2007 年 7 月 9 日
參考文件

立法會
資訊科技及廣播事務委員會

資訊保安

A. 目的

本文件旨在向委員報告公營機構及規管機構執行資訊保安改善措施的進展，以及政府決策局及部門 ("各局及部門")推行的資訊保安計劃。

B. 背景

2. 政府資訊科技總監辦公室於 2006 年 7 月及 8 月，就各局及部門、公營機構及規管行業的資訊保安狀況，完成有關調查。根據調查結果，立法會資訊科技及廣播事務委員會("委員會")在 2006 年 12 月 11 日會議席上建議盡快執行有關改善措施，並要求當局在 2007 年 7 月向委員會匯報工作進度，以及在 3 個月內提交中期報告。

C. 工作進度摘要

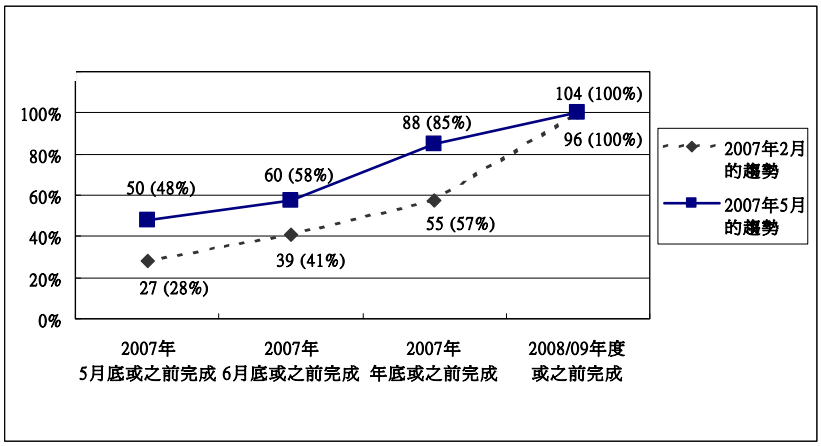
3. 政府資訊科技總監於 2006 年 12 月 27 日，建議各局及部門根據調查結果跟進轄下公營及規管機構的資訊保安改善措施，以及列舉現況可見的保安問題，並於 2007 年 2 月 13 日，要求各局及部門協調及收集轄下機構執行改善措施的進度。中期報告已經編纂及於 2007 年 4 月初提交給委員會。

4. 政府資訊科技總監於 2007 年 5 月 21 日，再次要求各局及部門協調及收集轄下機構執行改善措施的進度，以便編纂報告及在 2007 年 7 月向立法會提交。我們得到各局及部門的持續支持，已於 2007 年 6 月 13 日全數收到 104 個公營機構及 58 個規管行業的回覆。

D. 公營機構

5. 根據收集的數據，公營機構在執行改善措施方面有明顯進步。截至 2007 年 5 月底，在 104 個公營機構中，50 個(48%)已完成所有資訊保安改善措施，而在 2007 年年底或之前完成所需改善措施的公營機構數目，將累積至 88 個(85%)。如下圖顯示，相對中期報告的結果，分別爲 27 個(28%)及 55 個公營機構(57%)，目前的進度較中期報告的結果爲佳。

圖表1 – 公營機構的實施進度



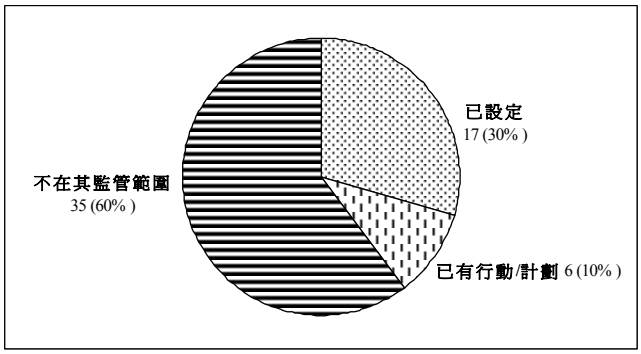
6. 16 個公營機構(15%)表示未能在 2007 年內完成所有改善項目，但已實施部分計劃，其中 8 個會在 2007/08 財政年度內完成所有項目。這些機構需要延長實施計劃，主要受相關的工作影響。

7. 至於個別改善措施，在全數 884 個改善項目中，661 個 (75%)已於 5 月底完成，而約 97%將於 2007 年內完成。餘下的 3%項目，主要是進行資訊保安風險評估及系統審計、改善外判資訊科技服務合約條款，以及實施更先進的保安功能。6 類保安措施的實施進度摘要載於**附件**，以供參考，當中包括保安管理、保安規管、保安技術的採用、限閱／機密資料的處理、員工的保安認知及培訓，以及資訊科技服務外判。

8. 收到的回覆顯示，所有類別均有持續進展，其中一些公營機構透過負責規管的決策局及部門，採納了政府資訊科技總監的建議，完成員工保安認知及培訓方面的改善計劃。資訊科技服務外判方面也有持續改善，大部分公營機構加強了外判工程的合約條款、質素保證及保安規管，確保承辦商遵守有關機構的保安規定。

E. 規管行業

9. 58 個規管行業全部提交回覆。調查的結果顯示，由於增加了一個規管行業已執行或將會執行資訊保安措施，個別規管行業這方面的整體狀況只有輕微改變。35 個規管機構認爲，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。



圖表 2 – 規管行業收緊規管制度的狀況

10. 除了收緊規管制度外，一些規管機構表示會採取行動，改善轄下行業的資訊保安，例如向規管行業發出催辦便箋，以強調保護客戶及僱員個人資料的重要性；要求規管行業在運作時遵從有關資訊保安作業模式事宜通告內的規定；促請規管行業參考政府資訊保安政策及指引；以及在定期視察時，建議有關資訊保安的良好作業模式。

F. 各局及部門

11. 確保資訊安全是每名政府僱員的個人責任，而在處理政府資料的時候亦必須遵照保安規例的一般指引。在處理電子資料時，各局及部門均須遵守政府資訊科技總監辦公室對有關方面不時發出的要求。爲了加強監察各局及部門在資訊保安政策的遵行情況，政府已實施中央統籌的保安審計，當中包括查核各局及部門有否恰當地完成保安風險評估、進行檢討和採取建議的跟進措施。我們會從 2007 年 5 月起，在兩年內爲各局及部門完成上述保安審計。各局及部門的首長有責任作出保安措施，保護轄下各類政府資料，並在違反保安規定的事件發生時採取行動，包括根據有關規例採取紀律處分。

12. 爲增強規管政府整體的資訊保安，以及協助各局及部門執行資訊保安的管理職務，我們要求各局及部門就政府資訊保安規定和政策的遵守情況進行自我評估，並向政府資訊科技總監辦公室提交由高級管理層批准的周年報告。報告的資料有助政府訂定新的工作方案，進一步加强整體的資訊保安。

13. 爲提升僱員對資訊保安及數據保護的認知，政府已透過多種渠道送達有關培訓資料，包括網上學習課程，以及各資訊保安課題的研習班。一個特別爲行政主任設計的全新研討課程系列《政府資訊保安》已於本年 5 月推出，用以加强同事在部門日常運作所需的保安知識和技能。

G. 總結

14. 結果顯示，公營及規管機構已更加了解資訊保安及數據保護的重要性。透過這些調查和執行改善措施，管理層更重視而員工亦更明白資訊保安，從而加強保安狀況。由於資訊保安是需持續關注的題目，公營及規管機構應留意網上威脅，並持續保護電腦資產和所保管的限閱/機密資料。政府方面，我們會繼續透過定期查核遵守保安規定的情況、保安審計及有效的員工訓練課程，加强內部的資訊保安和數據保護。

H. 未來路向

15. 爲提升公營及規管機構管理層的重視及員工的認知以及加強保安措施，政府會繼續監察有關資訊保安改善措施的進度，並經各局及部門提供建議和協助。政府資訊科技總監辦公室會定期更新政府的一站式資訊安全網站，提供最新的消息及參考資料，向各局、部門及市民發出保安警告，以及與業界合作，推廣資訊保安的認知和教育。

I. 徵詢意見

16. 請委員察悉本文報道的內容。

商務及經濟發展局
政府資訊科技總監辦公室
2007 年 7 月

附件

保安措施類別的實施進度

保安措施類別	建議措施數目				
	2007 年 2 月底或之前完成	2007 年 5 月底或之前完成	計劃於 2007 年 6 月底或之前完成	計劃於 2007 年年底或之前完成	計劃於 2008/09 年度或之前完成
保安管理	98 (40.3%)	178 (73.3%)	188 (77.4%)	235 (96.7%)	243 (100%)
保安規管	67 (42.1%)	112 (70.4%)	122 (76.7%)	156 (98.1%)	159 (100%)
保安技術的採用	63 (51.2%)	91 (74.0%)	94 (76.4%)	115 (93.5%)	123 (100%)
限閱／機密資料的處理	43 (46.7%)	70 (76.1%)	75 (81.5%)	89 (96.7%)	92 (100%)
員工的保安認知及培訓	52 (53.1%)	78 (79.6%)	82 (83.7%)	97 (99.0%)	98 (100%)
資訊科技服務外判	95 (56.2%)	132 (78.1%)	141 (83.4%)	164 (97.0%)	169 (100%)
總計	418 (47.3%)	661 (74.8%)	702 (79.4%)	856 (96.8%) (見下文備註)	884 (100%)

備註: 餘下3.2%的改善項目，主要是進行資訊保安風險評估及系統審計、改善外判資訊科技服務合約條款，以及實施更先進的保安功能。

保安措施類別的要項:

類別	要項
保安管理	政策及管理、營運保護措施、應變措施、保安風險評估及審計
保安規管	遵守規定測試、支援及隨機抽查
保安技術的採用	基本工具、特殊數據處理措施、與網絡有關的措施、資產保護
限閱/機密資料的處理	運作措施、技術工具
員工的保安認知及培訓	促進資訊保安認知、鼓勵員工考取資訊保安專業資格、定期發出催辦便箋
資訊科技服務外判	合約條款、質素保證及控制、保安監管及控制