力促進局中小企一站通，推出「中小企業網站免費保安檢查先導計劃」，向中小企推廣「檢查 - 行動 - 驗證」三個步驟，為他們的網站免費提供網站保安檢查及改進建議，並為網站提供驗證檢查以確認成效。

20. 香港協調中心已於2016 年年中完成第一輪檢查，為30 間參與的中小企提供網站安全檢查報告及免費諮詢服務，並於8 月舉辦座談會分享檢查結果及改進建議。第二輪檢查最近亦已完成，驗證各網站改進後的成效。中小企可通過該計劃了解其網站的保安風險及提升網站保安。在2017 年，資科辦將繼續與香港協調中心合辦相關活動，提升中小企的網絡安全水平。

21. 為進一步提高中小企對資訊保安的認知及對網絡安全威脅的防禦能力，我們與業界及不同機構合作，推出各項宣傳教育活動，包括專題研討會、電台節目、派發宣傳單張等，提醒企業加強網絡安全措施，保護其資訊系統和數據資產。我們亦在電台節目中播放十個系列的宣傳聲帶，涵蓋不同保安提示，促進企業和機構以最佳作業模式應對網絡安全挑戰。此外，資科辦與警務處及香港協調中心共同製作不同主題的宣傳單張，提供實用指引，協助中小企制訂相關保安措施。

22. 中小企在業務上採用雲端服務的比率近年不斷上升[2]。針對雲端服務的潛在保安風險，資科辦與工業貿易署中小企業支援與諮詢中心於2016年9月合辦「中小企雲端保安論壇」，讓中小企與資訊保安專家分享及討論有關採購和使用雲端服務時的保安考慮。

[2] "2016 Cloud Readiness Index", Asia Cloud Computing Association.

向公眾提供支援以應對惡意軟件

23. 在公眾層面，因應本港勒索軟件感染個案大幅增加，對企業和個人用戶都構成嚴重威脅，資科辦、警務處及香港協調中心以「防禦勒索軟件」為主題，為重要基礎設施營運商、企業及機構、學校及公眾分別舉辦主題研討會，讓他們更深入了解勒索軟件的感染途徑、影響和過程，並介紹有關應對勒索軟件攻擊的策略和技術。

24. 除舉辦研討會外，我們亦通過「網絡安全資訊站」、報章和電子傳媒，向中小企及公眾發放有關勒索軟件攻擊的訊息，並提供相關建議和風險緩解措施，包括一套「提防遭受勒索軟件感染」的資訊圖表，提供實用保安貼士，以供參考。此外，我們製作了一套題為「預防勒索軟件」的學習課程，提供適當的預防措施及應對方法，提醒公眾採取必要的預防措施，免受勒索軟件攻擊。

公眾認知及人力資源發展

加強青年人對資訊保安的認知

25. 隨着流動智能裝置和無線網絡普及，加上學校推行電子學習，青年人及學生有更多機會接觸互聯網及電腦設備。因此，向他們推廣資訊保安訊息更形重要。今年，資科辦繼續與資訊保安專業團體合作，在2016年1月至10月進行共30次學校探訪，接觸近10 000名學生及教師。

26. 此外，為提高全港各小學、中學及大專學生安全使用互聯網及社交媒體的意識，並發掘電腦科技人才，警務處與香港大學在2016年5月至7月期間聯合舉辦首屆香港「網絡安全比賽2016」，藉此推廣「網絡安全，由青少年做起」的訊息。我們亦會繼續安排學校探訪及其他活動，向本地青少年灌輸資訊保安的知識及正確使用互聯網的態度。

推動資訊保安業界的發展和合作

27. 資科辦積極鼓勵業界參與不同類型的網絡安全活動，了解最新保安威脅及保護措施，以加強他們在網絡安全方面的專業能力。我們在2016年4月舉辦了「2016香港—內地網絡安全論壇」，邀請香港及內地網絡安全專家就金融技術、雲端運算、大數據等方面所面對的網絡安全挑戰及當中的技術解決方案，向超過200名業界從業員作詳盡分析。

28. 為表揚出色的資訊保安管理和從業員對業界的貢獻，資科辦、警務處及香港協調中心在2016年9月合辦「網絡安全精英嘉許計劃」，鼓勵對資訊保安行業有貢獻的人士交流分享，提升業界保障網絡安全的能力。計劃首次舉辦已收到超過160份提名，評審工作現正進行中，頒獎禮將在明年1月舉行。

公眾認知

29. 資科辦致力向社會各界推廣資訊保安認知，定期與警務處、香港協調中心及其他專業團體舉辦不同的網絡安全推廣活動，當中包括「共建安全網絡」年度活動，以提升公眾的保安意識和能力。今年，我們亦安排了三場公眾研討會，讓社會大眾多了解網絡攻擊的趨勢，提醒他們在網上交易時要注意的風險，並鼓勵他們加強對個人和敏感數據的保護。

30. 除了舉辦公眾研討會外，我們在4月至7月期間舉辦了以「數據安全 交易放心」為主題的吉祥物設計比賽，宣傳如何保護電腦裝置、避免墮入網絡陷阱，以及保障數據和網上交易安全的重要性。比賽反應熱烈，共收到2 000份作品，頒獎禮已於11月底舉行。

31. 為了讓一般用戶、中小企以及學校接收到更多最新的保安資訊，資科辦不斷豐富「網絡安全資訊站」專題網站的內容，例如提供資訊保安公眾活動的消息、專家之言，以及由專業機構所提供的資訊保安故事等，為公眾提供實用的提示和建議有用的工具，以保護他們的電腦設備及網站。透過「網絡安全資訊站」，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。

32. 資科辦一直密切關注最新網絡安全威脅的情況。因應流動支付服務相繼推出、手機遊戲程式的發展，以及近期有關物聯網裝置衍生的網絡安全事故，我們在不同研討會和「網絡安全資訊站」均加入了相關的課題和內容，介紹使用手機遊戲、流動支付服務及家居網絡裝置時的保安風險，並提供適當的預防措施及應對方法，減低相關風險。

總結

33. 網絡攻擊不再是獨立的事件，網絡威脅亦無分國界，不斷演變。我們需要與本地及全球相關組織和專業團體保持緊密聯繫及加強分享資訊，持續偵測及了解不斷變化的網絡威脅，研究可行的預防及應對措施，使政府及各界能更有效就新興的網絡威脅做好準備。我們會繼續保持高度警惕，留意當前的保安威脅，並採取各項措施，保護政府的資訊系統和數據資產，提高社會各界的保安認知，與各持份者攜手保護香港的網絡環境。

創新及科技局
政府資訊科技總監辦公室
2016 年 12 月

附件

電腦保安事故及科技罪案的統計數字

香港協調中心處理的電腦保安事故

	2015		2016 (截至 10 月)	
黑客入侵／網頁塗改	151	*3%*	76	*1%*
仿冒詐騙	1 978	*40%*	1 635	*32%*
殭屍網絡	1 943	*39%*	1 611	*31%*
分散式阻斷服務攻擊	130	*3%*	94	*2%*
惡意軟件 (其中勒索軟件所佔數字)	277 (51)	*6%*	1 065 (278)	*21%*
其他	449	*9%*	665	*13%*
總數	**4 928**	***100%***	**5 146**	***100%***

香港警務處 - 有關科技罪案及其導致的財務損失

案件性質	2015 年	2016年 (截至9月30日)
與網上遊戲有關	416	304
網上商業騙案	1 911	1 217
非法進入電腦系統	1 223	847
其他性質	3 312	2 169
(i) 網上雜項騙案	*1 733*	*1 133*
(ii) 兒童色情物品	*53*	*27*
(iii) 分散式阻斷服務(DDoS)攻擊	*35*	*4*
(iv) 網上銀行	*3*	*2*
(v) 裸聊	*1 098*	*588*
(vi) 其他	*390*	*415*
總計	**6 862**	**4 537**
損失(百萬元)	**1,828.9**	**1,865.2**