立法會
Legislative Council

立法會CB(1)435/06-07(06)號文件

檔　號：CB1/PL/ITB

資訊科技及廣播事務委員會

2006年12月11日舉行的會議

有關資訊保安的背景資料簡介

目的

本文件旨在綜述委員就資訊保安事項提出的意見和關注。

背景

2. 在發生個人資料於互聯網上外泄事件後，事務委員會在2006年3月17日的會議上討論資訊保安議題。其後在2006年4月6日舉行的會議上，事務委員會決定跟進此議題，並要求政府當局提交綜合報告，說明各政策局、部門和公營機構現時的資訊保安狀況。

政策局和部門的資訊保安架構

3. 政府參考國際最佳作業模式，制訂了一套資訊保安政策、指引及有關程序，供政策局／部門採用，當中包括基準資訊科技保安政策、資訊科技保安指引、保安風險評估和審核指引及資訊保安事故處理指引。這些程序和指引會不時予以覆檢，以反映技術和保安威脅的轉變。它們在組織、管理、技術及程序各方面提供資料，讓各政策局／部門可按之自行建立資訊保安架構和作業模式。各政策局／部門亦須遵守政府《保安規例》的規定。在《保安規例》的條文當中，有一條是為資訊系統及資料的儲存、處理及傳送而設，所針對的課題包括機密資料、密碼匙管理、實體保安及妥善銷毀機密資料。

4. 為監管和執行政府內部的資訊保安，當局於2000年成立資訊保安管理委員會，其核心成員包括保安局及政府資訊科技總監辦公室的代表。此外，為了在行政上支援該委員會，政府成立資訊科技保安工作小組，負責在各政策局／部門推行及監察資訊科技保安政策及指引的實施。

5. 在中央層面，政府資訊保安事故應變辦事處已經成立，負責統籌和協助各部門處理政府資訊保安事故。為支援該辦事處的運作，政府資訊科技總監辦公室成立常設辦公室，24小時無間斷地監察電腦病毒及資訊保安事故，以及密切注視在全球各地爆發的病毒及有關警報。在有需要時，常設辦公室會知會保安架構中的有關單位，而當確定保安問題事態嚴重，則會立即向各部門發出病毒或保安警報。各主要政府基建系統的管理人員每周均須就系統的保安狀況及其他涉及資訊科技保安事宜，向政府資訊科技總監辦公室提交報告，以供管理監察及控制之用。

6. 在部門層面，所有部門均須委任一位高級人員，作為部門資訊科技保安主任，負責該部門的整體資訊保安管理及運作。此外，各部門須設立資訊保安事故應變小組，以處理一切有關日常保安事故的報告及回應的事宜。每個部門的資訊科技管理小組將會與相關部門主管共同留意該部門的資訊保安情況。

事務委員會委員提出的主要意見及關注

7. 委員知悉，政府已制訂一套全面的資訊保安政策和指引，供政策局／部門採用，但他們關注到，***各政策局／部門有否妥當依循既定的政策和指引***。此外，委員對於***公營機構的資訊保安狀況***亦感關注，以及***各規管機構如何確保其所規管的業界機構遵從資訊保安作業模式和規定***。

就資訊保安提出的立法會質詢

8. 在2006年12月6日的立法會會議上，單仲偕議員就資訊保安提出質詢。簡括而言，單議員關注到，資訊保安管理委員會及資訊科技保安工作小組在提高政府內部資訊保安能力所採取的措施的成效，以及公營機構的整體資訊保安能力。政府當局回答時表示，為確保資訊保安規定得到遵從，各政策局／部門必須為其資訊系統定期進行資訊保安風險評估及檢討。此外，政府每年對各政策局／部門進行資訊保安狀況調查。這些程序和措施對增強各政策局及部門整體的保安狀況證明有效。關於公營機構的資訊保安能力，政府資訊科技總監辦公室在2006年3月，曾向負責這些主要公營機構的政策局／部門進行調查，以瞭解這些機構所推行的資訊保安措施，並察悉這些機構已採取各種措施，以防範資訊保安威脅。2006年8月，政府當局進行另一項有關公營機構資訊保安狀況的調查，並會在2006年12月11日的會議上向事務委員會匯報結果。(單仲偕議員的質詢及政府當局的書面回覆載於**附錄I**。)

最新情況

9. 事務委員會要求政府當局在2006年12月11日的會議上向委員簡報以下事項：

(a) 各政策局／部門現時的資訊保安狀況；

(b) 各規管機構如何發揮監察作用，確保在個別規管職權範圍內的相關業界遵守和遵從有關資訊保安的規定；及

(c) 公營機構採取的措施，以維持及加強資訊保安(包括哪些機構拒絕提供所需資料，以便事務委員會參考)。

相關文件

10. 相關文件一覽表載於**附錄II**。

立法會秘書處
議會事務部1
2006年12月8日

附錄I

立法會問題第十七條
(書面答覆)

提問者：單仲偕議員　　會議日期：二零零六年十二月六日

作答者：工商及科技局局長

問題：

鑒於近期發生政府部門及公營機構洩漏市民個人資料的事件，政府可否告知本會：

(一) 現時資訊保安管理委員會及資訊保安工作小組採取了甚麼措施，以確保各政策局和政府部門遵守由政府資訊科技總監制定的資訊科技保安政策和指引；

(二) 有否評估上述措施能否有效加強政府內部的資訊保安能力；若有，評估的結果；若否，原因為何；

(三) 有否評估各政策局和政府部門及公營機構的整體資訊保安能力；若有，結果為何；若否，有否計劃進行評估；若有，有關的詳情；

(四) 會否考慮將資訊科技保安指引的適用範圍擴展至所有公營機構，以保障市民的個人資料；及

(五) 有否計劃撥出額外資源，包括撥款進行資訊保安工程及投資硬件，以改善各政策局和政府部門及公營機構的資訊保安能力？

答覆：

主席女士：

(一) 為監管和執行政府內部的資訊保安，政府成立了資訊保安管理委員會(ISMC)及資訊保安工作小組(ITSWG)。資訊保安管理委員會已制定及頒布一套完善的資訊科技保安政策、程序及有關指引供各局及部門遵守。為確保政府保安規定的遵行，各政策局／部門必須為其資訊系統定期進行資訊保安風險評估及檢討。在處理資訊保安事故方面，政府資訊保安事故應變辦事處(GIRO)提供指導及協助各部門處理政府資訊保安事故。而各部門均須委任一位高級人員，充當部門資訊科技保安主任(DITSO)，負責該部門的整體資訊保安管理及運作。此外，各部門須設立資訊保安事故應變小組(ISIRT)，以處理日常保安事故的報告及回應。

(二) 政府資訊科技總監辦公室在資訊保安的事情上與部門緊密合作，並定期檢討政府有關資訊科技保安規例、政策、程序及指引，以靠貼不斷發展的科技及國際／業界作業模式。此外，透過每年對各局及部門進行資訊保安狀況調查，讓我們得以了解各局及部門實施的保安措施，並提供有用的提示以持續增強所推行的資訊保安架構及科技措施。這些程序和措施對增強各局及部門整體的保安狀況証明有效。

(三) 透過每年對各局及部門進行資訊保安狀況調查，我們得以了解各局及部門實施的保安措施，而最近一次調查則在本年七月進行。為了解主要公營機構處理資訊保安威脅所採取的防範措施，在本年三月，政府資訊科技總監辦公室亦已就負責這些機構的決策局及部門進行調查。據有關決策局及部門表示，這些機構已採取各種措施，以防範資訊保安威脅。

於本年八月，政府資訊科技總監辦公室亦透過各局及部門的協助，對其負責規管的公營機構的資訊保安狀況作出調查。我們已準備了一份有關資訊保安的報告，當中包括各局及部門和公營機構的資訊保安狀況的資料，並安排於十二月十一日的立法會資訊科技及廣播事務委員會會議上提交，以作討論。

(四) 政府資訊科技總監辦公室已建議負責規管各公營機構的決策局及部門，鼓勵這些機構根據他們的情況採納資訊保安指引。這些指引已在供公眾可閱覽的「資訊安全網」(http://www.infosec.gov.hk)網站發布。此外，我們會和個人資料私隱專員公署及有關業界合作，宣傳保護個人資料對電子交易的重要性。

(五) 各局及部門須建立及不斷增強其資訊保安，而部門可透過現有的撥款程序申請有關資訊保安工程所須款項。而用作檢討及增強資訊保安工程所須的非經常性費用，將會由「基本工程儲備

基金總目710電腦化計劃」撥款來支付。至於公營機構的資訊保安事宜，他們須自行籌措所需的投資、資源及資金。

附錄II

相關文件一覽表

委員會	文件	立法會文件編號
資訊科技及廣播事務委員會2006年3月17日的會議	✧ 政府當局的文件："資訊保安"	CB(1)1097/05-06(01)
	✧ 單仲偕議員就"資訊保安"提出的質詢	CB(1)1096/05-06(07)
	✧ 政府當局回應單仲偕議員就"資訊保安"提出的質詢	CB(1)1214/05-06(01)
	✧ 會議紀要	CB(1)1382/05-06
資訊科技及廣播事務委員會2006年4月6日的會議	✧ 會議紀要	CB(1)1600/05-06