

立法會

Legislative Council

立法會CB(1)2063/06-07(01)號文件

檔 號：CB1/PL/ITB

資訊科技及廣播事務委員會

2007年7月9日舉行的會議

有關資訊保安的最新背景資料簡介

目的

本文件提供有關資訊保安議題的最新資料，並綜述委員對此議題表達的最新關注。

背景

2. 2006年年初發生一連串的个人資料於互聯網上外泄事件後，資訊保安已成為一個主要的關注事項。根據政府當局的資料，政府設有一套資訊保安政策和指引，以供政府決策局及部門(下稱"各局及部門")採用。政府還設有管理架構、技術保安措施及其他保安機制，以監察、偵察及堵截政府內的電腦系統和網絡懷疑及可能受到的入侵。該等措施的詳情載於"有關資訊保安的背景資料簡介"(立法會CB(1)435/06-07(06)號文件)，可登入此網頁瀏覽：<http://www.legco.gov.hk/yr06-07/chinese/panels/itb/papers/itb1211cb1-435-6-c.pdf>。

3. 就政府對公帑資助機構所擔當的角色，政府當局表示，政府透過負責的各局及部門，監察其職權範圍下的公營機構及規管機構的資訊保安狀況。關於公營機構採取的資訊保安措施，一般而言，該等措施包括保安管理架構、資訊保安政策或指引、保安修補程式管理、保安風險評估及審計、事故及應變管理等。至於規管機構，它們所採取的資訊保安措施大致上包括強制資訊保安管理、風險評估／審計／覆檢、資訊保安事故應變程序等。如欲瞭解詳情，請參閱政府當局的文件(立法會CB(1)435/06-07(05)號文件)，可登入此網頁瀏覽：<http://www.legco.gov.hk/yr06-07/chinese/panels/itb/papers/itb1211cb1-435-5-c.pdf>。

4. 在發生個人資料於互聯網上外泄事件後，事務委員會於2006年3月17日的會議上討論此議題。其後於2006年4月6日舉行的會議上，事務委員會要求政府當局提交一份綜合報告，說明各局及部門、公營機構及規管機構的資訊保安狀況。

各局及部門、公營機構及規管機構的資訊保安狀況報告

5. 因應事務委員會要求取得一份綜合報告，說明各局及部門、公營機構及規管機構的資訊保安狀況，政府當局就各局及部門、公營機構及規管機構進行調查，並於2006年12月11日舉行的事務委員會會議上匯報調查結果。

6. 委員從有關各局及部門的調查結果得悉，中央組織設有全面的管理架構和行之有效的政策，各類指引亦齊備，以供各局及部門遵守。各局及部門中約有84%已完成資訊科技保安風險評估和審計，而其餘的亦會在2007年3月底前完成有關工作。各局及部門已就其關鍵業務的資訊系統，制訂業務持續運作及／或運作復原的應變計劃，以應付網上保安事故。另外，各局及部門已推行修補程式管理措施，確保妥善堵塞軟件的保安漏洞。不過，為提高各局及部門對遵守保安規定的成效，政府已訂立一項新機制，規定各局及部門每年就其遵守政府資訊保安規定的情況，向政府資訊科技總監辦公室提交報告，以便可在較早階段發現任何異常情況。此外，當局亦實施一項由中央管理及統籌的隨機／抽樣保安審計，確定各局及部門已恰當地完成所需的保安風險評估及覆檢，以及各局及部門有妥善跟進各項改善建議。審計程序已於2007年年初開始，並將於兩年內完成各局及部門的審計。

7. 然而，在公營機構及規管機構方面，委員注意到，調查顯示40%的公營機構沒有制訂資訊保安管理架構，41%的機構沒有資訊保安政策或指引，更有多達41%的機構沒有採取任何保安風險評估及審計以作資訊保安保證，而34%的機構在短期內甚至沒有此計劃。關於防範限閱／機密資料於不慎的情況下洩漏，43%的機構沒有採用任何技術工具，例如資料加密以確保資料得以妥善儲存、傳送及處理。至於規管機構，85%的機構沒有設立強制資訊保安管理架構，62%的機構沒有進行風險評估／審計／覆檢，而31%的機構沒有設立資訊保安事故應變程序。

8. 有關上述兩項調查工作結果的詳情，可登入此網頁瀏覽：
<http://www.legco.gov.hk/yr06-07/chinese/panels/itb/papers/itb1211cb1-435-5-c.pdf>。

委員的關注

9. 鑒於上述有關公營機構及規管機構的資訊保安狀況，以及政府當局指出部分公營機構及規管機構有迫切需要作出改善，委員對這兩類機構的資訊保安狀況深表關注，並且認為，負責的各局及部門應盡快與職權範圍下的公營機構／規管機構跟進須採取的保安保護改善措施。政府當局亦應在數個月內提交中期報告，概述公營機構／規管機構採取跟進行動的進展，然後於2007年7月再次向事務委員會簡報此議題。事務委員會又認為，當事務委員會於2007年7月再次討論此議題，倘若屆時在有迫切需要作出改善的公營機構中，仍有部分尚未改善其資訊保安狀況，政府當局應披露它們的名稱，供事務委員會參考。

公營機構及規管機構所執行資訊保安改善措施的中期進展報告

10. 政府當局於2007年4月提交上述中期進展報告。根據政府當局的資料，截至2007年3月12日，在104家公營機構及58家規管機構中，分別收到96家公營機構及43家規管機構提交的所執行資訊保安改善措施的最新進展資料。在公營機構方面，28%的機構已完成資訊保安改善計劃，29%的機構已開展實施工作，以期在2007年年中／年底完成所需的改善措施。不過，43%的公營機構回覆未能在2007年內完成所有改善項目，理由是需待政策批准、項目撥款、計劃協調或選定技術方案及培訓課程。然而，必須的改善項目都已經完成或展開。

11. 在規管機構方面，39%的機構表示已設定規管制度，著重資訊保安及保護個人資料的重要性，而另外12%的機構則擬定了行動計劃，改善轄下行業的資訊保安。其餘49%的規管機構認為，現行的規管制度並無條文規定必須規管其轄下行業的資訊保安範疇；儘管如此，約半數規管機構表示會採取行動，加強轄下行業的資訊保安。

最新情況

12. 政府當局將於2007年7月9日舉行的事務委員會會議上，提供有關公營機構及規管機構所執行資訊保安改善措施的最新進度報告。

相關文件

13. 相關文件一覽表載於**附錄**。

立法會秘書處

議會事務部1

2007年7月5日

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	<ul style="list-style-type: none"> ✧ 政府當局的文件："資訊保安" ✧ 單仲偕議員就"資訊保安"提出的質詢 ✧ 政府當局回應單仲偕議員就"資訊保安"提出的質詢 ✧ 會議紀要 	CB(1)1097/05-06(01) CB(1)1096/05-06(07) CB(1)1214/05-06(01) 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	<ul style="list-style-type: none"> ✧ 會議紀要 	CB(1)1600/05-06
資訊科技及廣播 事務委員會 2006年12月11日 的會議	<ul style="list-style-type: none"> ✧ 政府當局的文件："資訊保安" ✧ 有關資訊保安的背景資料簡介 ✧ 跟進文件："資訊保安" ✧ 會議紀要 	CB(1)435/06-07(05) CB(1)435/06-07(06) CB(1)1329/06-07(01) CB(1)669/06-07