二零一三年七月八日

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二零一二年七月十日至今，政府各項資訊保安計劃的最新進展。

背景

2. 政府資訊保安計劃的目標，是制定及推行資訊保安政策及指引，以供各局及部門遵行及參考，確保政府的所有資訊科技[1]基建設施、系統及資料安全穩妥並具復原能力；以及推廣和提高工商機構及市民大眾對資訊保安和網絡風險的認知。因應上述目標，政府繼續致力提升其資訊保安防護能力，並採取措施保護其電腦系統及系統所涉及的資料私

[1] 在本文件，資訊科技一詞可引伸解作資訊及通訊科技。

隱。我們亦與社會各界合作，以協助提升各界人士保護其電腦系統及資料的能力。本文件按下列三個主要範疇匯報最新狀況：

(a) 資訊保安威脅和風險；

(b) 政府的資訊保安措施；以及

(c) 公眾的資訊保安。

資訊保安威脅和風險

3. 現代社會的資訊科技發展迅速蓬勃，讓個人、機構、大企業及小公司均能隨時隨地、方便快捷地互相連繫及處理業務。然而，因資訊保安風險而導致出現資料外泄或服務中斷的情況也不容忽視。香港電腦保安事故協調中心(下稱「協調中心」)在二零一二年共收到 1 050 宗保安事故報告，較二零一一年增加 30%，其中大部分是黑客入侵和仿冒詐騙事故。根據香港警務處罪案統計數字顯示，在二零一二年共有 3 015 宗科技罪案，大部分是有關非法進入電腦系統和網上商業詐騙的案件，較二零一一年增加 37%。上述統計數字均顯示資訊保安威脅有上升趨勢。

政府的資訊保安措施

4. 政府資訊科技總監辦公室(下稱「辦公室」)已制定全面的保安政策、指引及作業模式，訂明有關保護政府電腦系統和資料的保安規定。我們要求所有政府決策局和部門(下稱「各局及部門」)各自定期進行保安風險評估，並實施機制監察保安規定的遵行情況，以協助他們找出保安漏洞，繼而採取改善措施。辦公室透過造訪和會晤活動進行抽樣檢查，以查核各局及部門在遵行保安規定方面的情況。我們亦安排舉辦資訊保安研討會和培訓課程，以提升員工在處理保安事宜上的能力。各局及部門已經採用了下文概述的良好保安作業模式，以抵禦可能受到的資訊保安攻擊及黑客入侵。

(a) 檢討政府資訊保安規定

5. 在二零一二年，辦公室聯同保安局完成了有關政府資訊保安規例、政策及指引的檢討工作。這項檢討就流動裝置、社交網絡和雲端運算的使用訂立了更嚴格的保安規定，確保在使用這些新技術時，政府的資訊資產可獲得更妥善的

保護。在檢討期間，我們參考了其他經濟體系的保安政策和現行的國際資訊保安標準，例如ISO 27001[2]，以制訂更嚴格的政府保安規定。該檢討亦建議各局及部門應與時並進，覆檢本身的資訊保安政策和程序，以符合最新的保安規定。我們亦修訂和頒布了有關流動保安、雲端保安和私隱保障的保安指引和良好作業模式，以供各局及部門參考。

(b) 保安規定遵行情況和風險評估

6. 自二零一一年起至今，辦公室已造訪 27 個局及部門，並覆檢了他們的保安規管機制。透過這些造訪活動，我們與各局及部門通力合作，以查核保安規定的遵行情況，並為他們提供建議，以加強保安措施。在二零一三至一四年度，我們會繼續造訪另外 15 個局及部門。

7. 在二零一二至一三年度，各局及部門推出了 85 個與保安相關的項目，均旨在提升其資訊保安狀況，預算撥款為 6,580 萬元；在二零一一至一二年度，該等項目共有 71 個，預算撥款則為 3,430 萬元。這些項目包括進行保安風險評估

[2] 「ISO/IEC 27001:2005－資訊科技－保安技術－資訊保安管理系統－要求事項」是一個由國際標準化組織(ISO)和國際電工委員會(IEC)共同制定的標準。

和第三方審計；以及推行技術方案，加強保安和改進現有的保安基礎設施。

(c) 員工的資訊保安教育和專業發展

8. 我們須確保各有關員工明白資訊保安措施的重要性，並確保他們肩負起保護政府系統和資料的責任，這一點是非常重要的。根據我們的資訊保安政策，所有員工須定期接受資訊保安相關教育和培訓，以發展他們在這方面的能力，以便他們履行職責和執行職務。辦公室透過各種渠道提高員工對資訊保安的認知。在二零一二至一三年度，我們舉辦了10 場有關資訊保安的研討會及簡介會[3]，共有超過 1 400 人參加；並為超過 300 名資訊科技從業員安排舉辦 54 項有關資訊保安的深入培訓課程。於今年九月，我們會為各局及部門負責資訊保安的人員安排一個特別培訓課程，確保他們充分了解自己的職務和職責。

9. 我們認為，安排資訊保安支援人員接受正規的培訓，

[3] 有關資訊保安的研討會及簡介會涵蓋多個主題，當中包括「保護敏感資料的機密性、完整性和可用性」、「端點保護」、「有關開發流動應用程式的資訊科技保安和私隱須知」和「雲端－保安面面觀」。

對各局及部門推行保安措施有莫大幫助。目前，在各局及部門工作的有關人員已取得約200張國際認可的資訊安全專業證書[4]。在二零一三年，辦公室人員亦參與國際知名的資訊保安活動，例如出席ISO/IEC JTC 1/SC 27[5]會議和「全球保安事故協調中心組織」會議，與國際保安專家交流保安知識和經驗。

10. 隨着各界更廣泛採用雲端運算，我們在二零一二年七月發出了《雲端保安實務指南》，向各局及部門簡介有關採用雲端服務的保安須知和良好作業模式。我們亦在二零一三年一月印發了一套宣傳單張和海報，以提醒各局及部門在使用流動裝置和抽取式媒體時，須採用良好作業模式以保護資料。該套宣傳單張和海報亦已上載到我們的資訊保安專題網站（www.infosec.gov.hk），供公眾參考。

11. 為了確保各局及部門知悉即將出現的威脅，讓他們能迅速採取預防措施，我們會按需要發出嚴重保安警報（包括

[4] 資訊安全專業證書包括: 由國際資訊系統保安認證協會(ISC)2 所頒發的資訊系統安全師專業認證(CISSP)和由國際信息系統審計協會(ISACA)所頒發的註冊信息系統審計師(CISA)。

[5] ISO/IEC JTC 1/SC 27 是指國際標準化組織和國際電工委員會第一聯合技術委員會／第 27 分技術委員會。

可能出現的網絡攻擊）和有關資訊保安的催辦便箋，要求各局及部門即時處理。在二零一二至一三年度，我們發出了 82 次嚴重保安警報和三份有關資訊保安的催辦便箋。

(d) 資訊保安良好作業模式

12. 為了抵禦可能受到的資訊保安攻擊和黑客入侵，政府繼續採用以下資訊保安良好作業模式，加強我們的防護能力，包括：

(i) 在互聯網接口安裝防火牆、抗電腦病毒軟件和入侵偵測及防禦系統，以保護重要系統及應付保安威脅；

(ii) 適時更新系統軟件及使用最新病毒識別碼，以防止惡意軟件的入侵；

(iii) 所有機密資料在儲存和傳送時必須加密；以及

(iv) 定期為重要資訊系統進行保安風險評估及審計。

上述做法一直行之有效，可妥善保護我們的電腦系統。

公眾的資訊保安

13. 在公眾層面，辦公室亦與業界合辦多項活動，以提高公眾對資訊保安的認知，並推廣社會各界採用良好的資訊保安作業模式。

(a) 資訊保安認知推廣活動

14. 資訊保安認知對公眾甚為重要，可讓他們能抵禦嶄新和不斷演變的保安威脅。辦公室時刻留意全球資訊保安趨勢及發展，並通過一站式的「資訊安全網」網站，為市民提供許多有關資訊保安的參考資料和最新資訊。另外，辦公室繼續全年舉辦各類活動，以提高公眾對資訊保安的認知，並推廣社會各界採用良好的資訊保安作業模式。自二零一二年起，我們採用「共建網絡安全」為主題，透過公開研討會、電台節目、網站和海報設計比賽等活動，以提高公眾意識，使他們懂得加強保護自己的電腦設備免受網絡攻擊。在二零一三年，我們會舉辦四場公開研討會和一項短片比賽，目的是令公眾更注重採取保安措施以對付網絡威脅。

15. 辦公室一直支持業界舉辦的資訊保安活動。在二零一二至一三年度，辦公室參加了八場由本地業界或專業組織舉辦的資訊保安公開研討會，並就資訊保安課題向與會者發表講話。

(b) 採用良好作業模式和國際標準

16. 為了提高公眾、大型企業和中小型企業對雲端保安的認知，我們與雲端運算服務和標準專家小組[6]合作編製了兩份資訊保安備忘事項，供雲端服務用戶和供應商參考。該兩份備忘事項，分別為《雲端服務用戶的資訊保安備忘事項》和《雲端服務供應商在雲端平台上處理可識別個人資料的資訊保安及保障私隱備忘事項》，已透過二零一三年一月推出的「雲資訊網」專題網站發布。我們會繼續與業界合作，舉辦活動進一步推廣採用良好作業模式。

17. 政府致力推動及促進業界制訂和採用國際保安標準與良好作業模式。在二零一四年四月，我們將在香港主辦 ISO/IEC JTC 1/SC 27 會議。第 27 分技術委員會的工作範圍

[6] 雲端運算服務和標準專家小組是由辦公室於二零一二年四月成立，成員來自業界、學術界和政府，專責協助推動香港應用和發展雲端運算。

是就有關資訊保安的通用方法和技術制訂標準。我們預計會有約 300 名來自超過 30 個經濟體系的保安專家和專業人員出席會議，並在會議上討論資訊保安技術及相關標準。由第 27 分技術委員會管理的標準，包括 ISO 27001 和 ISO 27002 標準，定出了對資訊保安管理系統的要求，並就資訊保安管理良好作業模式提供了建議。

(c) 協調社會各界對威脅作出應變

18. 協調中心是協調本地企業及互聯網用戶處理電腦保安事故的機構，其職責是協助發布有關消息、就針對保安威脅的預防措施提供意見，以及推廣資訊保安認知。在二零一二年，協調中心共發出了 429 次保安警報，適時為市民提供了有關當前保安威脅和保安漏洞的消息。為了讓市民可透過其流動裝置得知最新的重要保安信息，協調中心於二零一二年五月推出了一個流動應用程式，以便市民接收最新的警報和消息。自二零一二年十二月起，「香港政府通知你」流動應用程式亦已在新設的「資訊保安」類別下轉發協調中心的保安警報。截至二零一三年六月初，這個類別的用戶數目約為 90 000 個。

19. 鑑於分布式拒絕服務的網絡攻擊有上升趨勢，協調中心在二零一二年十月進行了主題為「抵禦電腦黑客的網絡攻擊」的網絡保安演習，以提高參與機構[7]在處理此類攻擊的就緒度。是次演習成功測試了各參與機構的事故應變程序。另一次演習活動已計劃於本年較後時間舉行。

20. 辦公室正與香港警務處和協調中心緊密合作，互相交換有關嶄新保安威脅的情報，並合力採取措施對抗網絡攻擊。香港警務處在二零一二年十二月成立了網絡安全中心，以加強保護本港的關鍵基礎設施，並提升本港在抵禦網絡攻擊時的復原能力。該中心負責收集有關網絡保安的情報，並與各局及部門、本地及海外持份者緊密合作。在二零一三年首五個月，辦公室曾協調有關各方處理了八宗涉嫌攻擊政府服務的事故，並協助有關局及部門積極採取預防措施，使有關服務不受影響。

[7] 參與機構包括(固定和流動)網絡供應商、域名註冊服務機構、香港互聯網註冊管理有限公司、香港互聯網供應商協會、香港警務處、辦公室和協調中心。

總結

21. 我們會繼續保持警惕，留意當前的保安威脅，並採取各項措施，保護政府的資訊系統和資料、提高社會各界的保安認知，以及保護本地的網絡環境。

商務及經濟發展局

政府資訊科技總監辦公室

二零一三年七月