2016 年 3 月 14 日
參考文件

立法會資訊科技及廣播事務委員會

資訊保安

目的

本文件向委員匯報自 2015 年 7 月至今，政府各項資訊保安計劃的最新進展。

背景

2. 香港是一個擁有先進電訊基礎設施和廣泛採用資訊及通訊科技的城市。藉着有效使用互聯網服務（包括通訊、流動及智能裝置和應用、網上銀行、電子商務、電子政府及各種形式的電子服務），市民的生活質素得以大大提高，亦為經濟發展提供了穩健的基礎。另一方面，資訊保安及網絡威脅相關的風險為企業及互聯網服務的暢順運作帶來重大影響。因此，可靠及安全的網絡世界十分重要。所有持份者（包括政府、企業及個人）均須了解當中的風險，學習有關技能，並採取適當措施保護其資訊資產和資訊及通訊科技設施。

資訊保安形勢

3. 資訊保安及網絡威脅屬全球性問題，香港亦不例外。在 2016 年年初發表的一份資訊保安報告[1]指出，針對全球政府和企業的協調式攻擊在複雜程度和強度方面持續上升。根據一間國際網絡保安公司在2015年第3季發表的資訊科技威脅演化報告[2]，就銀行業界受網絡威脅方面，在最受針對的經濟體中，香港排名居第六位。

---

1 Akamai Flash Report – Hacktivist (2016 年 2 月）

2 卡巴斯基實驗室，2015 年第 3 季資訊科技威脅演化報告

4. 在2015年，香港警務處（下稱「警務處」）共收到6 862 宗科技罪案報告，較2014年的6 778宗及2013年的5 133宗多。雖然2015年收到的報告數目只是微增（約1%），但2015年的財務損失總額預計約為18億元，較2014年的12億元增加50%。科技罪案不但阻礙關鍵業務的運作，近期的案件亦顯示更多黑客以加密軟件挾持關鍵業務數據勒索要求贖金。

5. 香港電腦保安事故協調中心（下稱「香港協調中心」）在2015年共處理4 928宗保安事故，較2014年的3 443宗增加43%，當中有1 978宗涉及仿冒詐騙，較2014年的594宗大幅增加233%。仿冒詐騙是欺騙受害者透露其敏感資料，如銀行戶口資料、個人資料及其他私人資料。

6. 本文件按以下主要範疇匯報政府各項資訊保安計劃的進展：

(a) 政府層面的資訊保安；

(b) 廣泛社會層面的資訊保安措施；以及

(c) 公眾認知及教育。

政府層面的資訊保安

7. 政府致力保護其資訊基礎設施及數據資產。在2015-16年度，政府各政策局和部門（下稱「局和部門」）共推行120項與資訊保安相關的項目，預計開支總額為1.06億元。這些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。

資訊科技保安政策及管治

8. 政府已制定一套《政府資訊科技保安政策及指引》，供各局和部門遵行。在2016年，我們會完成對現行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，如惡意攻擊、資料外泄、網絡入侵和仿冒詐騙攻擊。

9. 政府資訊科技總監辦公室（下稱「資科辦」）為各局和部門定期進行「遵行審計」，以確保他們符合政府的資訊保安規例、政策和要求。在2015年，我們已為21個局和部門進行遵行審計，識別和建議須予改善的地方。在2016年，我們會另外為大約20個局和部門進行遵行審計。

保安措施及威脅警報

10. 鑑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，協助各局和部門推行適當的保護措施，並加強偵測威脅的能力。所有政府網站必須接受更嚴格的保安風險評估及定期安全檢查，包括保安漏洞掃描及滲透測試。我們亦會為有關支援人員安排培訓，更新他們對新興威脅的知識及技術性技能，以減低相關風險。

11. 網絡威脅可影響不同類型的資訊及通訊科技設施。因此，我們必須採取適當的保護及偵測措施，以防範潛在的資訊及網絡保安威脅。此外，我們亦必須對即將發生的網絡攻擊時刻保持警惕，並發出適時的警報及建議。在2015年，資科辦向各局和部門發出了68次嚴重的保安警報及8份有關資訊保安的催辦便箋，提醒他們採取管理及技術措施，以保護政府網站及數據。

12. 為了應對不斷增加的網絡保安威脅，資科辦計劃在2016 年年中增設一個專責小組及進行調配資源，以加強監察網絡威脅和分享相關資訊的人手及能力。我們亦計劃與業界合作，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，並為各局和部門和市民發布預警。

事故應變及業務持續運作

13. 隨着政府電腦保安事故協調中心（下稱「政府協調中心」）在2015年4月成立，我們會繼續與警務處合作，為各局和部門和互聯網基礎設施持份者舉辦網絡保安演習。通過各種模擬事故場景，測試參與者的事故分析能力、常設的事故應變程序及溝通機制的運作，並持續作出改善。自2015年6月起，我們已為8個局和部門進行網絡保安演習。我們來年會繼續進行此類演習。

能力發展

14. 在政府內部，我們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。在2015年，我們為政府用戶、管理員和資訊科技專業人員舉辦了12項培訓活動，提高他們的保安意識，並介紹最新的資訊科技保安技術及解決方案，藉此增進他們的知識，以保護政府的資訊系統和敏感資料。在2016年，我們會繼續為政府員工舉辦與資訊保安相關的活動。

廣泛社會層面的資訊保安措施

保護互聯網基礎設施

15. 自2015年7月起，我們啓動了3次互聯網基建聯絡小組[3]的保安警報機制，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。我們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。

支援中小型企業（下稱「中小企」）

16. 隨着互聯網及雲端技術的發展，許多中小企把握機遇在電子商務平台擴展業務。資科辦在2016-17年度會向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。我們並與香港協調中心及相關機構合作，為中小企舉辦研討會，提高中小企對網絡威脅的認知，以及分享資訊保安風險管理方面的良好作業模式。

17. 香港協調中心已推出「中小企業網站免費保安檢查先導計劃」，向中小企推廣對資訊保安及網絡威脅的認知，協助他們建立一個更安全的電子商務環境。通過這項計劃，香港協調中心會

[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、香港協調中心、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。

為參與的中小企免費提供網站保安漏洞掃描服務，以及提出改善保安方面的建議。

18. 此外，我們來年會與香港協調中心合作，向中小企推廣「檢查 - 行動 - 驗證」的方法，協助中小企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，以提高中小企的整體網絡保安水平。

與電腦保安事故應變小組社群合作

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，以便向市民發出保安預警。

20. 除了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

21. 由於網絡攻擊的數目持續增加，而且設計日趨精密，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，均會面對網絡保安風險。我們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，以便他們能夠採取適當措施保護電腦裝置及資訊資產。

宣傳及公眾教育

22. 資科辦會繼續聯同警務處、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。在2015年，活動的主題為「網絡保安、四面八方」。我們舉辦了3個公眾研討會，共有超過600人參加。這些研討會提醒公眾網絡威脅無處不在，在使用流動裝置或智能手機時必須保持警覺，並採取適當的風險緩解措施。由於用戶往往是資訊保安中最薄弱的環節，我們認為有需要提供持續的教育及保安認知培訓，向公私營機構推廣「資訊保安、人人有責」的觀念。此外，我們會繼續透過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。

專題推廣

23. 在2015年，資科辦推廣計劃的另一個重點是流動裝置及應用程式的保安事宜。我們播出有關「流動裝置保安」及「流動應用程式保安」的7條電台廣播訊息，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將會在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。峰會的主題包括本地及全球的最新網絡攻擊趨勢，並會舉辦工作坊，讓不同界別（特別是金融業）的網絡保安從業員參加。

亮點活動

24. 為了讓市民及學生對網絡攻擊保持警覺，我們在2015年舉辦了1個圖像設計比賽，參加者反應非常熱烈，共有超過1 500份參賽作品。我們將會與警務處及1間本地大學合作，在2016年年中舉辦「網絡安全比賽2016」，供小學、中學、大專及大學學生參加。我們亦計劃在2016年9月進行為期一周的推廣活動，包括學校探訪及吉祥物設計大賽，以提高學生、青少年及市民的資訊保安認知。

校園教育

25. 向年輕一代推廣使用電腦裝置和管理個人資料的正確態度和做法，是重要的工作。自2008年起，我們已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。在2015年9月至2016年1月，我們已進行約30次學校探訪，接觸了逾12 000名學生、教師及家長。我們會繼續安排更多的學校探訪。

專業培訓及證書

26. 我們鼓勵資訊科技從業員獲取認可的資訊保安專業證書，如國際標準化組織 / 國際電工委員會 27001 主任審核員、資訊系統安全師專業認證（CISSP）、註冊信息系統審計師（CISA）及註冊信息安全經理（CISM）[4]。獲取這些證書有助資訊科技從業員增進保安知識，令他們能夠妥善執行職務和提升服務質素。除了為政府

[4] CISSP: Certified Information Systems Security Professional; CISA: Certified Information Systems Auditor; CISM: Certified Information Security Manager

的員工提供資助以獲得這些資格外，資科辦亦會與業界合作，鼓勵其資訊科技從業員獲取專業證書。

總結

27. 黑客活動猖獗，加上與流動裝置、雲端運算、金融科技趨勢相關及針對終端用戶裝置的攻擊不斷增加，網絡保安所面對的挑戰愈來愈大。我們會致力與不同的持份者緊密合作，以維持一個安全、穩定和可靠的電子政府及電子商務服務環境。

創新及科技局
政府資訊科技總監辦公室
2016 年 3 月