立法會
Legislative Council

立法會CB(2)1189/2024(03)號文件

檔號：CB/PL/ITB

資訊科技及廣播事務委員會

2024年10月14日的會議

關於維護及推廣資訊保安的背景資料簡介

目的

本文件旨在就政府當局維護及推廣各項資訊保安的措施提供背景資料，並概述議員近年在資訊科技及廣播事務委員會("事務委員會")和發展智慧城市事宜小組委員會的會議上就相關議題表達的意見和關注。

背景

2. 政府當局各項資訊保安計劃的目標如下：

(a) 制訂和推行資訊保安政策及指引，以供各政策局及部門("局/部門")遵行和參考；
(b) 確保政府當局的所有資訊科技基礎設施、系統和資料安全穩妥並具復原能力；及
(c) 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. 政府當局針對以下3個主要範疇開展了多項計劃：

(a) 政府層面的資訊保安；
(b) 社會層面的資訊保安措施；及
(c) 專業培訓和公眾認知。

政府層面的資訊保安

加強政府及公營機構的資訊及網絡安全

4. 政府當局在2023年12月發布**《香港促進數據流通及保障數據安全的政策宣言》**，闡明政府在數據流通及數據安全兩方面的管理理念和策略，包括會就政府的資訊科技系統保安及數據安全提供使用及安全規範，以及**研究修訂《個人資料(私隱)條例》(第486章)及完善《版權條例》(第528章)**，以適時加強對個人資料和人工智能技術發展所提供的保障。

5. 為確保政府資訊科技系統的推行和運作暢順，政府資訊科技總監辦公室("資科辦")[1]於2024年2月推出一系列新措施，包括要求局/部門**推出大型及高風險資訊科技項目前安排額外的獨立網絡安全測試**，以便及早發現和修補相關系統漏洞，並評估系統在應對網絡攻擊時的偵測及復原能力。政府當局亦會在2024年下半年牽頭**舉辦網絡安全攻防演練**，並透過加入具備實力和經驗的內地攻防演練機構，測試和加強政府部門及公營機構的資訊系統安全。

6. 此外，資科辦已制訂並不時更新《政府資訊科技保安政策及指引》("《政策及指引》")，涵蓋資訊保安管理架構、政策及措施，供各局/部門遵守及使用，亦供業界(包括公私營機構)參閱。資科辦於2024年4月修訂《政策及指引》，加強不同領域的資訊保安控制措施，包括資訊保安事故通報機制，同時亦**提升對政府資訊系統安全的等級保護**，要求政府部門必須採用以風險為本評估系統安全的等級，並根據分級實施相關等級的保安控制措施，以期更有效保障政府的資訊系統及數據安全。

資訊保安遵行審計

7. 資科辦定期為各局/部門展開獨立資訊保安遵行審計，以確保局/部門嚴格執行政府的保安規定。資科辦已完成2022-2023年度的遵行審計，並提供建議協助局/部門持續優化其保安管理系統。政府當局計劃在2024年下半年展開新一輪資訊保安遵行審計。

---

[1] 資科辦及效率促進辦公室已於2024年7月合併為數字政策辦公室("數字辦")。數字辦專責制訂數字政府、數據治理及資訊科技政策。

關鍵基礎設施的電腦系統安全

8. 關鍵基礎設施是指一些維持香港社會正常運作和維持市民正常生活所必需的設施，例如銀行、金融機構、通訊網絡、供電設施、鐵路系統等。一旦其電腦系統受干擾或破壞，會嚴重影響社會正常運作。政府當局在2024年7月公布有關**加強保護關鍵基礎設施電腦系統安全**的建議立法框架。擬議立法框架旨在訂明關鍵基礎設施營運者須承擔的法定責任，令該等營運者採取適當措施，加強有關電腦系統的保安能力和減低必要服務因網絡攻擊被擾亂或破壞的可能，提升本港整體的電腦系統安全。政府當局預期於2024年年底前將相關條例草案提交予立法會審議。

社會層面的資訊保安措施

監測、預防和應對網絡威脅及攻擊

9. 香港網絡安全事故協調中心("事故協調中心")[2]為本地企業及市民協調資訊保安事故應變工作、監測和發布保安警報，以及推廣對資訊保安的認知。事故協調中心亦會與互聯網服務供應商合作，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。

10. 政府電腦保安事故協調中心("政府協調中心")[3]透過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緊急事故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。為加強交流合作及通報資訊

---

2 香港網絡安全事故協調中心(前稱香港電腦保安事故協調中心)由政府在 2001 年成立，現由香港生產力促進局管理，為本地企業及互聯網用户提供資訊保安事故的消息和防禦指引、事故回應及支援服務，以及提高公眾的資訊保安意識。

3 政府協調中心於 2015 年 4 月在資科辦轄下成立，專責為政府協調處理資訊及網絡安全事故。政府協調中心協助政府資訊科技管理人員及各部門的資訊保安事故應變小組，應對有關電腦緊急應變及事故處理的工作。政府協調中心與事故協調中心緊密合作，分享有關保安威脅及漏洞的資訊，並向公私營機構及市民提供建議，以保護他們的資訊系統及數碼資產。

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，包括亞太區電腦保安事故協調組織舉辦的年度聯合事故應變演習。

提升本港企業(尤其是中小型企業)應對網絡攻擊的能力

11. 為協助中小型企業("中小企")以有限的資源應對潛在的資訊保安風險，香港互聯網註冊管理有限公司("互聯網註冊公司")早於2019年開始向中小企網站提供免費檢驗服務，服務包括檢查網站是否存在安全漏洞、提供掃描報告及建議。事故協調中心亦於2021年9月推出"評估你的網絡保安狀況"線上自我評估工具，讓中小企更了解其網絡安全狀況，並提供建議幫助中小企提升整體資訊保安能力。同時，資科辦亦聯同互聯網註冊公司，透過"網絡安全資訊共享夥伴計劃"促進公營及私營機構之間交流網絡安全資訊。此外，政府當局透過科技券計劃等措施，為企業提供財政資助，協助他們提升維護資訊保安的能力。

公眾對網絡安全的認知

12. 政府透過不同渠道(包括電台、社交媒體、網站等)向公眾提供資訊保安建議，例如警務處透過全方位發放防騙訊息，包括舉辦"防騙月"、推出"防騙一站通"網站。此外，資科辦繼續聯同警務處及事故協調中心舉辦年度"共建安全網絡"資訊保安推廣活動，加強機構及公眾對網絡安全與國家安全的認識，並提醒他們須採取穩妥的網上行為，共同維護網絡安全。

13. 為進一步打擊電話及短訊詐騙，通訊事務管理局辦公室已於2023年12月底推出"**短訊發送人登記制**"("登記制")，並**率先於電訊業實施**，以協助市民識別短訊發送人的身份。根據登記制，所有已登記參與的公司或機構，會使用以"＃"號開頭的"已登記的短訊發送人名稱"發出短訊予本地流動服務用户。

<u>資訊保安人力資源發展</u>

14. 政府當局繼續透過推行"科技人才入境計劃"[4]，簡化

[4] 政府當局在2018年推出"科技人才入境計劃"，就輸入海外和內地

申請科技(包括網絡安全)人才入境從事研發工作的手續，從而加快吸納世界各地的網絡安全科技人才。當局於2022年12月推出優化措施，包括撤銷聘用本地僱員的要求、延長配額有效期至兩年，以及擴展至更多新興科技範疇。

議員提出的主要意見和關注

15. 議員提出的主要意見和關注綜述於下文各段。

政府當局的資訊保安政策

16. 議員察悉，自數碼港於2023年8月發生網絡安全事故後，資科辦已提醒各個**政府部門**須檢視其資訊保安系統，並**提升網絡安全防禦能力**。議員查詢有關工作的**進展**，並詢問資科辦會否成立網絡安全應變小組以應付突發情況和檢視《政策及指引》並作更新，及要求其他的公營機構遵行，以協助機構制訂相關措施。

17. 政府當局表示會積極跟進政府和公營界別等機構的網絡安全的事故。由於大部分政府系統集中在政府私有雲端平台上管理，通過中央互聯網通訊閘接達互聯網，因此保安安排也可較集中處理。當局採用多層網絡安全保安技術、防火牆、入侵偵測和應變系統等，監測系統流量、加以分析和作出警報。資科辦亦要求每個部門成立電腦保安事故應變小組，在發生事故時即時向資科辦通報。當局會加強攻防演練以檢視部門系統的漏洞，並和警方的網絡安全及科技罪案調查科保持緊密合作，定期評估網絡安全情況。當局日後將加強與業界的合作，以期維護香港的整體網絡安全。

18. 至於有關資訊科技保安的《政策及指引》，政府當局表示會定期作出更新，並已上載至網站供所有公私營機構參考。個別機構可因應情況，採用《政策及指引》所建議的管理保安風險原則和措施。議員促請政府當局**將不同的資訊保安指引整合**，以期向機構**提供更完備的指引**。為提高各局/部門對網絡安全風險的警覺性，資科辦定期提示各局/部門採取適切的保安措施，以保護政府資訊系統及數據。

科技人才實施快速處理安排，成功申請的公司會獲發配額以輸入相關人才從事研發工作。

應對網絡安全威脅的策略

19. 因應全球網絡攻擊事故越趨嚴重，議員認為政府當局應**制訂全面的資訊保安策略**，全方位應對網絡安全威脅。議員亦建議當局把內地開發的鴻蒙操作系統應用於政府電腦系統，以**減低對外國科技的依賴**。

20. 政府當局表示會與全球主要電腦保安事故應變組織及電腦緊急事故應變小組分享最新的網絡安全信息。透過"網絡安全資訊共享夥伴計劃"，資科辦與事故協調中心和互聯網註冊公司合作，提升本港企業，尤其是中小型應對各種網絡攻擊的能力，包括向以".hk"域名註冊的中小企網站提供免費檢驗服務、發布《資訊保安事故指南》、為中小企僱員編製培訓教材等。就政府資訊系統的安全保障方面，政府當局會提醒各局/部門從不同來源採購資訊及通訊科技產品，以減低保安風險和對單一產品或品牌的倚賴性。

關鍵基礎設施的電腦系統安全

21. 議員察悉，政府當局公布有關加強保護關鍵基礎設施的電腦系統安全的擬議立法框架，旨在訂明**關鍵基礎設施的營運者(不擬包括政府部門)**須承擔的法定責任，包括建立良好的防範管理體系，以確保其資訊系統和網絡安全運作。議員詢問，若政府部門不擬納入擬議條例，當局**有何措施確保政府部門的網絡安全**。

22. 政府當局表示，就政府提供的必要服務(例如供水、渠務、緊急救援等)，政府部門須循從全面和嚴謹的《政策及指引》，並且參照最新國際標準及業界良好作業模式定期檢討和更新，以確保政府資訊系統安全。由於《政策及指引》要求的水平與擬議條例對"關鍵基礎設施營運者"的法定要求相若，政府當局建議繼續沿用現有的行政方法規管政府部門，無需把政府納入擬議條例的規管範圍內。

協助中小企應對網絡安全風險

23. 議員詢問政府當局有何措施**協助中小企應對網絡安全風險**，並建議當局**與具規模的機構或商會合作**，為業界

提供協助。政府當局告知，政府會加強與業界的協作，從不同層面支援業界應對網絡安全風險，包括為中小企提供免費網絡安全檢測、設立員工培訓平台，以及與業界研究制訂《數據中心保安實務指引》，提高業界與公眾的網絡安全保護意識和能力。當局亦會與互聯網註冊公司合作推動網絡安全的宣傳教育及培訓工作，並提供"網健通"服務及資訊保安事故應變支援。

網上行騙情況

24. 議員對網上騙案數目顯著上升及所涉的損失金額表示關注。他們要求政府當局加強公眾教育和宣傳，**提高市民對網上欺詐及網絡安全的警覺性**。政府當局表示，警務處於2017年成立反詐騙協調中心，以加大力度打擊騙案，並推出"防騙一站通"網站，加強市民對行騙活動的認知。警務處亦會密切監察在網上可能發生的犯罪活動，針對性地在互聯網公眾平台搜尋可能與罪案有關的資料。

資訊保安人才

25. 議員關注到本港缺乏具備資訊保安專門知識的人才。議員建議由政府當局培訓相關人員，以期為各部門及公營機構進行資訊保安工程，加強有關方面的保護。政府當局表示，當局需持續加強有關資訊保安的專家的培訓，並會吸引海內外的網絡安全專家及機構來港支援相關工作。

26. 議員詢問，政府當局將如何**培養更多資訊保安人才**。政府當局表示會透過定期舉辦分享會或技術交流活動，例如邀請內地優秀的網安公司來港進行分享，加強與業界的交流，讓本港企業衍生更多網絡安全方面的需求，以期吸引內地企業和人才落戶香港，壯大香港的網絡安全人才庫。除了吸引世界各地的網絡安全科技人才外，當局亦鼓勵本地大專院校及科技培訓機構為資訊科技從業員提供專業培訓課程，讓他們吸收資訊保安方面的專業知識和技能。

立法會議案及質詢

27. 在2023年11月29日的立法會會議上，議員通過一項有關"全面打擊網絡詐騙罪行"的議案，促請政府優化現有打擊

網絡騙案的措施，包括全面審視本港的網絡安全風險、加強網絡系統的保護措施，以及協助中小企提升網絡安全水平等。議案措辭的超連結載於**附錄**。

28. 議員曾在立法會會議上就網絡安全、打擊網絡詐騙及保障個人資料私隱等事宜提出質詢。相關超連結載於**附錄**。

最新發展

29. 政府當局將於2024年10月14日向事務委員會匯報本港資訊保安的最新情況和政府在維護及推廣資訊保安方面的工作。

相關文件

30. 相關文件一覽表載於**附錄**。

立法會秘書處
議會事務部
2024年10月9日

附錄

有關維護及推廣資訊保安的工作

相關文件一覽表

委員會	會議日期	文件
資訊科技及廣播事務委員會	2022年4月19日	議程第IV項：資訊保安的最新情況 會議紀要
	2023年12月12日	議程第III項：促進數據流通及保障數據安全 會議紀要
	2024年4月8日	議程第V項：數碼港網絡安全事故 會議紀要
發展智慧城市事宜小組委員會	2024年7月12日	議程第I項：智慧城市發展的最新情況 會議紀要
財務委員會審核2024-2025年度開支預算特別會議	2024年4月19日	政府當局對議員就2024-2025年度開支預算提出的初步問題的書面答覆 (答覆編號：ITIB019、159、205、229、237、242及251) 逐字紀錄本

立法會會議	文件
2022年5月25日	第1項質詢：加強資訊保安
2022年10月26日	第2項質詢：打擊網上及電話騙案

立法會會議	文件
2023年5月10日	第10項質詢：開發或使用人工智能時保護個人資料
2023年7月5日	第6項質詢：築牢數字安全屏障
2023年7月5日	第13項質詢：社交媒體平台的詐騙案件
2023年10月18日	第17項質詢：提升網絡安全
2023年11月15日	第9項質詢：數據管治體系
2023年11月15日	第14項質詢：打擊網上及電話騙案
2023年11月22日	第11項質詢：政府部門和其他公營機構的網絡安全
2023年11月29日	議員議案：全面打擊網絡詐騙罪行 進度報告
2024年1月17日	第3項質詢：確保政府電子系統正常運作
2024年5月29日	第6項質詢：保障個人資料私隱
2024年5月29日	第18項質詢：政府部門和其他公營機構的網絡安全