2018 年 2 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

本文件向委員匯報本港資訊保安的最新情況和政府推行的有關措施。

背景

2. 香港是國際及區域的主要金融和商業中心，擁有先進的資訊及通訊科技設施。隨着網上服務、流動支付、雲端服務及智能家居等新興科技應用迅速發展，數碼訊息的傳遞變得更頻密，相關的資訊保安風險亦持續增加。

3. 政府十分重視本港的資訊保安，一直密切監察網絡攻擊的趨勢及安全威脅，適時作出應對和加強防禦措施，並通過各種渠道，讓各持份者（包括政府、企業及個人）更深入了解資訊保安的趨勢及網絡環境變化，以便採取有效措施保護其電腦系統和資訊資產。

4. 本文件就以下主要範疇匯報資訊保安的最新發展和過去一年政府在資訊保安方面的工作情況：

(a) 資訊及網絡安全的形勢；
(b) 政府應對網絡安全威脅的措施；
(c) 社會層面的資訊保安措施；以及
(d) 專業培訓及公眾認知。

資訊及網絡安全的形勢

5. 2017年，全球性的電腦保安事故時有發生。根據一間網絡安全產品公司發表的報告，2017年首六個月全球勒索軟件的攻擊次數與2016年同期相比增加接近一倍。繼影響廣泛的

WannaCry後，亦有其他勒索軟件（如Petrwrap）出現，顯示勒索軟件的功能、複雜性和手法不斷演變。另外，無線網絡加密通訊協定(WPA2)和電腦中央處理器設計相繼發現漏洞。這些漏洞都可能引發黑客攻擊，導致資料被竊取。各類電腦保安事故不斷發生，大大增加各持份者應對資訊及網絡威脅的難度，亦提高了公眾對各行各業保護敏感資訊的關注。

6. 整體而言，香港的資訊保安事故在2017年有上升趨勢。香港電腦保安事故協調中心（「香港協調中心」）全年共收到6 506宗保安事故報告，較2016年的6 058宗上升約7%。當中，惡意軟件攻擊的數目增至2 041宗，較2016年大幅上升79%，與殭屍網絡（2 084宗）及釣魚網站（1 680宗）成為本港最主要的網絡安全事故類別。在2 041宗惡意軟件攻擊中，勒索軟件共有1 388宗[1]。

7. 另一方面，香港警務處（「警務處」）在2017年錄得5 567宗科技罪案，相關損失金額約為14億元，兩項數字與2016年相比均有所下降。有關電腦保安事故和科技罪案的分項數字載於附件。

政府應對網絡安全威脅的措施

保安措施及威脅警報

8. 政府資訊科技總監辦公室（「資科辦」）密切監察政府網絡系統的日常運作，並監測、偵察及堵截潛在惡意攻擊，確保政府電腦系統正常運作。政府內部已採用多層保安措施，包括防火牆、入侵偵測及防禦系統、垃圾郵件過濾系統、防電腦病毒方案及實時監測工具，以抵禦外來的網絡攻擊。

9. 為進一步保護政府網站，資科辦在2017年為超過120個政府網站設置加密通訊協定，防止公眾在瀏覽政府網站時被黑客偷取或篡改資料。同時，為加強政府互聯網服務的網絡安

[1] 包括 178 宗勒索軟件報告及 1 210 宗 Bot-WannaCry 個案，後者涉及本地電腦感染了去年 5 月肆虐全球的 WannaCry 加密勒索軟件，唯其加密程式未有啓動，故未造成實際損失。

全，資科辦在2017年下半年亦為其託管的政府互聯網域名安裝數碼簽署，以防止公眾被連接至仿冒網站。

10. 2017年，資科辦向各局和部門合共發出87次關於電腦系統或軟件漏洞的保安警報，提醒他們採取管理及技術措施，例如適時安裝修正檔案和更新系統或軟件的版本；並協助各局和部門為超過500個政府網站進行測試，堵塞保安漏洞，以保護政府網站及數據。

檢討指引及審核

11. 參照最新國際標準(ISO/IEC 27001/27002)及業界良好作業模式，資科辦在2016年年底完成《政府資訊科技保安政策及指引》的檢討工作，並頒布經修訂的政策及指引，在個別保安範疇加強要求，以及更新和編製新指引。經修訂的政策及指引已上載於資科辦的網站，供公眾及企業參考。

12. 為評估各局和部門就《政府資訊科技保安政策及指引》的執行情況及提供改善建議，資科辦在2016年年底開展新一輪保安「遵行審計」工作。2017年，資科辦已為15個局和部門完成「遵行審計」，整個項目預計於2019年年中完成。

事故應變及保安演習

13. 政府已制定一套事故應變機制及措施，並定期進行演習。在遇到保安事故時，例如針對個別局和部門網站的攻擊，有關部門須即時向資科辦的政府資訊保安事故應變辦事處通報及提交事故調查報告，並立即報警，以便警方跟進調查。

14. 為加強政府對網絡安全事故的整體應變能力，資科辦聯同警務處分別在2017年1月及2018年1月舉辦跨部門網絡安全演習，共有約60個政府部門參與，在多個模擬環境下體驗如何有效應對網絡安全事故，以加強政府部門保護資訊系統和處理網絡安全事故的能力。演習會每年恆常舉辦。

國際及區域合作

15. 政府電腦保安事故協調中心（「政府協調中心」）一直與各地電腦緊急事故應變小組合作，包括加入「電腦緊急事故應變小組統籌中心」(CERT/CC)、「全球保安事故協調中心組織」(FIRST)及「亞太區電腦保安事故協調組織」(APCERT)。為加強交流合作及通報資訊保安情報，政府協調中心積極參與不同組織舉辦的相關活動，包括由「國家計算機網絡應急技術處理協調中心」(CNCERT/CC)舉辦的「中國網絡安全年會」、CERT/CC及FIRST舉辦的年會，以及APCERT舉辦的年度聯合事故應變演習。

網絡風險資訊共享平台

16. 有見網絡安全威脅不斷增加，資科辦於2017年4月在政府內部推行網絡風險資訊共享平台先導計劃，利用大數據分析技術收集和分析不同來源的網絡安全威脅資訊，進行整理和評估，為各局和部門提供更具針對性的網絡安全威脅預警。

員工培訓

17. 政府致力提升員工的資訊保安意識及知識。2017年，資科辦舉辦了多個研討會及解決方案展示會，為超過1 600名部門管理層人員及資訊保安相關員工提供適切的培訓和學習機會。這些活動涵蓋業界良好作業模式、勒索軟件及流動應用程式安全等課題。資科辦計劃在2018年繼續舉辦有關培訓，以提升政府人員在網絡安全方面的知識及技能。

社會層面的資訊保安措施

18. 在社會層面，資科辦與香港協調中心及不同持份者緊密合作，為不同行業提供有關網絡安全的支援。警務處轄下的網絡安全及科技罪案調查科（「網罪科」）致力打擊科技罪行和提升重大網絡安全或大規模網絡攻擊事故的應變能力，並適時進行網絡安全威脅的審計及分析，以防止及偵查針對重要基礎設施的網絡襲擊。網罪科一直採用多機構合作模式，加強重要基礎設施及企業資訊系統網絡的可靠性，以及提升香港保護

資訊系統網絡和防禦網絡攻擊的能力。香港協調中心亦會與提供互聯網服務的機構合作，推廣資訊保安良好作業模式，推動香港成為安全的互聯網樞紐。

支援個別行業對網絡安全的認知和防禦

19. 基於近月接連發生涉及旅行社的網絡安全事故，香港協調中心正為旅遊業及其他行業（例如零售業及基金管理業等）舉辦專題講座，加強相關行業對網絡安全的認知和防禦攻擊的能力。同時，香港旅遊業議會亦將推出多項措施，進一步提高旅行社對網絡風險的意識，例如為會員舉辦網絡安全講座、向會員發出通告、重申網絡安全的重要等，藉此增強會員的網絡防衛及應對資訊保安事故的能力。香港協調中心亦會繼續與各大行業商會合作，向業界宣傳及推廣網絡安全的重要性。

提升應對勒索軟件攻擊的能力

20. 鑑於近年勒索軟件攻擊有上升趨勢，資科辦通過「網絡安全資訊站」(www.cybersecurity.hk)發放提防勒索軟件的實用建議。香港協調中心亦在報章專欄撰文，提醒公眾有關保安風險及防禦方法，並在其網站設立勒索軟件專頁，深入介紹不同種類勒索軟件的入侵途徑及影響。

21. 政府協調中心及香港協調中心在2017年9月合作推出「齊抗勒索軟件運動」，舉辦公眾講座及在社交媒體設立「勒索軟件情報站」[2]，分享勒索軟件的最新情報和分析、保安警示及培訓資訊等。截至2017年12月已舉辦四次公眾講座，並發布近30篇文章。

支援中小企

22. 為加強中小企的長遠競爭力，政府於2016年11月在創新及科技基金下以先導形式推出五億元的科技券計劃，資助中小企使用科技服務及方案，提高生產力或升級轉型。科技券計

[2] www.facebook.com/ransomware.hk

劃亦涵蓋網絡安全方案，為中小企提供防禦網絡攻擊的方法及運作復原方案，藉此減低中小企在資訊系統方面蒙受損失的風險。先導計劃為期三年，以二對一的配對形式為每間合資格中小企提供最多20萬元資助。

23. 中小企在業務上採用雲端運算服務的比率近年不斷上升。針對雲端運算服務的潛在保安風險，資科辦在其雲端運算專題網站上載優質資訊科技專業服務常備承辦協議及雲端運算的服務承辦商資料，以及雲端運算服務的保安及採購指引等，供中小企參考。

24. 為更有效向中小企傳達不同範疇的資訊保安知識和推廣良好作業模式，資科辦在2017年製作了多個系列的宣傳訊息在不同電子媒體播放，內容涵蓋如何提升網站安全、防禦勒索軟件及應對分散式阻斷服務攻擊等保安提示，鼓勵中小企採用良好作業模式應對網絡安全挑戰。

專業培訓及公眾認知

專業人員培訓和表揚

25. 警務處、政府協調中心及香港協調中心自2016年起聯合舉辦「網絡安全精英嘉許計劃」，表揚傑出的資訊科技管理人員及從業員對業界的貢獻，並鼓勵資訊保安行業的人員交流經驗，提升行業網絡安全防護能力。第二屆「網絡安全精英嘉許計劃」頒獎典禮將會在2018年2月舉行。

26. 在職業培訓方面，香港生產力促進局、香港協調中心及政府協調中心不時聯同業界機構舉辦會議、專題研討會和工作坊，包括資訊保安證書課程及「資訊保安高峰會」年度活動，以提升資訊科技人員的資訊保安技術及知識。

27. 政府亦鼓勵大專院校在資訊科技相關學科提供更多資訊保安課程，並繼續聯同資訊保安專業團體向資訊科技人員推廣專業認證，以培訓更多具備資訊保安專業知識及技能的人員，鼓勵資訊科技從業員投身資訊保安專業。

加強青年人對資訊保安的認知

28. 隨着流動裝置、雲端服務及社交網絡的普及，青年人及學生有更多機會接觸互聯網及資訊科技設備。因此，加強他們對資訊保安的認知更形重要。資科辦與資訊保安專業團體合作舉辦學校探訪及「資安探訪團」活動，在2017年進行了32次學校探訪，接觸近萬名學生、家長及教師。資科辦會繼續安排學校探訪，向他們灌輸資訊保安的知識及正確使用互聯網的態度。

29. 另一方面，政府積極通過舉辦不同活動，培養青年人對資訊保安的興趣，發掘電腦科技人才。為推廣「網絡安全，由青少年做起」的訊息，警務處與香港大學繼續合辦「網『樂』安全比賽」。比賽分大、中、小學組進行，共吸引近7 600名學生參與，內容包括網上問答比賽、分析模擬電腦內的保安漏洞和製作有關網絡安全的專題報告。

公眾認知

30. 隨着智慧城市的發展，互聯網裝置變得更普及和多元化。資科辦、警務處及香港協調中心以「智慧家居 安全生活」為主題，在2017年4月及9月舉辦了兩場網絡安全研討會，讓企業、學校及大眾了解與互聯網裝置相關的風險，提醒他們對保安漏洞保持警惕，以及採取適當保安措施保障這些裝置及數據的安全。2017年9月舉辦的研討會講題包括防禦勒索軟件、安全使用流動支付及社交媒體等。除了舉辦研討會外，資科辦亦通過不同渠道，包括社交媒體、研討會、論壇、資料單張或小冊子、電視及電台廣播、學校探訪等，向公眾發放有關勒索軟件攻擊的訊息，提供相關實用建議及風險緩解方案。

31. 為進一步協助大眾應對網絡安全威脅，資科辦製作了「提防遭受勒索軟件感染」、「安全網上購物」及「家居網絡安全有辦法」等資訊圖表，提供簡單實用的保安貼士供大眾參考。資科辦亦在「網絡安全資訊站」發布主題為「預防勒索軟件」及「安全使用流動支付服務」的學習課程。政府會繼續通過「資訊安全網」及「網絡安全資訊站」網站及其他宣傳渠道，向公眾發布有關資訊保安的參考資料及訊息。

展望

32. 資科辦會繼續推動與業界、企業及香港協調中心共享網絡風險資訊，加強通報網絡安全威脅，聯手防禦網絡攻擊。資科辦將於2018年第二季開展由資訊保安持份者參與的「網絡安全資訊共享夥伴試驗計劃」，並在下半年推出其網絡安全資訊共享平台，促進公私營機構的網絡安全資訊共享，以提高香港整體應對網絡攻擊的防衞及復原能力。

33. 物聯網及電子支付等新興科技發展迅速，在促使社會不斷創新的同時，亦帶來不同的網絡安全威脅。故此，各持份者絕對不能掉以輕心。政府會繼續就新興科技（包括雲端運算、大數據分析、物聯網、金融科技及人工智能等）的風險及威脅，加強各局和部門、業界和公眾的認知，並參考其他地區的相關政策、國際標準及業界良好作業模式，制定和更新相關的資訊保安規定及技術要求。

創新及科技局
政府資訊科技總監辦公室
2018 年 2 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

	2016		**2017**	
黑客入侵／網頁塗改	82	*1%*	26	*<1%*
仿冒詐騙(釣魚網站)	1 957	*32%*	1 680	*26%*
殭屍網絡	2 028	*34%*	2 084	*32%*
分散式阻斷服務攻擊	148	*2%*	54	*1%*
惡意軟件（其中勒索軟件所佔數字）	1 139 (309)	*19%*	2 041 (1 388)	*31%*
其他	704	*12%*	621	*10%*
總數	**6 058**	***100%***	**6 506**	***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	**2016 年**	**2017年**
與網上遊戲有關	363	311
網上商業騙案	1 602	1 996
非法進入電腦系統	1 107	822
其他性質	2 867	2 438
(i) 網上雜項騙案	*1 563*	*1 542*
(ii) 兒童色情物品	*43*	*29*
(iii) 分散式阻斷服務攻擊	*6*	*9*
(iv) 網上銀行	*2*	*0*
(v) 裸聊	*697*	*305*
(vi) 涉及勒索軟件的勒索案	*63*	*43*
(vii) 其他	*493*	*510*
總計	**5 939**	**5 567**
損失(百萬元)	**2,300.8**	**1,393.0**