立法會
Legislative Council

立法會 CB(4)246/16-17(05)號文件

檔號：CB4/PL/ITB

資訊科技及廣播事務委員會

2016 年 12 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各項資訊保安計劃時提出的意見和關注。

背景

2. 政府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；確保政府的所有資訊科技基建設施、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

4. 政府致力保護其資訊基礎設施及數據資產。各局/部門所推行與資訊保安相關的項目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。在資訊科技保安政策及管治方面，政府已制訂一套《政府資訊科技保安政策及指引》，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。政府資訊科技總監辦公室("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。

5. 鑒於分布式拒絕服務攻擊及網頁塗改所帶來的高風險，資科辦採取積極措施，協助各局/部門推行適當的保護措施，並加強偵測威脅的能力，包括保安漏洞掃描及滲透測試。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。資科辦亦對即將發生的網絡攻擊時刻保持警惕，並向各局/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。資科辦計劃與業界合作，在 2017 年建立一個網絡威脅資訊共享平台，積極收集和分析網絡威脅的資訊及數據，並為各局/部門和市民發布預警。

6. 隨着政府電腦保安事故協調中心("政府協調中心")在 2015 年 4 月成立，資科辦會繼續與香港警務處("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。在政府內部，當局一直鼓勵員工參加與資訊保安相關的簡報會、研討會、工作坊及專業培訓。這些培訓課程旨在提高他們的保安意識，並增進他們對最新資訊科技保安技術及解決方案的知識，藉以保護政府的資訊系統和敏感資料。

廣泛社會層面的資訊保安措施

7. 為保護互聯網基礎設施，資科辦自 2015 年 7 月起啟動了 3 次互聯網基建聯絡小組的保安警報機制[1]，加強監察大型活動的網絡保

[1] 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、香港電腦保安事故協調中心、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。

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。政府告知資訊科技及廣播事務委員會("事務委員會")，政府會繼續積極聯繫各持份者，促進在威脅認知及情報共享方面更緊密的合作，以維持本地互聯網基礎設施的穩定性、安全性、可用性及復原能力。

8. 資科辦在 2016-2017 年度向香港電腦保安事故協調中心[2] ("香港協調中心")提供約 1,000 萬元資助，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。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。資科辦亦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。

9. 香港協調中心推出"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。政府協調中心則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。

公眾認知及教育

10. 由於市民使用不同的科技，如流動裝置、雲端服務及社交網絡應用程式時，均會接觸到網絡保安風險，因此政府定期安排保安認知培訓，與市民分享有關的知識及最新的良好作業模式，使他們能採取適當措施保護電腦裝置及資訊資產。資科辦告知事務委員會，該辦公室會繼續聯同警務處、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，包括舉辦研討會，提醒公眾網絡威脅無處不在，促使他們採取適當的風險緩解措施；以及透過政

[2] 香港電腦保安事故協調中心("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。

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。

11. 在推廣及教育方面，資科辦播出有關"流動裝置保安"及"流動應用程式保安"的電台廣播訊息，並在各研討會加入這些主題。警務處、香港金融管理局及香港應用科技研究院在2016年5月合辦為期3天的"2016網絡安全峰會"，分享有關用以保護重要資訊基礎設施的資訊系統的策略及技術。自2008年起，資科辦聯同教育局及專業機構進行學校探訪，以提高學生、教師和家長的資訊保安認知，並提供保護電腦設備及個人資料的建議。

12. 在專業培訓及證書方面，資科辦告知事務委員會，該辦公室除了為政府的員工提供資助，以助其獲得資訊保安的專業資格外，亦會與業界合作，鼓勵資訊科技從業員獲取專業證書。

過往的討論

資訊科技及廣播事務委員會

13. 在2016年3月14日事務委員會會議席上，政府當局向委員簡介自2015年7月以來，政府各項資訊保安計劃的進展及發展情況。委員關注的主要事項包括資訊保安形勢、推行資訊科技保安政策及管治、保護互聯網基礎設施、與電腦保安事故應變小組社群的合作、提升公眾認知和教育，以及為中小企業提供資訊保安方面的支援。

資訊保安形勢

14. 部分委員關注科技罪案的統計數字及科技罪案造成的財務損失。應事務委員會的要求，政府當局提供進一步資料，按有關罪案所引致財務損失的性質，提供了2015年科技罪案的分項數字及這些罪案的偵破率，以及按事件的性質、受害者及財務損失，提供了香港協調中心在2015年處理的保安事故報告的分項數字。政府當局的書面回應於2016年5月9日隨立法會CB(4)958/15-16(01)號文件發出，並載於**附錄I**。

推行資訊科技保安政策及管治

15. 部分委員察悉，政府當局已檢討現行法例及相關行政措施，以應付電腦罪案，他們關注到，創新及科技局會否接手保安局的工作，領導另一次就資訊保安事宜進行的檢討。政府當局表示，當局定期檢討資訊保安政策，並會於 2016 年年中向各局/部門發出有關處理政府資料的《政府資訊科技保安政策及指引》。政府當局亦告知事務委員會委員，創新及科技局會繼續與保安局聯手制訂資訊保安政策。

保護互聯網基礎設施

16. 部分委員關注到政府的物聯網設施是否安全可靠。政府當局表示，各局/部門會進行定期檢討，確保其資訊科技系統符合政府的保安要求。委員亦獲悉，政府當局於 2014-2015 年度委聘獲國際認可的保安專家對政府的互聯網應用系統進行保安漏洞掃描及滲透測試，結果確定政府的互聯網應用系統具備抵禦網絡攻擊的能力。

17. 至於政府當局每隔 4 年為各局/部門進行遵行審計，部分委員關注到，當局會否更頻密地進行這項工作，以確保各局/部門已按照政府的資訊科技保安規則和要求進行內部系統審計。政府當局表示，遵行審計的工作涉及大量資源，因此每 4 年進行一次是恰當的做法。政府當局補充，如情況證實有此需要，可考慮為個別局/部門進行較頻密的遵行審計。

與電腦保安事故應變小組社群的合作

18. 部分委員詢問政府當局與其他司法管轄區的資訊科技保安當局為應付針對政府資訊科技基礎設施的網絡攻擊而展開的合作。政府當局表示，政府協調中心一直與亞太區、澳門和內地的類似機構緊密合作，分享有關網絡保安威脅的資訊和協調事故應變工作。除分享網絡保安資訊外，政府協調中心亦與其他電腦保安事故應變小組合辦活動，進行知識及技能分享、培訓，以及地區和全球性的跨境事故應變演習。

提升公眾認知和教育及為中小型企業提供資訊保安方面的支援

19. 部分委員關注到，有必要讓年輕一代意識到使用互聯網社交媒體時無意中觸犯法律的風險。委員亦詢問政府當局為確保中小企

業在日常運作中的資訊安全而為這些企業提供的支援。政府當局表示，當局已進行學校探訪，目的是提高學生、教師和家長對資訊保安的認知，並講解保護電腦設備及個人資料的重要性。政府當局會安排為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。

財務委員會

20. 在2016年4月7日的財務委員會特別會議上，莫乃光議員詢問2015-2016年度政府網絡及網站遭受網絡攻擊次數、2015-2016年度政府各局/部門用於保安風險評估及審計的開支，以及2015-2016年度政府各局/部門開發的網站、應用系統和流動應用程式有否進行資訊保安風險評估和檢查等事宜。單仲偕議員亦詢問為政府網站和網上應用系統進行保安檢查的開支及詳情。政府當局的答覆載於**附錄II**。

最新情況

21. 政府當局將於2016年12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情況。

相關文件

22. 相關文件一覽表連同其超連結載於：

http://www.legco.gov.hk/yr15-16/chinese/panels/itb/papers/itb20160314cb4-689-3-c.pdf
http://www.legco.gov.hk/yr15-16/chinese/panels/itb/papers/itb20160314cb4-689-4-c.pdf
http://www.legco.gov.hk/yr15-16/chinese/panels/itb/minutes/itb20160314.pdf
http://www.legco.gov.hk/yr15-16/chinese/panels/itb/papers/itb20160314cb4-958-1-c.pdf
http://www.legco.gov.hk/yr15-16/chinese/fc/fc/w_q/itb-c.pdf

立法會秘書處
議會事務部4
2016年12月7日

附錄 I

資訊科技及廣播事務委員會
在2016年3月14日會議上要求提供的資料

(a) 在2015年，有關科技罪案導致的財務損失金額分項數字如下：

2015年科技有關的罪案	**罪案宗數**	**財務損失金額（百萬元）**
網上遊戲	416	2.4
網上商業騙案	1 911	40.4
非法進入電腦系統	1 223	1 462.4
社交媒體騙案	1 422	60.0
分散式阻斷服務攻擊	35	0.1
其他	1 855	263.6
總數	**6 862**	**1 828.9**

在6 862宗科技罪案當中，904宗已偵破，破案率為13.2%。

(b) 在2015年，香港電腦保安事故協調中心處理的保安事故分項數字如下：

2015年電腦保安事故	**保安事故數字**	**佔百分比**
黑客入侵/網頁塗改	151	3%
仿冒詐騙	1 978	40%
殭屍網絡	1 943	39%
分散式阻斷服務攻擊	130	3%
惡意軟件	277	6%
其他	449	9%
總數	**4 928**	**100%**

受害者類別	保安事故數字
家庭及個人	2 083
大型企業及機構	146
中小型企業	374
教育界	109
其他本地及海外網絡用戶	99
未能分類（未能直接聯絡網絡用戶）	2 117
總數	**4 928**

香港電腦保安事故協調中心主要向事主在事故應變和復原上提供意見，在過程中，事主無需向協調中心提供財務損失的相關數字。

附錄 II

審核 2016-17 度
開支預算

答覆編號
ITB198

管制人員的答覆

(問題編號：1946)

總目： (47) 政府總部：政府資訊科技總監辦公室

分目：

綱領： (1) 政府內部資訊科技的使用

管制人員： 政府資訊科技總監(楊德斌)

局長： 創新及科技局局長

問題：

就推動網絡及資訊保安的措施方面，請告知：

(一) 2015-16 年度政府網絡及網站遭受網絡攻擊次數(被塗改網頁、入侵網絡及資訊系統或分布式拒絕服務攻擊)，請以表按照部門名稱及保安事故類別列出；

(二) 2015-16 年度政府各政策局和部門用於保安風險評估及審計的開支，及佔每年資訊科技開支的比率；

(三) 2015-16 年度政府各政策局和部門開發的網站、應用系統和流動應用程式有否進行資訊保安風險評估和檢查的詳情及開支為何；

(四) 就政府資訊科技保安政策的研究和檢討工作的開支預算和 2016-17 年度工作所涉及的人手及開支為何？

(五) 請以表列出過去三年已進行、目前進行中及 2016-17 年度計劃進行的政府部門資訊保安遵行監測及審計的政策局及部門；及

(六) 請以表列出過去三年已進行、目前進行中及 2016-17 年度計劃進行的保安認知研討會及培訓項目的日期、內容、培訓部門、出席對象及出席人數。

提問人：莫乃光議員(議員問題編號：9)

答覆：

所需資料提供如下：

(一) 在 2015-16 年度，政府資訊保安事故協調中心下的應變辦事處共接獲 4 宗涉及政府網站遭受網絡攻擊的事故報告，包括 2 宗網站遭到塗改及 2 宗分布式拒絕服務攻擊，涉及 4 個不同部門。該 4 宗保安事故並不涉及資料外泄。

(二) 各局和部門在推出新的資訊系統或就現有資訊系統作大規模升級前會進行保安風險評估，並須定期對資訊系統進行審計，確保已遵行資訊科技保安政策和採取有效的保安措施。這些工作一般已納入有關資訊系統的開發和維修保養開支內，因此我們沒有相關的分項開支資料。

此外，各局和部門會定期(約兩年)進行部門的整體資訊保安風險評估及審計工作。在 2015-16 年度，政府用於保安風險評估及審計的總開支預算約為 1,210 萬元，佔該年度資訊科技全年總開支預算的比率約為 0.26%。

(三) 各局和部門為開發的網站、應用系統和流動應用程式進行資訊保安風險評估屬強制規定，一般已納入有關資訊系統的開發和維修保養規定內。由於資訊保安的開支通常會計入其他涉及資訊科技的開支內，因此我們沒有這方面的分項開支數字。

(四) 我們已委聘顧問公司，進行政府資訊科技保安政策的研究和檢討工作，開支總預算為 300 萬元。

(五) 在過去 3 個年度已進行、進行中和在 2016-17 年度計劃進行資訊保安遵行審計的局和部門數目，表列如下：

資訊保安遵行審計	2013-14 年度 (局和部門數目)	2014-15 年度 (局和部門數目)	2015-16 年度 (局和部門數目)	2016-17 年度 (局和部門數目)
已完成	8	8	25	-
在進行中	-	-	2	-
計劃進行	-	-	-	18

(六) 在過去 3 個年度內，有關研討會及培訓項目的數目表列如下：

	2013-14 年度	2014-15 年度	2015-16 年度
研討會及培訓場數	48	65	53
出席人數	1 342	2 213	1 617

研討會及培訓項目內容包括安排給各部門員工的資訊保安認知培訓、部門資訊科技保安主任及事故應變小組組長的資訊保安複修課程，以及資訊科技保安管理及專業人員的專題研討和專業培訓。

在 2016-17 年度，我們會繼續安排相關研討會及培訓項目，詳細資料現時未能提供。

-完-

審核 2016-17 度
開支預算

答覆編號

ITB238

管制人員的答覆

(問題編號：5037)

總目： (47) 政府總部：政府資訊科技總監辦公室

分目：

綱領： (1) 政府內部資訊科技的使用

管制人員： 政府資訊科技總監(楊德斌)

局長： 創新及科技局局長

問題：

就為政府網站和網上應用系統進行保安檢查，有關當局可否告知本會：

a) 有關保安檢查開支為何？有否得出什麼結果及評論？如有，有關詳情為何？當局如何處理及回應相關檢查結果，並提升政府內部資訊系統的保護能力？如無原因為何？

b) 當局於 2016-17 年度會否為政府內部資訊系統的保護能力繼續提高？如會，詳情為何？所涉及開支為何？如否，原因為何？

提問人：單仲偕議員(議員問題編號：46)

答覆：

所需資料提供如下：

a) 保安檢查是透過調配資源進行，並不涉及額外資源。結果顯示各局和部門均已制定有效的資訊保安措施，防禦網絡攻擊。此外，各局和部門亦會定期進行保安風險評估，並適時提升各資訊系統的保護能力。

b) 在 2016-17 年度，資科辦會完成對現行《政府資訊科技保安政策及指引》的檢討，以加強相關的遵行規定要求和保安作業模式，藉此應對不同類型的新興威脅，整項檢討工作的預算開支約為 300 萬元。此外，資科辦計劃於 2017 年建立一個網絡威脅資訊共享平台，透過收集和分析不同來源的網絡保安漏洞及威脅的資訊，適時發出警報及提供應對建議，以保護政府內部資訊系統，這個項目預算開支約為 600 萬元。

各局和部門亦會按各資訊系統的風險水平及網絡威脅，提升各系統的保護能力。我們沒有各局和部門在 2016-17 年度相關開支的預算數字。

-完-