

辦公室數據保安的挑戰

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. 背景.....	3
個人化的數據傳輸裝置.....	3
辦公室的環境變化.....	3
II. 影響數據保安的因素.....	5
可能的威脅.....	5
資訊保安的趨勢.....	6
III. 數據保護的計劃.....	7
意識與責任.....	7
定時評估與政策.....	7
數據的分類.....	7
IV. 數據保護的技術.....	8
接達的限制.....	8
流動裝置的保護.....	8
網絡的防護.....	8
公用渠道的保安措施.....	8
適當的程序.....	9
V. 結論.....	10

摘要

現在的日常生活中，任何人都可藉流行的工具與技術，如流動電話、電子郵件、即時通訊服務、可攜式的儲存器，以及經無線網絡接達互聯網的能力，輕易地攜帶及處理大量數據。隨著攜帶數據的便利，許多機構已基於公開標準與相容界面的流行設備，建構了提供產品和服務的資訊系統。此外，機構還促使內部員工和大眾無論在家中或辦公室，都可使用互聯網接達相關數據。但這種方便卻大增了公司敏感數據被洩漏的機會。

I. 背景

個人化的數據傳輸裝置

透過使用可移動的儲存媒體及實體的儲存器，如磁帶與磁碟，去傳輸電腦數據是最傳統的方法。最新的產品則是體積極小的flash drive儲存器。它擁有數十億字節（gigabytes）的數據容量，可以儲存超過數以百萬頁的文字或成千上萬的圖片。而這些產品的數據傳輸速度也相應地提高，且可透過通用串列匯流排（USB）的界面在短短的幾秒鐘就能夠複製數十到數千頁A4頁面大小的文件。

外部的儲存器分為許多種類，而它們大多數透過普遍使用的USB界面與桌上型電腦連接。外部儲存器的例子有thumb drive儲存器、外接式硬碟、MP3播放機、流動電話，及快閃記憶卡閱讀器等，部份的裝置甚至能夠支援無線網絡的應用。

最新型的流動電話就像一部迷你電腦，結合了桌上電腦的功能；包含多媒體的液晶螢幕、隨機接達記憶體（RAM）、唯讀記憶體（ROM）、可移動的儲存媒體，與多國語言文字的輸入等。這些裝置也可用來攝影相片及攝錄影片。除了作一般電話功能外，較新的機種還能夠透過Wi-Fi（802.11 b/g）之類的無線網絡來接達互聯網作通訊之用，且也可使用藍芽傳輸技術在短距離內與其它配置或電腦相連接。最新的3G流動通訊規定也促使流動電話能夠用作瀏覽網頁及收發電子郵件等用途。

這些科技的發展，使一般人也能使用價格較低廉的設備與服務來複製、儲存、及處理大量數據。

辦公室的環境變化

以往，大多數公司的數據系統都是利用一個昂貴的中央主機電腦來處理，或利用迷你電腦來處理。這些用作儲存數據的電腦，使用彼此不相容且專屬的網絡協定標準。因為當時須用來轉譯或解碼數據的設備和知識不易得到，所以要與其它系統互相連接實在困難，使彼此的接達、轉譯與較無關連的部門互換資料（即使是在同一個機構內）變得幾乎不可能。

推行系統的費用、機構/部門間更容易連接的趨勢、和互聯網的興起已經提高了數據系統的開放標準應用。現在，很多應用程式都是由價格便宜或是免費下載的工具來開發的。愈來愈多的資訊科技基礎建設都建立在開放式標準上，這些開放式的標準能使不同硬件的平台與不同的產品間互相連結運作¹。

¹ http://www.thocp.net/reference/stones_and_pebbles/numbers.htm

這意味著如電子郵件系統、作業系統，以及網路的路由器等被廣泛應用的應用程式和技術細節，都能讓機構外的人作更深入的研究。表示有更多人擁有接達公司資訊的必要技術，而且在一些極端的情況下，也能揭露系統的弱點。

普羅大眾所使用的及採用相同作業系統和界面操作的個人電腦，已取代了大型主機系統的終端機。被用來接達重要商業應用程式數據的桌上電腦，現已可同時透過互聯網來傳送電子郵件和瀏覽互聯網。數據也可以透過通用串列匯流排(USB)埠快速地儲存到flash drive儲存器上。關鍵的機構資料可以儲存到個人設備中，或利用公共訊息服務處理，還有很多其它不當的方式可能使資料洩漏到公眾的領域。

II. 影響數據保安的因素

可能的威脅

數據的保護曾經依賴實體性的防禦或完全隔離原始數據的策略，也就是限制接達在大型主機系統、磁帶或磁碟上儲存的數據位元與字節。時至今日，這種策略已不足夠應付保護數據的要求，因限制接達這種靜態的防禦方法並不適合使用於現代的商業實務上。因為公用客戶端（電腦及流動裝置）能使用相容的界面標準與公司的服務溝通，所以只要有渠道和機會的存在，任何人都可接達與轉譯從任何來源的數據。在現代的辦公室中，有許多方法能做到這件事，而最主要的兩種既有弱點的方法是：（1）實體的儲存，與（2）數據網絡。

1. 實體的儲存

流動裝置的體積纖小且方便攜帶。但它們也非常容易被遺失。若恰好被人撿到，資訊外洩就有可能發生。流動電話內的應用程式亦儲存了敏感的商業機密如聯絡人與行事曆資料。丟棄已舊配備的機主可能會忘記移除儲存在其中的敏感數據內容，而讓有犯罪意圖者有機可成。

流動裝置同時也有可能是一個帶有惡性程式碼（如病毒與特洛伊木馬）的媒體；若將其接達至正在連接到機構網絡的使用者電腦上，就可能造成一些意料之外的保安事故。

具備內建攝影功能的流動電話也有潛在的風險，因為它們可以用來記錄印有資訊的文件，或者用作監視裝置的影像攝錄器。

2. 數據網絡

現時，互聯網是許多商業與機構的主要通訊渠道，同時也很容易就成為一個重大的數據保安威脅。若不適當加以保護，機構的伺服器就很可能會成為外來惡意攻擊的受害者，導致如遺失顧客資訊、損毀公司網站或者損壞網上交易等重大損失。

惡性程式碼，如病毒與特洛伊木馬，都是使用非直接的方式來攻擊系統。它們通常藏在可下載的檔案或者電子郵件的附件檔中而經由互聯網散佈。

現今，有許多辦公室的工作環境已經使用無線網絡，但假如沒有適當地設定對數據加密的啟動，無線網絡便成為一個資料外洩的潛在保安漏洞。

現時的流動電話已可以接達互聯網，卻經常欠缺一些保安上的防護。儘管公司的伺服器與網絡通常會有可監視與記錄網絡活動的設備，卻往往無法監視個人流動通訊的活動。

資訊保安的趨勢

在2007年，InformationWeek委託一家顧問公司，Accenture，進行一項全球資訊保安調查名為「Global Information Security survey」。共有3092位（1101位是來自美國與1991位是來自中國）²在商業技術與保安上的專業人員接受面談。其中一項結果便是參與調查公司最關心的保安威脅之排名清單。如電腦病毒般的傳統惡性程式碼威脅，仍然排行在清單的頂端。然而，下述三項關於數據遺失的陳述則是列在清單上較低的位置；

1. 「未經授權的雇員接達檔案與數據」（*unauthorised employee access to files and data*）此點被美國的受訪者排行至第四，而中國的受訪者則把此點排行至第三；
2. 「顧客數據被外人所竊取」（*customer-data theft by outsiders*）此點被美國的受訪者排行至第五，而中國的受訪者則把此點排行至第六；
3. 「儲存在流動裝置內的公司數據遺失或遭竊取」（*loss or theft of mobile devices containing corporate data*）此點被美國的受訪者排行至第七，而中國的受訪者則把此點排行至第九。

不管有關數據遺失事故的新聞出現有多頻密，這些排名顯示遺失數據對許多公司在資訊保安方面，仍然不是最關心的威脅。

² <http://www.informationweek.com/shared/printableArticle.jhtml?articleID=201001203>

III. 數據保護的計劃

意識與責任

對任何一個機構³來說，數據都是最重要的資產之一，且雇員往往是保安鏈中較弱的一環⁴。所以，透過教育與定期的提示，使內部工作人員充分意識他們的共同責任，是相當重要的。故資訊保安的重要性是不容忘卻與忽視的。每個雇員都必需充分意識自己的責任、他們在資訊接達的限制、及任何可能造成保安事故的紀律處分。這些都可被視為數據保安上自我改善的驅動力。

定時評估與政策

一個成功的項目通常有一個好的計劃。在做任何改變之前，評估建設在公司內各處的資訊系統，以及確認其必須改善的地方，是一個很好的概念。建立一個保安政策去管理隨之而來的指引與程序的發展是必須的。定期執行持續的評估也是很重要的，這使既有的程序能因應工作條件與新的技術作出更新與改善。

數據的分類

並非所有的數據都屬於相同等級的重要性或敏感性。舉例說，如促銷用的廣告小冊子就不必受到像薪金帳冊數據那種等級的保護。為了善用資源，應該以公司數據的保安等級來作優先次序，把保安上所用的資源先集中在最重要的數據上。

評估所有公司數據的固定與臨時的儲存位置，以及依照數據保護的強度來對其加以分類也相當重要。舉例說，thumb drive儲存器是較不安全的儲存裝置而又最適用於較不重要的數據儲存，而對儲存在眾多系統並需要認證方可接達備份伺服器的資料庫而言，其可靠的數據保護便適用於這種較重要的資料庫。

³ <http://whitepapers.zdnet.co.uk/0,1000000651,260084021p,00.htm>

⁴ http://www.schneier.com/blog/archives/2007/03/social_engineer_3.html

IV. 數據保護的技術

接達的限制

軟件以及機密數據的接達應該是僅能給予經過授權的員工。用密碼或權標這類型的認證方式來保護接達是屬於較常見的技術，且可根據使用者的角色，把不同的授權配置檔應用於不同使用者上。審計追蹤是認證的另一個補充辦法，且全面的活動記錄也能夠提供有用的資訊去改善保安措施的效率。數據加密對未經授權的數據接達提供了另一層次的保護。

流動裝置的保護

流動資訊處理裝置與儲存在其中的數據，不論是遭盜竊或者是在沒有人看管的情況下，都會很容易被遺失。實體的防護方法，如用防盜安全鎖，就是最常見的第一道防線。還有額外的授權要求如密碼，也可以防衛未經授權的接達。使用者應自行判斷在這些裝置上儲存機密資料的風險以及必要性，且不管如何都要定期進行數據備份。

網絡的防護

防止從互聯網的入侵或攻擊是一個很大的課題。如防火牆以及代理伺服器這些產品都已經可提供某一程度的數據與系統保護。但每家公司的數據系統都有不同的架構，通常都必須受到評估，並設計出針對該公司營運所需的保護措施。

惡性程式碼是透過網絡作另一種非直接的攻擊方式，目前已有些先進的工具能夠防衛這種問題。要維持這種防護的有效性，便應定期掃描硬碟與可攜式的儲存器，以及即時更新修補程式、病毒識別碼特徵檔（virus signature pattern files）和惡性程式碼定義。

公用渠道的保安措施

公用通訊的渠道，如即時通訊（IM）、無線網絡的接達以及公共網上電子郵件服務等，都有可能帶有公司的資訊。在辦公環境中使用這些公用渠道的控制措施，有時候是必要的：

1. 發展一套清晰的通訊使用政策，且發布這些訊息給所有員工知道；
2. 考慮推行一個相當於企業的統一解決方案，而非使用公用通訊服務；
3. 在適當的地方實施保安防護系統；
4. 將一些不安全的服務停止，如遠端啟動的錄影機。

適當的程序

當丟棄已舊的電腦配備或內存非揮發性數據的儲存媒體，便需要一個適當的程序去保證所有的資訊和數據都已經被清除，如對儲存媒體作實體破壞、覆寫資料，或是重新格式化。

在某些情況下，防止員工攜帶個人物品（包括流動電話在內）進入工作範圍，也許是值得建議的，這有助於排除一些數據被竊取的機會。

V. 結論

現代辦公室環境中所使用的資訊科技系統，大多已經轉移到具有開放式標準的平台和系統上。如今，也有許多可讓外人接達企業數據的渠道。實體上將原始數據加以單獨隔離的傳統技術再不能夠確保數據的安全。機構必須規劃與審視其政策與程序，以保護他們的數據。通常，採用許多不同的措施是必須的，這包括員工的教育訓練、接達的限制、登入的審計記錄、數據的加密與網絡的保護等。