

PUBLISHED ON 21 MAY IN SING TAO DAILY IT SQUARE

「星島日報 IT Square」特稿
二零零八年五月十三日

積極面對數據保安問題

香港電腦學會副會長
吳傑莊博士

電腦數據保安問題由來已久，近月來在香港社會更不斷升溫。這邊廂，接二連三的 USB 手指遺失事件，對個人私隱構成了極大挑戰；加上互聯網的非法共享，使機密資訊轉瞬間蔓延四散。那邊廂，連整部電腦伺服器都可遺失，客戶資料付諸一旦，甚至有機會外洩，怎不駭人聽聞？

在社會各界的紛紛議論下，電腦數據資料的安全性備受質疑，甚至連電腦及便攜式儲存裝置的應用價值也受到衝擊。更有人提出禁止員工把 USB 手指帶離公司範圍。此舉是否「因噎廢食」實屬見仁見智，但毋庸置疑的是，本來為人類生活創優增值的先進電腦設備，一夜之間頓變「洪水猛獸」。

歸根究底，電腦設備始終是予人便利的。它們能否發揮應用價值，抑或帶來不必要的負累，完全視乎它們是否用得其所。且看現時引起軒然大波的電腦保安問題，我們與其斬「手指」避沙蟲，倒不如以更積極的態度去面對。

加密技術日新月異

電腦世界瞬息萬變，數據保安技術也不斷推陳出新。當中不乏針對因電腦硬件丟失而洩漏數據的技術。最有效的方法，莫如替便攜式儲存裝置內的數據加密，即使遺失、被盜或落入不法人士手上，也得物無所用。數據加密功能亦與時並進，當傳統的文字/數字組合密碼繼續大行其道，以圖案序列為基礎的密碼也開始普及，讓用戶擁有更多元化的加密技術可以選擇，不法之徒要加以破解就難上加難。

與此同時，生物測定學 (Biometrics) 在數據加密方面也日漸派上用場。近年為人津津樂道的指紋密碼即為一例。人類指紋是與生俱來的，據說每人的指紋都獨一無二，要仿製或偽造十分困難。利用它來識別用戶身分就最適合不過了。

加密技術雖能防止遺失了的電腦設備被攻破，但卻不能尋回因丟失電腦設備而人間蒸發的數據。因此，企業必須定期替重要數據進行備份，萬一資料有失，也可以還原後備數據一解燃眉，確保業務運作無間。對於講求 24 x 7 全天候運作的企業而言，數據備份攸關重要。

內部監察不可或缺

數據流失的原因多不勝數，除了硬件丟失以及黑客和病毒入侵等外來因素，企業內部的數據盜案亦屢見不鮮。日防夜防家賊難防，企業內部的數據竅匪往往更難防避。因為他們對企業營運瞭若指掌，有些更深諳企業電腦系統的深層架構，知道在何時何地「下手」最神不知鬼不覺。有些大老闆甚至連數據外洩了也蒙在鼓裡，直至痛失訂單、商譽受損或發生其他大災難時才恍然大悟。

與其惶惶不可終日，企業總可主動出擊。例如在公司內的重要位置裝設攝錄機及監察網絡，追蹤內部所有可疑活動。但最重要是把錄像妥為保存，否則在關鍵時刻無法檢索及還原錄像也是徒然。

另外，企業可引入嶄新的人面識別技術。每當使用者嘗試登入電腦系統，旁邊的鏡頭都會自動探測並識別其身份，經認證才可登入系統。如被拒絕，鏡頭更會錄下被拒者的面部照片，然後儲存備案，以便事後追蹤。這麼一來，不法人士自然無所遁形。

喚醒大眾安全意識

技術以外，用戶的教育同樣重要。企業固然要制定政策，教導員工如何善用電腦設施；甚至釐定數據使用規例，限定誰人在哪時候可以在什麼情況下使用何種數據。政府在這方面也可發揮作用，例如向市民大眾灌輸有關數據保安的正確知識，提倡以積極態度面對數據安全問題及防患於未然。

群策群力是解決問題的最佳方法。只要我們在數據加密及備份，以至內部察監和用戶教育方面多管齊下，數據保安問題自然逐步迎刃而解。

-- 完 --