2019 年 2 月 18 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整體資訊保安的最新情況和過去一年政府在資訊保安方面的工作。

背景

2. 資訊科技的普及提升了我們的生活質素，帶來不少機遇，但同時亦帶來挑戰。香港要成為安全的智慧城市，資訊保安風險實不容忽視。政府、本地企業和機構及市民均須時刻保持警覺，並保護其資訊系統和數據資產。現今網絡攻擊日趨頻繁，攻擊手法亦層出不窮，企業或機構單憑自身能力未必能應付不斷演變的網絡威脅。因此，各行各業須建立緊密的協作關係，共享網絡安全資訊，並積極了解資訊保安的新趨勢，以及早防範和應對網絡攻擊。政府資訊科技總監辦公室（「資科辦」）一直通過多管齊下的策略應對資訊保安的事宜，包括：設立香港電腦保安事故協調中心（HKCERT,「事故協調中心」）發布網絡安全事件及保安建議、保障政府資訊系統及重要資訊基礎設施、培育網絡安全的專業人才，以及加強公眾教育。

3. 政府在2001年成立由香港生產力促進局管理的「事故協調中心」，為本港企業及互聯網用戶提供電腦保安事故相關的服務，包括收集有關資訊保安威脅的資訊，向公眾發布最新資訊以提高他們的保安意識，和就一些重要的保安威脅（如釣魚攻擊及勒索軟件）提供應對的建議。資科辦亦積極參與全球性及區域性的電腦保安事故應變組織，例如參與「全球保安事故協調中心組織」（FIRST），並與其他地區的電腦保安事故協調中心保持

緊密聯繫，以便更迅速和全面地掌握網絡安全資訊，並作出適切防範。

資訊保安的整體形勢

4. 根據一份業界的報告[1]，2018年首6個月仿冒詐騙及資料外泄事故在全球均呈上升趨勢。香港的資訊保安形勢亦大致相同，整體的保安事故宗數在2018年有所上升。「事故協調中心」在2018年共收到10 081宗保安事故報告，較2017年的6 506宗上升約55%。當中三個主要類別，即殭屍網絡（3 783宗）、惡意軟件（3 181宗[2]）及仿冒詐騙（2 101宗）事故的宗數均有明顯上升。

5. 另一方面，香港警務處（「警務處」）在2018年共錄得7 838宗科技罪案，相關損失的總金額增至約27.7億元，較2017年全年的13.9億元上升接近一倍，而每宗平均損失金額亦明顯增加。科技罪案數字上升主要由於網上騙案、網上勒索及盜用電腦個案的增加。其中亦有數宗涉及外泄大量企業擁有的客戶資料。有關保安事故及科技罪案的分項數字載於附件。

社會層面的資訊保安措施

提升本港企業應對各種網絡攻擊的能力

6. 根據香港生產力促進局在2018年進行的調查，來自6個行業共350家受訪的本港企業（包括中小企）為確保業務運作暢順和數據資產安全，已採取基本的資訊保安措施應對網絡攻擊，惟在保安管理和主動性方面仍有進步空間。為了進一步加強企業的保安管理，資科辦、警務處及「事故協調中心」向不同行業提供了不同支援。

---

[1] 2018 Midyear Security Roundup: Unseen Threats, Imminent Losses, Aug 2018, TrendMicro (https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/unseen-threats-imminent-losses)

[2] 這包括 114 宗勒索軟件報告及 2 426 宗 Bot-WannaCry 個案；後者涉及本地電腦感染 2017 年 5 月肆虐全球的 WannaCry 加密勒索軟件，但有關加密勒索程式未有啓動，故受感染的電腦沒有實際損失。

7. 資科辦及「事故協調中心」一直密切監察網絡攻擊的趨勢及相關保安威脅，並適時提醒各機構和市民保持警覺，為其電腦設備和數據資產做好保安措施。過去一年，「事故協調中心」共發布93項相關保安建議及指引，範圍包括堵塞產品漏洞、應對勒索軟件，以及預防殭屍網絡等。

8. 因應個別行業遭受網絡攻擊的情況，「事故協調中心」與相關行業商會（例如香港投資基金公會、香港零售管理協會及香港旅遊業議會等）合作，向業界宣傳網絡安全的重要性，推廣資訊保安良好作業模式，並且促請其成員機構做好資訊保安風險管理，採取各種最新防範措施，妥善處理和保障顧客的個人資料，以增加市民對網上服務的信心。警務處亦定期舉辦資訊保安研討會，提升銀行及金融、交通及航運、通訊、公共服務等界別應對網絡安全事故的整體防禦能力。

9. 為協助中小企以有限的資源應對潛在的資訊保安風險，「事故協調中心」及資科辦經常聯同業界組織舉辦相關會議、專題研討會及工作坊，涵蓋的課題包括雲端計算和人工智能的應用。資科辦及「事故協調中心」於2018年就中小企經常遇到的資訊保安問題，製備多個系列的宣傳訊息（例如提防電郵騙案和防禦惡意軟件等），通過不同渠道如社交及電子媒體發布。

10. 創新科技署在2018年2月擴大「科技券計劃」的資助範圍及資助額。現時所有本地非上市公司（包括中小企）均可申請資助，採購防禦網絡攻擊和系統修復的服務和方案，藉此進一步減低資訊保安的風險。

「網絡安全資訊共享夥伴試驗計劃」

11. 資科辦在2018年9月開展為期兩年的「網絡安全資訊共享夥伴試驗計劃」（「夥伴試驗計劃」），並牽頭設立了一個跨行業的「網絡安全資訊共享協作平台」（Cybersechub.hk）。「夥伴試驗計劃」的成員可以通過這個平台全面交流網絡安全威脅、緩解方法、良好作業模式等資訊，並適時向公眾發布有關訊息。平台亦將加入人工智能元素，協助整合和分析網絡安全資訊，藉此提升共享資訊的效率。

12. 截至2018年年底，已經有超過100間機構加入「夥伴試驗計劃」。我們會繼續促進更多不同界別的機構加入，並持續收集意見以完善計劃。我們會於今年下半年檢討「夥伴試驗計劃」的運作及成效，以便訂定有關計劃的長遠路向。

公眾認知及教育

13. 隨着近年資訊及通訊科技設備和電子支付服務的普及，相關的仿冒詐騙攻擊（包括欺詐網站及偽冒電郵）有所增加，手法亦層出不窮。因應最新的事故及趨勢，資科辦、警務處及「事故協調中心」在2018年舉辦一系列宣傳活動，提升公眾對防範網騙的認知。活動包括網絡安全研討會及宣傳短片創作比賽等，向企業、學校及市民宣傳網絡安全訊息，並讓公眾掌握相關的知識及技術。

14. 為進一步協助大眾應對仿冒詐騙攻擊，資科辦於「網絡安全資訊站」設立一站式的「提防仿冒詐騙攻擊」專題網頁，內容涵蓋常見的攻擊類型、相關的風險及影響、偵測及應對策略、防避建議等。資科辦會繼續通過「網絡安全資訊站」及各類宣傳渠道，向公眾發放其他資訊保安的訊息。

15. 繼2017年推出第一輪網絡安全運動應對殭屍網絡的潛在保安威脅，警務處在2018年推出第二輪網絡安全運動，提升市民對保護流動智能裝置的認知，並向市民提供免費的手機防毒及掃描應用程式，協助他們防範包括殭屍網絡及惡意軟件等針對智能裝置的網絡攻擊。

16. 在2017/18學年，資科辦與專業團體合作探訪學校，接觸超過9 100名老師及學生，加深他們對資訊保安的認知及宣傳使用互聯網的正確態度。有見活動反應正面，我們在2018/19學年繼續安排學校探訪。截至2018年12月，我們在本學年已向超過5 900名師生傳遞資訊保安訊息。

資訊保安人力資源

17. 根據職業訓練局的《2018年創新及科技業人力調查報告》，本港從事資訊科技工作的專業人員有95 780名，估計當中約4 000多名負責資訊保安及相關職務。鑑於資訊保安的最新形勢，我們認為有需要加強有關人才培訓的工作。在職業培訓方面，政府繼續聯同業界舉辦會議、專題研討會及工作坊，包括「資訊保安高峰會」年度活動，以支援業界的資訊保安培訓工作。政府亦聯同專業團體向資訊科技人員推廣資訊保安專業認證，提升資訊科技人員的資訊保安知識及技術，並且鼓勵他們投身資訊保安專業，培養更多合資格的網絡安全專業人才。此外，政府積極鼓勵大專院校在相關學科增加更多資訊保安課程，以培訓更多具備資訊保安專業知識及技能的人才。

18. 政府在2018年6月推出「科技人才入境計劃」，透過快速處理安排，為合資格科技公司及機構輸入海外和內地科技人才（包括網絡安全人才）來港從事研發工作。此外，勞工及福利局在2018年8月公布的首份香港人才清單提出可配合香港經濟高增值及多元化發展的11項專業，亦包括資深網絡安全專家。

政府內部應對網絡安全威脅的措施

遵行審計及政策檢討

19. 為保障政府的資訊系統及數據資產，資科辦參照國際標準制訂了一套全面的《政府資訊科技保安政策及指引》（《政策及指引》），涵蓋多個範疇，包括：資訊保安的管理架構及人力資源的保安要求、資訊系統及數據資產的保護和加密要求、接達及存取控制、網絡及外判服務的保安，以及事故應變和復原等。為確保各局和部門嚴格執行《政策及指引》的規定，資科辦在2017年及2018年已為約60個局和部門完成資訊保安遵行審計，並提出改善建議。資科辦將於今年年中前完成餘下局和部門的審計工作，並隨即於下半年展開新一輪的審計工作。

20. 面對科技高速發展和新興保安威脅，資科辦將會在今年就《政策及指引》開展新一輪檢討工作。檢討工作將繼續參考

最新國際標準及業界良好作業模式，並因應資訊及網絡安全的最新形勢，在有關的範疇加強或調節保安要求。

保安警報

21. 鑑於網絡安全威脅不斷增加，資科辦在政府內部也推行網絡風險資訊共享平台，加強監察網絡安全威脅和更有效地分享相關資訊。在2018年，資科辦發出約100次關於電腦系統或軟件漏洞的保安警報，提醒各局和部門及早採取適切的防禦措施。

保安科技措施

22. 為防止網絡攻擊及入侵，政府已採用多層式保安措施以保護政府資訊系統及網絡，包括：防火牆、分散式阻斷服務攻擊防護方案、入侵偵測及防禦系統、資料加密、防電腦病毒，以及實時監測等工具。資科辦又不時提醒各局和部門須檢視政府網站運作的保安管控，例如：保持軟件更新以堵截保安漏洞、檢查系統存取記錄、定期進行安全風險評估和審計等。為應對新的資訊保安挑戰，資科辦會繼續增設更多網絡及系統檢測工具，協助局和部門進行網頁編碼檢測及滲透測試，以抵禦針對政府資訊系統及網絡的攻擊。

事故應變及保安演習

23. 為提升各局和部門對新興網絡安全威脅的認識及應變能力，資科辦自2017年起，每年聯同警務處合辦跨部門網絡安全演習，通過不同模擬網絡攻擊場景，加強部門應對網絡攻擊的應變能力。至今，所有局和部門均已參加過以上的演習。

公務員培訓

24. 資科辦在2018年舉辦多個研討會及解決方案展示會，為超過1 800名部門管理層人員及資訊保安相關員工提供適切的培訓。這些培訓活動涵蓋最新的保安及網絡安全趨勢，例如物聯網、智慧城市及仿冒詐騙等方面的保安知識。為加強香港警務人員應對網絡攻擊的能力，警務處轄下的網絡安全及科技罪案調

查科於2018年12月成立了網絡靶場（Cyber Range）。網絡靶場是一個先進的網絡安全培訓及技術設施，通過模擬各種網絡環境、攻擊及場景為學員提供實際操作體驗。

25. 鑑於仿冒詐騙是近年主要的網絡攻擊手法，資科辦將在今年安排一系列活動，包括研討會、專題網站及防範仿冒詐騙演習，以提升政府人員防禦相關攻擊的知識。

展望

26. 網絡安全威脅已成為全球最重大的安全問題之一，亦是香港必須持續關注的問題。除了繼續邀請更多不同界別的企業及機構加入「夥伴試驗計劃」，資科辦和「事故協調中心」會加強與警務處和相關機構（例如個人資料私隱專員公署及香港互聯網註冊管理有限公司）合作，進一步提高社會各界對網絡安全及保障個人私隱的認知和能力，並為本地企業提供適切的專業支援，致力為社會提供一個安全穩妥的網絡環境。

徵詢意見

27. 請委員備閱文件內容。

創新及科技局
政府資訊科技總監辦公室
2019 年 2 月

附件

保安事故及科技罪案的統計數字

事故協調中心處理的保安事故宗數

事故類別	**2017**		**2018**	
黑客入侵／網頁塗改	26	*<1%*	59	*<1%*
仿冒詐騙（釣魚網站）	1 680	*26%*	2 101	*21%*
殭屍網絡	2 084	*32%*	3 783	*37%*
分散式阻斷服務攻擊	54	*1%*	17	*<1%*
惡意軟件 （其中勒索軟件所佔宗數）	2 041 (1 388)	*31%*	3 181 (2 540)	*32%*
其他	621	*10%*	940	*9%*
總數：	**6 506**	***100%***	**10 081**	***100%***

香港警務處 - 有關科技罪案宗數及其導致的財政損失

案件性質	**2017 年**	**2018 年**
網上騙案	4 231	6 354
（i） 網上商業騙案	*1 996*	*2 717*
（ii） 電郵騙案	*693*	*894*
（iii） 網上銀行騙案	*0*	*3*
（iv） 社交媒體騙案	*1 063*	*2 064*
（v） 網上雜項騙案	*479*	*676*
網上勒索	399	504
（i） 裸聊	*305*	*281*
（ii） 其他網上勒索	*94*	*223*
盜用電腦	138	224
（i） 網上戶口盜用	*92*	*174*
（ii） 入侵系統活動	*37*	*47*
（iii） 分散式阻斷服務攻擊	*9*	*3*
其他性質	799	756
總計（宗數）：	**5 567**	**7 838**
財政損失（百萬元）：	**1,393**	**2,771**