2006 年 12 月 11 日會議
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的資訊保安狀況及政府爲加強資訊保安而採取的各項措施。

B. 背景

2. 政府曾於本年 3 月 17 日，向資訊科技及廣播事務委員會（“委員會”）提交參考文件(立法會文件第CB(1)1097/05-06(01) 號)，闡述政府就保護決策局及部門(“各局及部門”)的資訊資產及個人資料所採取的措施。隨著資訊及通訊科技的急促發展，相關的網上保安風險正日益增加。面對這趨勢，政府有需要相應地提高現有保安措施的水平。

C. 各局及部門、公營機構及規管機構的資訊保安狀況報告

3. 政府因應委員會在本年 4 月 6 日會議席上提出的要求，已就各局及部門、公營機構的資訊保安狀況，以及規管機構如何監察轄下組織的資訊保安概況，完成有關調查。調查結果載於本文**附錄A**。

D. 建議跟進行動

4. 有鑑於近日發生的資訊保安事故，並參考了上述調查的結果，政府已在整體資訊保安計劃中納入新行動，以加強本港的資訊保安措施。下文將簡述這方面的最新進展及政府擬就現有措施將作出的提升。

(i) 以各局及部門爲目標的措施

5. 政府將繼續以身作則，在資訊及通訊科技應用的同時，確保各局及部門能達致穩固的資訊保安狀況。

政策及規管

6. 政府會對資訊保安規例、政策、程序及指引作定期的檢討及強化，以配合急速發展的科技及國際間／業界良好作業模式和標準，與及不斷出現的保安威脅。最近一次檢討及修訂已於 2006 年 5 月完成和發佈給各局及部門遵行有關的修改。

保證與遵從

7. 政府資訊科技總監已籲請各局及部門的首長，必須定期進行資訊保安風險評估、保證及審計，而對於關鍵業務的資訊系統，則最低限度要每兩年進行一次。新近的備忘通告已於 10 月初發出。另外，我們正準備推行一項新增的機制，規定各局及部門每年就保安規定的遵守情況提交報告。該報告必須由各局及部門的高級管理層認同。

外判資訊科技服務標書的規定

8. 政府資訊科技總監辦公室已在中央管理的合約內加入條款，以確保資訊科技及相關服務的承辦商與其分判商，按照合約條款履行資訊保安規定，一如政府人員須遵守這些規定。我們亦已提醒各局及部門，就自行安排的相關服務合約內加入相若的條款。

9. 我們提醒各局及部門要謹慎考慮，在擬定外判資訊科技服務的採購標書中訂立對資訊系統的品質要求，以確保處理個人資料及機密資料時能夠遵守政府資訊保安規定。在審批外判安排時，各局及部門必須確認政府基準資訊科技保安政策的各項保安規定已被考慮，而這些規定亦已在採購標書內詳細列明。這些規定包括外判資訊系統的保安、實體保安、接達控制保安、數據保安、應用系統保安、網絡及通訊保安等。

獨立保安審計

10. 因爲各局及部門對其業務最爲清楚，所以進行內部檢視對保安規定的遵守程度亦責無旁貸。爲提高各局及部門在檢視工作的成效，政府將實施一項由中央管理及統籌的隨機／抽樣保安審計，以確定各部門有恰當地完成保安風險評估和作出切合的改善跟進。我們計劃從2007 年初開始，於兩年內爲各局及部門作上述保安審計。

員工保安認知及教育

11. 政府資訊科技總監辦公室已發出有關資訊保安事宜的通告，及經常提醒各局及部門應該留意新近發現的軟件保安漏洞、保安警報通

告，與及處理保安事故的技巧。政府資訊科技總監已籲請各局及部門的首長向所有工作人員傳閱與資訊保安有關的通告、公告及保安警報。此外，我們亦建議各局及部門應該定期傳閱該等文件，以維持員工的保安認知。爲提高政府人員對資訊保安的認知和知識，我們會研究及提供多種渠道來送達資訊保安和數據保護的培訓資料，以便同事能按適合自已的方法和時間學習。

(ii) 以公營機構爲目標的措施

12. 從公營機構資訊保安狀況的調查發現，有部份機構需要急切改善其資訊保安狀況。這些資訊保安不足的機構，更容易蒙受到保安攻擊，資料外泄或數據流失的問題。爲改進公營機構的資訊保安狀況，政府資訊科技總監辦公室建議負責規管這些組織的決策局及部門必須根據調查報告的建議與有關機構跟進和作出改善及修補漏洞。

(iii) 以規管機構／行業爲目標的措施

13. 資訊保安事故，例如任何機構泄漏個人資料，都可能對有關機構所屬的行業造成嚴重後果，例如削弱其可信度、甚或引起訴訟。政府資訊科技總監辦公室建議負責規管機構的決策局及部門，關於向受規管的業內組織解釋需要採取保安措施的重要性。各規管機構甚至應該考慮收緊有關行業的規管，以強調資訊保安及個人資料保護的重要性。下述的公眾認知和教育工作亦能切合規管機構／行業的需要。

(iv) 以市民大眾爲目標的措施

保護個人私隱

14. 鑑於社會人士對電子通訊及交易所涉及的資料保密問題日表關注，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。另外，我們會爲業界人士及有關從業員舉辦會議、研討會及展覽，鼓勵大家分享數據保護的優良作業模式和經驗。

社區推廣和教育

15. 政府資訊科技總監辦公室正採用不同的資訊發放渠道，向市民推廣和灌輸有關資訊保安的知識。「資訊安全網」(http://www.infosec.gov.hk) 是一個一站式的入門網站，爲市民提供有關資訊保安的最新消息、參考資料和保安警報。爲了不斷加强該網站的內容，我們在 2006 年內，已把該網站的內容頁數已由 1,200 頁增加至 1,400 頁。我們亦推出了一連串的公眾推廣活動(詳情載於**附錄B**)。這些活動包括加强網站的內容供市民大眾參考、舉辦研討會、展覽會、電台節目、電視特輯，以及派發宣傳小冊子和舉辦嘉年華會等。

16. 爲方便使用電子服務來進行商業交易或私人通訊時能夠採用恰當的接達控制，政府會在 2007/08 年度公布一份有關保安風險評估和電子認證的指引。這份指引將有助電子服務供應商和用戶，就電子交易釐定合適的電子認證規定。

與業界合作

17. 政府資訊科技總監辦公室與香港警務處及香港電腦保安事故協調中心合作，在本年 11 月舉辦了「全城電腦清潔日 2006」活動，以提高各界的資訊保安認知，並鼓勵市民採用簡單易用的技巧加強電腦保安，以防網上攻擊。

18. 此外，政府資訊科技總監辦公室會繼續與亞太區電腦保安事故協調組織、事故應變與安全小組論壇，及亞太經合組織電訊及資訊工作小組進行地區性及國際性合作，以增強政府在搜集有關情報、交換資訊、以及處理重大保安事故等方面的能力。

E. 結語

19. 資訊保安管理是一個持續的過程，有賴所有人的關注和承擔。政府會持續加強各局及部門的資訊保安措施，以及透過負責監察各公營機構和規管機構的決策局及部門，向這些機構提供如何加強資訊保安措施的建議。隨着數碼 21 資訊科技策略的方針，我們會繼續宣傳和推動公眾教育，以提高公眾對資訊保安和私隱保護的認識，旨在建立香港成爲一個擁有穩妥電子商貿環境的數碼城市。

F. 徵詢意見

20. 請委員察悉本文報道的內容。

工商及科技局

政府資訊科技總監辦公室

2006 年 11 月

附錄A

政府決策局／部門、公營機構及規管機構的資訊保安狀況調查報告

此附錄就政府決策局／部門、公營機構及規管機構的資訊保安狀況進行調查所得的結果作出報告。

A. 背景

2. 資訊科技及廣播事務委員會(“委員會”)在2006年4月6日的會議席上，要求政府就各局及部門現時的資訊保安狀況，以及各規管機構如何行使監察職能，確保受其規管的行業遵從保安規定，提交一份全面報告。另外，委員會還要求政府，向公營機構搜集有關該等組織爲增強資訊保安而採取的措施的資料。

B. 調查方式

3. 爲搜集擬備上述報告所需的資料，政府進行了兩項調查。有關各局及部門的調查屬周年性的工作，由政府資訊科技總監辦公室於本年7月進行，目的是衡量政府的整體保安狀況。至於另一項調查，則在負責監察公營機構及規管機構的決策局及部門的協調下進行，有關的問卷於本年8月回報。

4. 每個受調查的機構組別，都使用配合其特性的問卷。所有問卷回報均經核實以確保其原整性，而若有需要的情況下，並會附帶補充資料加以澄清。各組別的資料經校對、分析和結集後，便成爲編纂本報告所依的數據。

C. 資訊保安狀況

政府各局及部門

5. 此部份的分析結果是根據 84 個局及部門(全數 84)的問卷回報的資料。調查結果主要包括保安管理及規管、處理機密資料的保護措施、外判資訊科技服務和採用保安技術措施等各方面。主要的分析結果如下。

(i) *保安管理及規管*

6. 政府的中央組織和個別決策局及部門已設立全面資訊保安政策和管理架構。相關的資訊保安規例、政策、程序和指引已經齊備，供各局及部門遵守。資訊保安的規管和控制的權責亦有清楚的界定。

7. 各局及部門中約有 84%已完成資訊保安風險評估和審計，而其餘的亦會在本財政年度內完成有關工作。各局及部門已就其關鍵業務的資訊系統，制訂業務持續運作或運作復原的應變計劃，以應付可能發生的保安事故。

(ii) 限閱／機密資料的處理

8. 大多數的局及部門有處理個人及機密資料，並已推行保安措施，以確保資料保密。這些措施包括數據加密；對應用系統的開發、保養及操作作出適當的接達管理；機密資料及其實體儲存媒體要妥善保管及加上標籤等。

(iii) 資訊科技項目外判安排

9. 各局及部門中約有 80%採用資訊科技外判服務，並已於有關的採購合約制訂多種保安和監察措施。此外，各局及部門逾 90%已在合約中納入必須的資訊保安條款，供合約人員遵守。中央管理的合約已包含有關的條款，確保承辦商及其分判商履行政府資訊保安規定。

(iv) 科技措施

10. 各局及部門已推行修補程式管理措施，以堵塞軟件的保安漏洞。逾 70%的部門並已把修補程序自動化，以確保能盡快安裝修補程式。

(v) 員工的保安認知、教育及培訓

11. 政府資訊科技總監辦公室負責爲政府人員中央統籌保安認知計劃和培訓課程。爲配合各局及部門的個別需要，有 29%已經舉辦爲其員工特別制訂的培訓班及認知課程。

公營機構

12. 此部份的分析結果是根據 104 個公營機構(全數 104)的問卷回報的資料(名冊參考附件 1)。調查結果包括一般資料、保安管理及規管、處理機密資料的保護措施、外判資訊科技服務、採用保安技術措施和員工保安認知與培訓等。

(i) 一般資料

13. 公營機構的概要，包括組織規模、應用資訊科技的程度和資訊保安預算趨勢載於參考列表 1、2、3。

列表 1 -組織規模(按在職上班人數釐定)

45%	小型 (1 至 9 名員工)
20%	中型 (10 至 99 名員工)
35%	大型 (99 名員工以上)

列表 2 -資訊科技應用(辦工室／運作自動化及資訊科技／業務整合)

4%	採用尖端資訊科技應用系統
94%	資訊科技一般應用
2%	剛開始使用

列表 3 -資訊保安預算趨勢

12%	比上個財政年度有所增加
84%	沒有改變
4%	比上個財政年度有所遞減

14. 各機構使用的個人電腦數目，與組織的規模大約成正比。這些個人電腦一般都接駁互聯網，因此有可能成爲網上攻擊的目標。調查中的機構約有一半認爲系統故障，包括發生資訊保安事故，會對其業務運作造成影響，而約 30%則相信系統故障會嚴重影響其內部行政。

(ii) 保安管理

15. 調查詢問各公營機構有否採用任何保安管理措施。所得結果見於列表 4 和 16 及 17 段。

列表 4 -公營機構採納的資訊保安管理措施

管理措施類別	調查結果
政策／管理規管	93%的機構已採取最少一項保安政策／管理規管措施。這些措施包括： - 管理架構(60%) - 政策或指引(59%) - 遵守法例及／或規例規定(78%)
營運保護措施	各機構已推行最少一項營運保護措施。這些措施包括： - 保安修補程式管理(88%) - 抗禦電腦病毒管理(100%)
應變措施	72%的機構已制訂最少一項事故應變措施。這些措施包括： - 事故及應變管理(61%) - 業務持續運作管理(63%)
員工保安認知及培訓	19%的機構提供強制的認知及培訓計劃。
保安風險評估及審計	59%的機構已採取納保安風險評估及審計。

16. 上述結果顯示 40%的機構沒有制訂資訊保安管理架構，而 41%的

機構沒有資訊保安政策或指引。在營運方面，12%的機構沒有推行保安修補程式管理以防禦網上攻擊。

17. 結果亦顯示只有 19%的機構提供強制的資訊保安認知及培訓計劃，反映這方面有嚴重不足之處。另有 41%的機構沒有採納任何風險評估及審計以作保安保證，而 34%的機構在短期內亦沒有此計劃。

(iii) 保安措施履行及實施的規管

18. 調查詢問各公營機構如何確保保安管理措施已徹實履行及實施。所得結果見於列表 5。

列表 5 -公營機構採納的資訊保安規管措施

規管機制類別	調查結果
對遵守規定的測試	67%的機構已透過最少一項措施，對機構有否遵守保安規定進行測試。這些措施包括： - 定期覆檢(65%) - 保安事故／復原演習(37%)
支援及隨機抽查	69%的機構已推行最少一項抽查。這些抽查包括： - 內部審計(50%) - 突擊檢查(16%) - 業務持續運作程序(50%)
指導及鼓勵	93%的機構已採取最少一項指導及鼓勵措施。這些措施包括： - 提示便箋／通告(88%) - 批核撥款準則(31%) - 員工表現評核報告(19%)

(iv) 限閱／機密資料的處理

19. 超過 85%的公營機構有需要處理限閱／機密資料。常見的資料包括姓名、地址、香港身分證號碼及電話號碼。有少數機構還涉及處理信用卡號碼和銀行帳戶號碼。

20. 調查詢問各公營機構有否於處理限閱／機密資料時，有否採用運作措施和技術工具。所得結果見於列表 6 和 21 及 22 段。

列表 6 - 公營機構於處理限閱／機密資料時採用的措施及工具

措施及工具類別	**調查結果**
運作措施	89%的機構已訂立最少一項運作措施。這些措施包括： - 數據定義(73%) - 授權定義(55%) - 批授接達權的程序(73%) - 員工接達的控制程序(63%) - 庫存管理及控制(63%) - 備份／復原／棄置程序(74%)
技術工具	57%的機構採用技術工具，例如資料加密以確保資料得以妥善儲存／傳送／處理。

21. 上述結果顯示在處理限閱／機密資料上，適當的授權定義與接達的控制程序有需要加強。此外，亦發現 26%的機構沒有備份、復原及棄置程序去處理限閱／機密資料。

22. 在防範限閱／機密資料於不慎的情況下泄漏，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。

(v) 資訊科技項目外判安排

23. 約 80%的機構已把各種不同的資訊科技工作外判，例如系統的開發、保養和運作；技術支援；設施管理及服務臺等。調查詢問有關機構有否於工作外判的同時採用保安管理措施。所得結果見於列表 7 和 24 及 25 段。

列表 7 - 公營機構於資訊科技項目外判時採納的保安措施

保安措施類別	調查結果
合約條款	93%有外判資訊科技項目的機構已作出安排，在合約中納入最少一項保安條款。這些條款包括： - 不可向外披露資料協議(80%) - 服務水平協議(69%) - 接達控制程序、更改控制程序、升級處理程序和事故應變規定(75%) - 遵守保安規定的聲明(48%)
質素保證及控制	75%有外判資訊科技項目的機構已推行最少一項質素保證及控制措施。這些措施包括： - 不同測試階段的保安控制(66%) - 質素保證(53%)
保安規管及控制	82%有外判資訊科技項目的機構已制訂最少一項保安規管措施。這些措施包括： - 數據保安控制(61%) - 定期查核對保安規定的遵守(45%) - 界定職務和責任(71%) - 庫存控制(57%)
人事保安審核	12%有外判資訊科技項目的機構曾進行人事保安審核。

24. 上述結果顯示，有多至 34%有外判資訊科技項目的機構沒有在測試階段時採取相應的保安控制。結果亦顯示 47%的機構在外判資訊科技項目的安排上沒有制定任何質素保證，而有 39%的機構沒有爲外判資訊科技項目的數據作保安控制。

25. 在保安規管方面，29%的機構沒有與外判商界定職務和責任，而有超過半數的機構沒有查核外判商對保安規定的遵守。

(vi) 科技措施

26. 調查詢問各機構有否採用資訊保安技術和工具以保護電腦數據及設施。所得結果見於列表 8 和 27 段。

列表 8 - 公營機構採納的技術和工具

技術和工具類別	**調查結果**
基本措施	79%的機構已採用最少一項基本技術措施以保護其電腦數據和設施。這些措施包括： - 用戶帳戶設有密碼(100%) - 防禦電腦病毒工具(100%) - 防禦間諜軟件工具(45%) - 保安修補程式管理工具(82%) - 防火牆(94%)
特殊數據處理措施	74%的機構已採用最少一項特殊數據處理措施。這些措施包括： - 檔案／數據加密(64%) - 穩妥數據移除工具(38%)
較爲先進的認證／接達控制技術	77%的機構已採用最少一項較爲先進的認證／接達控制技術。這些技術包括：

技術和工具類別	調查結果
	- 公開密碼匙基礎建設(32%) - 身份管理(55%) - 雙重或多重認證(25%) - 審計記錄和追蹤工具(69%)
與網絡有關的措施	88%的機構已採用最少一項保護網絡的措施。這些措施包括： - 電郵過濾工具(75%) - 入侵偵察／防範工具(52%) - 穩妥網絡(59%)
資產保護	86%的機構已採取最少一項資產保護措施。這些措施包括： - 實體保安(70%) - 備份復原(85%)

27. 上述結果顯示 18%的機構仍然沒有採用保安修補程式管理工具，這些機構受網絡攻擊的風險會因此提高。結果亦顯示 62%的機構沒有採用穩妥數據移除的工具，45%的機構沒有身份管理，41%的機構所用的網絡並不安全，及 30%的機構沒有實體保安措施以保障電腦資產。

(vii) 員工保安認知、教育和培訓

28. 調查詢問各機構推行員工保安認知和培訓計劃。所得結果見於列表 9 和 29 段。

列表 9 - 公營機構的教育和培訓計劃

教育類別	調查結果
促進資訊保安認知	66%的機構採用最少一項培訓措施以增強員工的資訊保安認知。這些培訓包括： - 內部培訓(39%)

教育類別	調查結果
	- 外間培訓(54%) - 網上學習課程(13%)
鼓勵員工考取資訊保安專業資格	11%的機構鼓勵員工考取資訊保安方面的專業資格。
定期提示便箋	93%的機構定期向員工發出提示便箋，以提醒員工的保安意識。

29. 調查詢問各公營機構其認知計劃和培訓課程所包含的課題。約有7%的機構提供涵蓋各主要課題的全面培訓，包括保安認知、保安管理、事故應變、外判安排、技術運用技巧和保安專業認證等。

規管機構／行業

30. 規管機構共交回 58(全數 58)份問卷(名冊參考附件 2)。而以下的調查結果是根據其中 11 個規管機構轄下 13 個行業的問卷回報。其餘的行業在考慮其情況因沒有資訊保安顧慮或規管機構認爲不需要特別監管轄下組織的資訊保安概況，因此，實際的回覆是沒有資料可提供。

(i) 一般資料

列表 10 -行業組織規模分布(按規管機構監察的組織數目區分)

46%	少於 20 個組織
8%	150 至 199 個組織
23%	200 至 499 個組織
23%	超過 500 個組織

(ii) 規管措施及監察對保安規定的遵守

31. 調查詢問各規管機構在規管和監察轄下組織時，所採用的資訊保安措施。所得結果見於列表 11 和 32 段。

列表 11 -規管機構採納的規管及監察措施

規管及監察措施類別	調查結果
政策／管理	所有回報機構已採取最少一項政策／管理措施向其規管的業內組織進行監察。這些措施包括： - 規則及規例(100%) - 強制資訊保安管理架構(15%)
保安保證	62%的回報機構要求業內組織進行最少一項保安保證措施。這些措施包括： - 定期風險評估及審計(38%) - 報告資訊系統的重大變更(46%)
應變措施	69%的回報機構要求業內組織制訂最少一項應變機制。這些機制包括： - 資訊保安事故應變程序(69%) - 業務持續運作計劃(46%)
員工認知及培訓	54%的回報機構要求業內組織爲員工提供資訊保安培訓。

32. 根據調查結果，有些規管機構還會頒布作業守則，規定業內組織須制訂經核准的資訊保安政策和程序，以保護由其處理的數據。有些規管機構則爲業內組織成立協會，以商討及制訂應付保安事故的措施和指引。

(iii) 保護限閱／機密資料

33. 在 13 個受規管的行業中，92%有處理限閱／機密資料，當中包括

姓名、地址、香港身分證號碼和電話號碼。少數行業還要處理涉及財務、合約、商業交易、法例修訂建議的資料。

34. 調查詢問各規管機構有關業內組織通常用以保護個人資料、限閱／機密資料的保安措施。所得結果見於列表 12 和 35 段。

列表 12 -業內組織採納的保安措施

保安措施類別	調查結果
政策／管理	85%的規管行業已推行最少一項政策／管理措施。這些措施包括： - 管理及規管包括保安政策、規例、標準、指引及良好作業模式(85%) - 保安控制及程序(77%)
技術措施	77%的規管行業已採用保安技術措施，包括數據加密、身份認證、入侵偵測與防範系統、以及追蹤記錄等。
保安保證	54%的規管行業已採取保安風險評估／審計。
應變措施	69%的規管行業已採用最少一項應變措施。這些措施包括： - 保安事故應變管理(62%) - 業務持續運作管理(69%)
員工認知及培訓	69%的規管行業已爲員工舉辦認知及培訓課程。

35. 負責規管這些行業的機構約有 70%滿意有關業內組織所執行的資訊保安措施。並認爲已對有關行業實施足夠和有效的監察。

D. 總結

36. 調查結果顯示三類公共機構的資訊保安狀況。

37. 在政府各局及部門方面，由於中央組織已設立全面的資訊保安政策、管理架構及相關的指引，各局及部門必須確保遵守嚴謹的政府資訊保安規定。

38. 調查發現部份公營機構及規管機構／行業有急切的需要改善其資訊保安狀況。由於大部份公營機構都有處理個人或其他限閱資料，那些機構應當儘快加強其保安管理、規管、技術和程序等措施，以防止資料外泄等保安事故的發生。保持現況可帶出連串的保安問題，詳情載於附件 3。

公營機構名冊

項目	公營機構名稱
1	香港機場管理局
2	建築師註冊管理局
3	石棉行政管理委員會
4	認可人士及註冊結構工程師紀律委員團
5	認可人士註冊事務委員團
6	稅務上訴委員會
7	廣播事務管理局
8	香港中醫藥管理委員會
9	香港中文大學
10	脊醫管理局
11	香港城市大學
12	製衣業訓練局
13	建造業訓練局
14	建造業工人註冊管理局
15	消費者委員會
16	承建商註冊事務委員團
17	香港醫學專科學院院務委員會
18	香港會計師公會理事會
19	人類生殖科技管理局
20	危險品常務委員會
21	香港牙醫管理委員會
22	紀律審裁委員團(土地測量)
23	當值律師服務
24	教育統籌委員會
25	選舉管理委員會
26	僱員再培訓局
27	工程師註冊管理局
28	平等機會委員會
29	地產代理監管局
30	消防 (裝置承辦商) 紀律委員會
31	岩土工程師註冊事務委員會委員團
32	香港演藝學院
33	香港應用科技研究院有限公司

項目	公營機構名稱
34	香港藝術中心
35	香港藝術發展局
36	香港浸會大學
37	香港學術評審局
38	香港吸煙與健康委員會
39	香港數碼港管理有限公司
40	香港存款保障委員會
41	香港考試及評核局
42	香港出口信用保險局
43	香港教育學院
44	香港互聯網註冊管理有限公司
45	香港金融管理局
46	香港按揭證券有限公司
47	香港理工大學
48	香港生產力促進局
49	香港科技園公司
50	香港體育學院
51	香港旅遊發展局
52	香港貿易發展局
53	香港科技大學
54	醫院管理局
55	房屋經理註冊管理局
56	人體器官移植委員會
57	廉政公署
58	投訴警方獨立監察委員會
59	九廣鐵路公司
60	土地測量師註冊委員會
61	香港法律改革委員會
62	法律援助服務局
63	立法會
64	嶺南大學
65	酒牌局
66	強積金管理局
67	香港醫務委員會
68	香港助產士管理局
69	香港地下鐵路公司

項目	公營機構名稱
70	香港護士管理局
71	職業安全健康局
72	法定代表律師辦事處
73	申訴專員公署
74	香港公開大學
75	香港外展訓練學校
76	藥劑業及毒藥管理局
77	規劃師註冊管理局
78	菲臘牙科醫院
79	個人資料私隱專員
80	公務員敍用委員會
81	優質教育基金
82	輻射管理局
83	註冊承建商紀律委員團
84	土地(雜項條文)覆核委員團
85	證券及期貨事務監察委員會
86	保安及護衞業管理委員會
87	社會工作者註冊局
88	中國香港體育協會暨奧林匹克委員會
89	公務員薪俸及服務條件常務委員會
90	首長級薪俸及服務條件常務委員會
91	紀律人員薪俸及服務條件常務委員會
92	司法人員薪俸及服務條件常務委員會
93	結構工程師註冊事務委員團
94	輔助醫療業管理局
95	測量師註冊管理局
96	城市規劃上訴委員會
97	城市規劃委員會
98	交通投訴組
99	信託基金、廟宇及墳場聯合秘書處
100	大學教育資助委員會
101	香港大學
102	市區重建局
103	獸醫管理局
104	職業訓練局

規管機構 / 行業名冊

項目	規管機構名稱	規管行業
1	建築師註冊管理局	建築師註冊
2	石棉行政管理委員會	環保
3	認可人士及註冊結構工程師紀律委員團	建造業
4	認可人士註冊事務委員團	建造業
5	廣播事務管理局	廣播事務
6	香港中醫藥管理委員會	香港中醫藥
7	脊醫管理局	醫療業
8	建造業工人註冊管理局	建造業工人註冊
9	承建商註冊事務委員團	建造業
10	人類生殖科技管理局	人類生殖科技
11	香港牙醫管理委員會	牙醫
12	衞生署	醫療與健康
13	紀律審裁委員團(工廠及工業經營(安全管理)規例)	工業
14	紀律審裁委員團(土地測量)	土地測量
15	紀律委員團(升降機及自動梯(安全))	升降機及自動梯承辦商
16	機電工程署	電力承辦商
17	機電工程署	電力 - 管制計劃協議
18	機電工程署	電力供應商
19	機電工程署	氣體供應商
20	機電工程署	家庭電器產品供應商
21	機電工程署	升降機及自動梯工程
22	地產代理監管局	地產代理
23	消防 (裝置承辦商) 紀律委員會	消防裝置承辦商
24	消防處 - 消防裝置承辦商	消防裝置承辦商
25	岩土工程師註冊事務委員會委員團	建造業
26	香港金融管理局	金融業
27	人體器官移植委員會	人體器官移植
28	土地測量師註冊委員會	土地測量
29	酒牌局	售賣酒精飲料
30	強積金管理局	強積金

項目	規管機構名稱	規管行業
31	香港醫務委員會	醫療業
32	香港助產士管理局	醫療業
33	香港護士管理局	醫療業
34	保險業監理處	保險業
35	政府資訊科技總監辦公室	認可核證機關
36	電訊管理局	電訊
37	藥劑業及毒藥管理局	醫療業
38	輻射管理局	醫療業
39	註冊承建商紀律委員團	建造業
40	證券及期貨事務監察委員會	交易及結算
41	證券及期貨事務監察委員會	證券及期貨
42	證券及期貨事務監察委員會	股票註冊
43	保安及護衞業管理委員會	保安及護衞業
44	社會福利署	幼兒中心督導組
45	社會福利署	藥物倚賴者治療中心牌照事務處
46	社會福利署	安老院牌照事務處
47	社會工作者註冊局	社會工作者註冊
48	結構工程師註冊事務委員團	建造業
49	輔助醫療業管理局	醫療業
50	運輸署	駕駛訓練
51	運輸署	運輸業 - 專營巴士客運公司
52	運輸署	運輸業 - 專營巴士客運公司 (龍運巴士)
53	運輸署	運輸業 - 專營巴士客運公司 (新大嶼山巴士)
54	運輸署	運輸業 - 專營巴士客運公司 (城巴)
55	運輸署	運輸業 - 鐵路 (九廣鐵路公司)
56	運輸署	運輸業 - 鐵路地下鐵路公司)
57	運輸署	運輸業 - 隧道及青馬橋
58	獸醫管理局	獸醫管理

公營機構現況可見的保安問題

要項	現況可見的保安問題
1. 保安管理	
(a) 政策／管理規管	缺乏高級管理層發布的政策及管理指引，有關機構僅可倚靠技術措施保護資訊資產。而最重要的包括人爲因素引發的問題，極易引致網上攻擊及資料外泄的事故。
(b) 營運保護措施	沒有採取足夠的營運保護措施，有關機構的資訊資產無疑地會直接受到襲擊的威脅，令其可靠性和完整性陷於危機。
(c) 應變措施	缺乏業務應變計劃及員工的演習排練，有關機構將不能對所發生的保安事故作出應變及得到儘快復原。在顧客服務及業務運作上亦會帶來不同程度的負面影響。
(d) 員工保安認知及培訓	員工保安認知及培訓是保證員工遵守資訊保安政策及指引的必要途徑。未能爲員工提供適當的培訓會導致有關機構更易受保安威脅。
(e) 保安風險評估及審計	未能及時糾正保安威脅、漏洞及不當行爲，除了增加網上攻擊的可能外，亦在發生事故時，削弱了業務繼續正常運作的能力。
2. 保安規管	
(a) 對遵守規定的測試	除非定期檢討和進行對遵守保安規定的測試，以驗明有沒有需要改善的地方，否則保安措施在推行一段日子後，可能會因業務、應用系統、科技或環境因素的轉變而失效。
(b) 支援及隨機抽查	系統如果缺乏對不能預測或沒有協調的異常情況又或者未能偵測到罔顧保安規定，可能由此引發成災難性的情況。
(c) 指導或鼓勵	需採取措施要不時更新、提醒和鼓勵員工有關資訊保安的事宜，否則員工可能會忽略有關問題或疏於遵守保安規定因而引致保安威脅。在有人手變動或其他轉變的情況下尤其重要。

要項	現況可見的保安問題
3. 限閱／機密資料的處理	
(a) 運作措施	有關機構極有可能因無意之失或受惡意攻擊，而令到該等資料的完整性遭破壞或導致資料泄漏。
(b) 技術工具	沒有採取適當的技術工具以保護資料，該等資料可能在儲存或傳送時，被未獲授權或非法接達，而令到其完整性及機密性遭破壞。
4. 外判資訊科技項目的有關安排	
(a) 合約條款	承辦商如果無責任遵守保安規定，就只會按其隨意、不及格甚至沒有的作業模式來運作。
(b) 質素保證及控制	承辦商的服務質素將難以得到保證，因而導致資訊保安出現漏洞或問題。
(c) 保安監管及控制	未有採取必要的保安控制，由承辦商處理的資訊系統及數據未必能夠得到適當的保障。
(d) 人事保安審核	由未經審核的人員擔任資訊保安要職並處理高度敏感資料，會令有關機構蒙受極大風險。
5. 科技措施	
(a) 基本措施	因防禦措施存有弱點，有關機構很易受到網上直達的攻擊（例如電腦病毒、蠕蟲、入侵、數據外泄等）。
(b) 特殊數據處理措施	該等資料在傳送、儲存及棄置時，將會容易受到攻擊或破壞。
(c) 較先進的認證／接達控制科技	在未能以妥善的認證方式來達到對機密性、完整性、不可否認性所需的要求時，進行對保安要求較高的交易將蒙受相當風險。
(d) 與網絡有關的措施	數據在沒有受到充分保護的網絡上傳送，其完整性及機密性不能得到保證。
(e) 資產保護	電腦資產在缺乏實體保安保護下，任何其他保安措施均沒有意義及無法生效。
6. 員工保安認知、教育及培訓	

要項	現況可見的保安問題
(a) 促進資訊保安認知	員工如果沒有受過資訊保安方面的培訓，他們有更多機會會違反或破壞資訊保安政策及指引而導致有關機構更容易受到保安威脅。
(b) 鼓勵員工考取資訊保安專業資格	員工可能會對有效地推行資訊保安計劃所需的技巧不感興趣或未能即時掌握這些技巧，因而阻礙了機構的計劃推行。
(c) 定期提示便箋	員工可能會誤解、忘記或違反資訊保安規定，這些情況在出現人手變動或其他轉變時尤其重要。

附錄 B

資訊保安推廣及教育計劃

渠道	活動內容	日期
網上資源	● 在「資訊安全網」網站 (www.infosec.gov.hk) 設立專題網頁推廣「全城電腦清潔日 2006」活動	2006 年 9 月
	● 在網站登載有關國際資訊保安標準及專業認證的參考資料	2006 年 12 月
研討會	● 與香港警務處和香港電腦保安事故協調中心爲市民合辦免費的保安研討會	2006 年 11 月
	● 與香港電腦保安事故協調中心和專業協會合辦公眾會議，以推廣國際資訊保安標準和專業認證	2007 年 3 月
電台節目	● 播放介紹如何保護個人私隱和適當使用保安保護軟件的電台節目	2006 年 7 月 – 2007 年 3 月
電視特輯	● 在《警訊》節目中播放特輯，專題介紹如何保護無線網絡、流動裝置和個人私隱	2006 年 11 月
刊物	● 透過不同渠道例如圖書館、社區會堂、學校、制服團體等，向市民派發強調保護個人電腦的重要和介紹相關措施的小冊子	2006 年 10 月
嘉年華會	● 舉辦「全城電腦清潔日 2006」嘉年華會	2006 年 11 月 25 日