立法會
Legislative Council

立法會 CB(4)577/17-18(04)號文件

檔號：CB4/PL/ITB

資訊科技及廣播事務委員會

2018 年 2 月 12 日舉行的會議

有關資訊保安的最新背景資料簡介

目的

本文件綜述議員過往在討論政府當局各項資訊保安計劃時提出的意見和關注。

背景

2. 政府當局各項資訊保安計劃的目標，是制訂及推行資訊保安政策及指引，以供各政策局及部門("局/部門")遵行及參考；確保政府當局的所有資訊科技基礎設施、系統及資料安全穩妥並具復原能力；以及推廣和提高機構及市民大眾對資訊保安和網絡風險的認知。

3. 政府當局開展了多項計劃，以針對加強政府資訊系統及其互聯網基礎設施的保安，並與主要的持份者合作，分享良好作業模式及指引，從而加強市民的資訊保安意識及知識。政府當局資訊保安計劃的發展，可歸納為以下 3 個主要範疇：

(a) 政府層面的資訊保安；

(b) 廣泛社會層面的資訊保安措施；及

(c) 公眾認知及教育。

政府層面的資訊保安

預防措施

注視網絡風險趨勢

4. 政府當局致力保護其資訊基礎設施及數據資產，並且在政府內部採用多層保安措施，以應對日益增加的網絡攻擊事故及相關安全威脅。政府資訊科技總監辦公室("資科辦")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，並適時向各局/部門發出保安警報及催辦便箋，以及協助政府資訊科技人員及各局/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。

5. 為加強政府監察網絡威脅和分享相關資訊的能力，資科辦採用大數據分析技術，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，俾能為各局/部門提供更針對性的網絡威脅預警訊息，亦讓業界、企業和香港電腦保安事故協調中心("香港協調中心")[1]共享網絡風險資訊。

進行風險評估及跟進工作

6. 各局/部門已推行與資訊保安相關的措施，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。資科辦為所有局/部門進行獨立的資訊保安遵行監測及審計。在評估過程中，資科辦協助有關局/部門持續改善保安管理系統，以應對新興保安威脅。

數據保護措施

7. 為確保政府的數據資產得到保護，政府當局在儲存和傳送敏感數據及文件時，以業界最高標準進行加密。資科辦已要求各局/部門加強數據保護，並構建系統以加強政府監測、偵察

[1] 香港協調中心由香港生產力促進局管理，為本地企業及互聯網使用者協調電腦保安事故的應變工作。

及堵截資料外泄的能力。各局/部門亦須監控網絡中的可疑流量，進行分析並在有需要時進行堵截。

拒絕服務攻擊

8. 資科辦協助各局/部門推行適當的保護措施及加強偵測威脅的能力，包括保安漏洞掃描及滲透測試，以防範分布式拒絕服務及網頁塗改攻擊。資科辦亦向各局/部門發出適時的警報及建議，使其採取管理及技術措施，保護政府網站及數據。

勒索軟件及惡意軟件攻擊

9. 資科辦不時向各局/部門發出嚴重保安警報及有關加強資訊保安措施的催辦便箋，以及發出針對勒索軟件的資訊保安指引，並提醒所有員工不要開啟可疑電郵及其附件和連結，防止電腦遭受感染。資科辦亦提醒各局/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。

<u>資訊科技保安政策及管治</u>

10. 政府當局已制訂一套《政府資訊科技保安政策及指引》("《指引》")，供各局/部門遵行，藉此加強相關的遵行規定要求和保安作業模式，俾能應對不同類型的新興威脅，如惡意攻擊、資料外泄、網絡入侵和仿冒詐騙攻擊。

11. 政府當局已參照最新版的 ISO 27001 國際標準及業界良好作業模式檢討《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。

12. 資科辦為各局/部門定期進行遵行審計，以確保其符合政府的資訊保安規例、政策和要求。資科辦亦就使用外置儲存裝置傳送政府文件制訂實務指引及保安要求，並協助各局/部門採用適當技術加密政府數據。

<u>培訓政府員工</u>

13. 支援人員獲安排接受培訓，以更新他們對新興威脅的知識及技術性技能，從而減低相關風險。資科辦特別協助政府資

訊科技人員及各局/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。資科辦亦為政府各級人員定期舉辦與資訊保安相關的簡報會、研討會及培訓工作坊等，以提高他們的保安意識，並加強有關網絡攻擊和最新資訊科技保安技術及解決方案的知識。這些培訓工作亦旨在提升政府員工的資訊保安技能，從而增強各局/部門預防網絡攻擊和保護政府資訊系統及敏感資料的能力。

政府內部及與業界的合作

14. 資科辦透過政府電腦保安事故協調中心("政府協調中心")[2]與香港警務處("警務處")合作，為各局/部門和互聯網基礎設施持份者舉辦網絡保安演習。

廣泛社會層面的資訊保安措施

監察大型活動的網絡保安

15. 在保護互聯網基礎設施方面，資科辦按需要啟動互聯網基建聯絡小組[3]的保安警報機制，以加強監察大型活動的網絡保安和提供支援，防範本地的互聯網基礎設施受到聲稱發動的網絡攻擊所影響。

---

[2] 政府協調中心於 2015 年 4 月在資科辦轄下成立，以處理協調資訊及網絡安全事故的工作。政府協調中心是為政府資訊科技管理人員及用戶而設的協調中心，負責有關電腦緊急應變和事故處理的工作。政府協調中心與香港協調中心緊密合作，處理影響私營機構及市民的資訊保安威脅及事故。在國際方面，政府協調中心會與其他政府和地區的電腦緊急事故應變小組及國際組織合作，促進資訊及知識交流，以減少保安漏洞，減低風險，並處理威脅及攻擊。

[3] 資科辦在 2005 年成立互聯網基建聯絡小組，與互聯網基礎設施持份者緊密聯繫，並致力確保互聯網基礎設施能夠穩健運作。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、政府協調中心、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。

本地合作

16. 資科辦資助香港協調中心，為本地企業及市民協調電腦保安事故應變工作、監測和發布保安警報，以及推廣對資訊保安的認知。

國際聯繫

17. 政府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，與負責其他地區電腦保安事故的緊急應變小組保持緊密聯繫，藉以適時分享保安威脅、漏洞和保安事故的資訊。政府亦積極參與各組織所舉辦的技術交流活動，包括亞太區電腦保安事故協調演習。政府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。

支援中小型企業

18. 資科辦與香港協調中心及相關機構合作，為中小型企業("中小企業")舉辦研討會，提高中小企業對網絡威脅的認知，以及分享資訊保安風險管理方面的良好作業模式。政府當局已推出的措施包括：

(a) 與香港協調中心合作，向中小企業推廣"檢查——行動——驗證"的方法，協助中小企業識別潛在的網絡威脅，並採取改善措施和驗證相關措施的成效，以提高中小企業的整體網絡保安水平；

(b) 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"，向中小企業推廣對資訊保安及網絡威脅的認知，協助他們建立更安全的電子商務環境；

(c) 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，以及保護其資訊系統和數據資產；及

(d) 透過資科辦與工業貿易署中小企業支援與諮詢中心的合作，於 2016 年 9 月舉辦"中小企雲端保安論壇"，讓中小企業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。

19. 政府協調中心一直與香港協調中心和其他地方的電腦保安事故應變小組緊密合作，分享有關網絡保安威脅的資訊和協調事故應變工作，協助向市民發出保安預警。除分享網絡保安資訊外，政府協調中心亦與電腦保安事故應變小組社群合辦活動，包括知識及技能分享活動、培訓及工作坊，以及地區和全球性的跨境事故應變演習。

向公眾提供支援以應對惡意軟件

20. 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。當局已透過網絡安全資訊站(www.cybersecurity.hk)、報章和電子傳媒，向中小企業及公眾發放有關勒索軟件攻擊的資料。

公眾認知及教育

21. 政府當局定期安排活動及保安認知培訓，使市民認識最新的良好作業模式以保護其電腦裝置及資訊資產，以免蒙受網絡保安風險。資科辦會聯同警務處、香港協調中心及其他機構舉辦全年活動，以提高市民對資訊保安的認知。這些活動包括：

(a) 舉辦研討會，以及透過政府網站和其他媒體及宣傳渠道，向市民發布最新的保安警報及資訊；

(b) 與資訊保安專業團體合作進行學校探訪，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；

(c) 舉辦"2016 香港——內地網絡安全論壇"，由香港及內地網絡安全專家就金融技術、雲端運算、大數據

等方面的網絡安全挑戰及當中的技術解決方案作出詳盡分析；

(d) 在2016年9月舉辦"網絡安全精英嘉許計劃"。這項活動由資科辦、警務處及香港協調中心合辦，旨在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；

(e) 定期舉辦不同的網絡安全推廣活動，包括"共建安全網絡"年度活動，以提升公眾對網絡保安和網絡攻擊趨勢的認識，並鼓勵參加者加強對個人和敏感數據的保護；及

(f) 豐富網絡安全資訊站(資科辦的專題網站)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。

過往的討論

資訊科技及廣播事務委員會

22. 在2016年12月12日的資訊科技及廣播事務委員會("事務委員會")會議上，政府當局向委員簡介政府各項資訊保安計劃的進展及發展。

公眾教育及認知

23. 部分委員關注到市民對網絡保安風險缺乏認知，並詢問政府當局將如何處理這個問題。政府當局表示，當局已透過網絡安全資訊站(www.cybersecurity.hk)、報章和電子傳媒，向中小企業及公眾發放有關勒索軟件攻擊等最新的網絡安全威脅訊息，以及相關保安貼士。當局製作了一套題為"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，避免受勒索軟件攻擊。

針對惡意軟件及仿冒詐騙網站的措施

24. 委員詢問，政府當局有何措施提高公眾對仿冒詐騙網站及惡意軟件的資訊保安意識，以及已採取哪些風險緩解措施或將會推出哪些機制。政府當局表示，資科辦與香港協調中心及業界緊密合作，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，與社會分享有關保安威脅及漏洞的資訊。

25. 資科辦透過網絡安全資訊站，為公眾提供實用提示和建議有用的工具，以保護他們的電腦設備及網站。創新科技署推出的"科技券計劃"，讓中小企業能採用科技服務及方案，包括加強網絡保安的資訊科技。

26. 此外，資科辦與香港互聯網註冊管理有限公司(".hk"域名的管理機構)合作，推廣使用域名系統安全擴展，以改善".hk"網頁的可靠程度，並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，以及保護其資訊系統和數據資產。

27. 至於針對仿冒詐騙網站的風險緩解措施，政府當局告知事務委員會，警務處的網絡安全及科技罪案調查科已有既定程序及機制打擊網絡罪案，包括應付本地及外國的仿冒詐騙網站。

人力資源及培訓

28. 部分委員關注到資訊及通訊科技人手短缺，並詢問政府當局會採取哪些措施加強培訓，以擴充資訊及通訊科技人手。事務委員會委員建議，政府當局應在適當階段進行相關的資訊及通訊科技業人力調查，讓政府更加了解業界的人力需求。

29. 政府當局告知事務委員會，資科辦一直與本地大學及專上院校保持溝通，俾能為學生和資訊及通訊科技人員提供相關教育課程，以及與資訊及通訊科技業界商討提供更多實習名額，鼓勵學生及畢業生投身業界。

30. 就資訊保安專業人員的認證，資科辦會與資訊保安專業團體協調，以期提供更多專業課程及認可，藉此拓展資訊及通

訊科技人手。資科辦亦已為政府人員提供專業培訓及認可，以核證其資訊保安知識。

針對網絡攻擊的措施

31. 部分委員詢問，政府當局在政府內部採取哪些措施應對受到的網絡攻擊。政府當局解釋，資科辦定期進行惡意軟件掃描，並會繼續研究最新的技術，例如大數據分析，以改善網絡監察及識別惡意軟件攻擊的工作，俾能作出緊急應變及加強防範措施。資科辦亦提醒所有局/部門必須遵從政府的資訊保安政策及指引，以及採取適當防禦措施處理電郵及保護政府的系統和數據資產。

立法會會議

32. 莫乃光議員、廖長江議員、鄭松泰議員及葛珮帆議員等議員曾在立法會會議上就有關資訊保安的事宜提出書面質詢。議員的質詢載於**附錄**。

財務委員會

33. 在2017年4月3日的財務委員會特別會議上，莫乃光議員詢問當局在2017-2018年度推動網絡及資訊保安的措施。葛珮帆議員亦詢問現時政府當局有何政策、措施、工作單位及設備以維護政府及社會的資訊系統安全。涂謹申議員詢問政府為加強執行資訊科技保安守則、政策及指引而推行的措施。政府當局的答覆載於**附錄**。

最新情況

34. 政府當局將於2018年2月12日向事務委員會簡介政府各項資訊保安計劃的進展及發展。

相關文件

35. 相關文件一覽表載於**附錄**。

立法會秘書處
議會事務部 4
2018 年 2 月 6 日

附錄

相關文件一覽表

文件來源	會議日期/ 發出日期	文件
立法會會議	2016 年 12 月 7 日	廖長江議員提出的第 8 項質詢 網絡安全
	2016 年 12 月 14 日	莫乃光議員提出的第 19 項質詢 香港的資訊保安
	2017 年 1 月 11 日	鄭松泰議員提出的第 8 項質詢 網絡安全資訊共享平台及網絡風險資訊共享平台
	2017 年 5 月 31 日	莫乃光議員提出的第 9 項質詢 政府部門、公營機構及工務工程相關機構的資訊保安情況
	2017 年 6 月 7 日	葛珮帆議員提出的第 22 項質詢 香港的機構應付大型電腦保安事故的能力
	2017 年 11 月 29 日	莫乃光議員提出的第 15 項質詢 提升資訊保安的措施
資訊科技及廣播事務委員會	2016 年 12 月 12 日	政府當局就資訊保安的最新情況提供的文件 立法會 CB(4)246/16-17(04)號文件 有關資訊保安的最新背景資料簡介 立法會 CB(4)246/16-17(05)號文件 會議紀要 立法會 CB(4)515/16-17 號文件
財務委員會特別會議	2017 年 4 月 3 日	政府當局就議員初步問題的書面答覆(答覆編號 ITB175、ITB203 及 ITB207) http://www.legco.gov.hk/yr16-17/chinese/fc/fc/w_q/itb-c.pdf