

資訊科技服務外判保安

2008 年 2 月

©香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

免責聲明：政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

目錄

摘要.....	2
I. 介紹.....	3
II. 資訊科技服務外判之管理.....	4
資訊科技服務外判的風險.....	4
資訊科技服務外判的管理.....	4
持續監控.....	5
其它最佳作業實務.....	6
III. 結論.....	7

摘要

當機構外判部份資訊科技服務的時候，外判供應商便可能成為公司裡另一個”內部人員”，處理公司內敏感而且重要的資料。雖然由外判供應商提供服務可能為公司帶來利益和成本效益，但在外判資訊科技服務時，機構必須有適當的安全管理程序來保護敏感的資料和客戶的私隱。數據擁有者必須監管和覆檢外判商的所有接達權限，以確保重要資料的安全。底線是：一個機構可以外判它的運作，但是不能外判它的責任。

I. 介紹

在有限資源下，很多公司同時面對客人在服務質素上不斷的要求，以及市場劇烈的競爭。服務外判便成為許多機構重要決策之一。資訊科技服務外判（I.T. Outsourcing）是將原本由內部員工負責的資訊服務或功能交給其他公司負責。本文會討論當機構將資訊系統外判給其他服務供應商時會產生的一些風險。

驅使一個機構考慮外判有兩個動力，一是可獲得外判商裡的專家所提供的更有效率、更有效能的服務，其服務質素甚至可能會比之前自己機構內所提供的更好。另一個動力是外判帶來的成本效益。外判非核心的功能和程序，可以使機構更能專注於核心的營運活動。

資訊科技服務外判可以涵蓋各種不同服務的範圍，包括應用程式的開發和維修、網絡管理、桌上電腦管理、資訊科技服務支援熱線（helpdesk）及電腦中心的管理。資訊科技服務外判也有不同的形式，例如以項目為主，或是以某一個部門為基礎的外判¹。

近年來，世界各地都有關於洩漏敏感或個人資料的事故發生，對一個機構來說，這些事故將會造成重大的經濟損失和聲譽的損害。一個機構除了了解資訊科技服務外判所帶來有形及無形的效益外，也需要注意外判供應商的資訊保安程序，以確保敏感和個人資料的安全²。

¹ http://www.info.gov.hk/digital21/eng/sme/sme_intro.html

² http://www.lawyersweekly.com.au/articles/Outsourcing-the-poisoned-chalice_z69057.htm

II. 資訊科技服務外判之管理

資訊科技服務外判的風險

當一個第三方服務供應商為某機構開始提供外判服務時，它便可能會獲得機構裡的內部資料，進而對機構構成一定的風險：

1. 供應商得到機構內的人事資料、基礎設備、程序、批核渠道，甚至系統內（包括資訊科技及非資訊科技系統）既存的弱點和缺陷；
2. 為了提供服務，供應商可能會接觸到相關的資料和系統，並因此獲得敏感或機密的資訊，甚至其他個人資料。
3. 供應商可能會獲得有效的用戶賬戶和密碼，用以操作某些高度敏感的系統。

對入侵者或有犯罪意圖者來說，這些內部運作的資料是很有用的，甚至可用於惡意的社會工程中。科技發展的日新月異，如電子郵件、互聯網、移動儲存設備（如：小型USB快閃磁碟機）等技術的普及，加上可以利用遠程接達來連接機構內的資訊系統，由內部員工所造成的濫用系統事故以至資料盜竊（包括知識產權的盜用）等風險是不能低估的。如果沒有及時終止離職員工的系統賬戶和接達權限，便會產生保安上的漏洞。在最壞的情況下，如果系統不能夠識別個別用戶及提供適當的記錄，詐騙、數據保安的問題和違反私隱的事故都可能在沒有留下任何痕跡的情形下發生。

資訊科技服務外判的管理

如向一個或多個第三方服務供應商外判資訊系統，必須制定適當的保安全管理程序以保護數據，同時降低相關外判資訊科技項目／服務的保安風險。以下列出應該考慮的幾個方向：

1. 在擬定外判服務合約時，機構應在合約中訂明將會外判的資訊系統保安要求（例如：如何處理所有私人和敏感的資料）。這些要求應為招標程序的基準及系統效能測量的一部份。
2. 外判合約應規定第三方服務供應商及銷售商的所有工作人員簽署不可向外披露資料協議，以保護系統中的敏感數據。合約亦須包括一系列服務水平協議（SLAs）。服務水平協議用於界定所要求的各項保安控制的預期水平，描述可量度的成效，以及就任何經確認的違約行為訂明補救及應變措施。除訂立服務水平協議外，合約應包含一套解決問題及事故應變的通報處理程序，以便處理事故，盡量減低事故對機構造成的影響。

3. 在聘請提供資訊科技服務的供應商時，機構應確保他們遵守機構的相關保安政策、適用的政府規例（例如銀行機構須遵守香港金融管理局的規定）及其它業界最佳作業實務。服務供應商必須如同機構內部人員一樣，遵守相同的資訊保安規定及承擔相同的資訊保安責任。
4. 機構應積極及定期監控和覆檢服務供應商及用戶的保安控制遵行情況，並保留審計服務水平協議所界定責任的權利、安排獨立第三方進行審計。
5. 機構應確保服務供應商有適當的資訊系統應變計劃及備份程序。
6. 機構應清晰界定和載述與外判資訊系統有關的第三方服務供應商、內部員工及終端用戶的保安職務和職責。
7. 機構應確保所有被第三方服務供應商處理的資料，都有明確和適當的機密級別分類。接達權限應以工作上的需求，或以合約上的服務需要來分配。
8. 雖然資訊系統能被外判，但是機構仍須承擔所有違反敏感或個人資料的法律責任。

持續監控

商業環境是不斷變化的，科技亦然。資訊保安的技術，以及保安職務和職責，可能都會隨著時間而改變。機構應要對保安運作和接達控制作出定期的檢討。在外判合約開始前，服務供應商可能會忽略了某些外判運作上的一些細節，定期覆檢可提供一個渠道讓雙方互相評估服務，並作出必要的調整。

保持安全性的最佳做法，包括自動更新電腦病毒識別碼、定期檢測和更新偵測及修復引擎、定期覆檢並在操作系統及應用系統安裝最新的保安修補程式或修復程式，並且在任何時候都要實行嚴格的密碼政策。在某些情況，機構需要將一些特殊權限帳戶（如Windows伺服器的administrator管理員帳戶或Unix系統的root帳戶）授予服務供應商。機構應對這些特殊權限帳戶的活動進行監察、記錄及定期作出檢討，並與更改要求作出比較。當一個服務供應商的員工辭職或離開後，所有分配予該員工的帳戶和接達權限必須盡早予以撤銷或收回。

為了確保有效及全面地進行檢討，機構須保存：

1. 一份載有服務所需伺服器及系統的清單，以及那些系統會儲存敏感或個人資料。
2. 一份服務供應商支援人員的名單，包括授予的用戶帳戶和接達權限。
3. 一份已交給服務供應商的資料（尤其是敏感或個人資料）之清單。

這些資料應保持準確，並不斷更新。不準確或不完整的清單，可能是外判服務管理上發生問題的徵兆之一。故應該定期進行審核，以確保合約上的安全控制機制得到完善的執行。

其它最佳作業實務

一個機構可以將其資訊系統和流程外判給服務供應商，但是沒有機構可以外判自己的責任，尤其是與其客戶間的法律責任。在外判時，企業主管、資料的擁有者和終端用戶都必須確保資訊安全。

資訊科技從業員

如果外判服務會涉及寄存資訊系統在第三方的數據中心時，機構必須先對寄存公司進行現場環境之保安評估，然後才可作出是否採用其外判服務的最後決定。

同樣地，如果客戶資料或其它敏感資料會被傳送至一個由服務供應商所擁有的伺服器時，就必須在資料傳輸到該伺服器之前，為其場地的實體和邏輯保安控制進行風險評估。服務供應商應為機構設立一個獨立的環境，用以分隔機構與其他客戶的資料。必須確保用來傳輸資料的通訊路徑之安全；敏感的資料也應該使用嚴格的加密算法。當伺服器設在另一個國家，應加以考量評估因不同的司法制度所造成的影響。

因為服務供應商的工作人員在執行外判服務時，可能會接達機構的內部資料，資料擁有者必須知道資料儲存在什麼地方，有哪些人可以接達等。在批准任何工作人員對資料的接達權之前，必須充分了解為何需要接達，以及所要的最小權限是什麼，並應定期進行賬戶及接達權限的審查，以確保沒有授予過大的接達權限。也應對審計追蹤作出定期查核檢討，以確保沒有任何可疑的活動（如突然增加的文件下載量），因為這可能是反映違反保安的徵兆。

此外，亦應定期以最新的電腦病毒識別碼及其偵測及修復引擎，為服務供應商員工所連接到機構網絡的電腦進行全系統的病毒掃描。

終端用戶

終端用戶在使用伺服器、電腦終端機、工作站或微型電腦時，應啟動系統內的自動保護功能（例如有密碼保護的屏幕保護程序、鍵盤鎖……等），以防止其他人非法地使用系統。另一替代方案可在登錄和連接超過預定時間後便終止其連線。在結束每天的工作前或長時間不操作的情況下，用戶應關閉工作站。

III. 結論

執行和監控一個大型的外判項目是一件不容易的事情。任何對資訊科技管理的不足都可對企業營運帶來重大的影響。在享受資訊科技服務外判所帶來的成本效益或其它方面的利益之餘，管理人員更應謹記，任何機構只能外判其服務，但不能外判其責任。保安影響的分析和風險評估應在起草合約時就開始，並將服務供應商和機構的資訊科技環境等因素都納入考慮範圍。持續的監測和定期的覆檢也必須遵行，以確保能妥善而全面地管理資訊科技外判項目及服務。