斯諾登事件引發**資訊保安**的關注

英國《衛報》和美國《華盛頓郵報》於 2013 年 6 月 9 日，披露了在香港訪問美國中央情報局前僱員和國防承包商博思艾倫諮詢公司的斯諾登（Edward Snowden）的詳情。斯諾登揭露美國國家安全局從 2007 年起，以國家安全和反恐為理由，部署「稜鏡計劃（PRISM）」監控電子郵件、視頻語音交談、視頻、照片、VoIP 通話、文件傳輸和社交網上的詳細資訊。這段報道震驚全世界，各國領袖都為之嘩然，影響深遠。其影響包括計劃的合法性、美國與各國的政治關係、資訊保安、侵犯個人隱私等。斯諾登於 6 月 23 日離開香港後，至今仍滯留在莫斯科，引發了中、港、美、俄和拉丁美洲的外交風波和角力，局勢未明，斯諾登的最終去向，留待讀者自己關注。

從斯諾登事件和他所提供的資料可見，電腦數據可透過互聯網竊取。儘管各國政府包括香港特區政府及有關機構，堅持香港的電腦系統是安全的，沒有被入侵的紀錄。但從資訊科技角度去分析，電腦系統被入侵是極有可能的。

香港人是善忘的，過往發生的電腦事故，仍然歷歷在目。例如：千年蟲、電腦病毒、黑屏事件、情書電郵等。又例如，股災每十年八年發生一次，樓市泡沫也又重臨，但無論怎樣勸籲，都會有人忠言逆耳。

再說到電腦的連接，在未有互聯網之前是利用專用網絡或撥號連線。個人電腦自上世紀 70 年代興起以來，是透過通訊端口（Comm Port）與其他電腦和週邊裝置連接，例如：打印機、滑鼠等，交換訊息，這些都是硬件端口，要直接插入電腦才能存取訊息，只要電腦存放在安全的環境裡，數據便是安全的。

竊取方法剖析

在現時的互聯網環境下，有兩大方法去竊取電腦資料：（一）植入惡意程式如特洛伊木馬（Trojan Horse），（二）利用互聯網和透過 TCP 端口 / 服務。

惡意程式與電腦病毒（Virus）最大的分別，是特洛伊木馬通常不會自我複製，而特洛伊木馬程式是一種遠端管理工具，但可用來窺探和竊取電腦中的機密。

入侵方式：為了能夠順利入侵電腦，首先必須把一小程式植入電腦，再透過這個程式進行資料竊取。這個小程式是透過電郵或下載檔案時，同時被植入。後果：植了木馬並不會因此而馬上當機，木馬在電腦中潛伏，蒐集任何有價值的資料，例如：信用卡號碼、身分證號碼、銀行帳號等。

第二種方法是透過 TCP 端口 / 服務，直接連到你的電腦上，查看檔案目錄，然後將有用的檔案拷貝出來，這兩種入侵都不動聲色，很難追查。

個人電腦的隱患

首先要了解現今個人電腦的漏洞何在，才能徹底堵塞這些隱患。

互聯網（Internet）和萬維網（Worldwide Web）自 1990 年興起和盛行，電腦從單一運作而成為網絡式連接。採用了傳輸控制協定 Transmission Control Protocol（TCP）和透過 65,536 個 TCP 端口，上了互聯網，便可與其他電腦連接，遙控遠方電腦，不動聲色「隔空取物」，存取資料，完全不留痕跡。當其中一台終端機有漏洞而受襲，有可能影響整個網絡上所有的終端機。當然，若駭客惡意破壞，事主發現電腦受損，追尋原因，才知到曾被入侵。

微軟的視窗操作系統是上世紀 80 年代的產品，單一的個人電腦的設計是以方便為主，是將機內的 TCP 端口全部開通，這樣非常方便，令訊息暢通無阻，這些方便也給日後帶來隱患。就好像將家裡的門窗全部打開，自由出入，與此同時，盜賊也有機可乘。這種格局一直相安無事，直至 1990 年互聯網普及時，用

戶除了方便自己，對駭客也大開方便之門，讓駭客透過 TCP 端口，進入電腦，為所欲為。若關掉所有端口或門窗，正常的網上服務都不能運行。

資訊保安可從多方面加強，大部分的使用者對電腦的認知不透徹，往往貪圖方便而忽略安全。首先是電腦系統本身，個人電腦的漏洞是結構性問題，為方便用戶，透過簡單程序便可隨意更改系統的設定，即使有密碼保護，都很容易破解，可防君子，卻阻不了駭客。我們上互聯網，是以 TCP / IP 的協定，透過 65,536 個連接埠（Port）將資料傳送，比喻為家裡的門窗，作業系統有 65,536 套門窗，全部打開，自由出入，方便傳送資料，方便自已之餘同時方便了駭客，成為資訊保安的隱患。

裝了防火牆是否萬無一失？

有些用戶誤以為裝了防火牆，就可安寢無憂。防火牆有兩大功能，除了有指定功能的連接埠，例如：80（瀏覽網頁）、110（電郵）等打開外，將其餘的連接埠關閉。另一功能是封包過濾，監察及限制透過連接埠的數據封包。聰明的駭客可利用開通了的連接埠，透過必須的正常服務，並利用 Outlook 及 IE 的漏洞，導入程式，依 Outlook 的地址簿，向親朋好友發放有毒郵件，又向瀏覽器作出攻擊或盜取資料，防火牆形同虛設，竊取資料和將電腦病毒擴散。

Linux 擁有大型電腦系統的保安架構，很多銀行和政府都採用，比微軟安全得多，內置防火牆將不必要的連接埠關閉，若要開某些服務時，例如：採用 SSL 加密服務時，連接埠 995 會因應打開，關閉服務時，連接埠也相應關閉，方便又安全。Linux 只容許 Root 才能安裝軟件及更改設定的權限，即使 Linux 系統被攻破或感染電腦病毒，只要將病毒刪除，重新開機，就不會將病毒擴散。

方便與保安的平衡

所有系統都沒有絕對的安全！在決定電腦系統時應要作出適當的取捨，究竟取其方便或

安全呢？兩者要取得適當的平衡，若貪圖方便，可能面對嚴峻的資訊保安風險及重大損失。很多國家的政府和企業都擔心微軟的封閉式系統及在保安上的結構未有全部公開，斯諾登也透露，微軟將漏洞的詳情先通知美國國家安全局，讓該局有時間在未修補漏洞前入侵他人電腦系統。

電腦用戶如何自保？求人不如求己！1991 年開放源嗎軟件誕生以來，有超過百萬位電腦專家參與修改，每兩星期更新一次，質量和安全性遠優勝於任何一間軟件公司，二十多年來，開發了 Linux 和成千上萬的優質應用軟件，是集體智慧的成果，讓大家免費下載和使用，讀者可瀏覽 www.sourceforge.net和下載。在 Linux 和開放源碼的環境，網絡和資訊更安全，中小企和家庭用戶可自學和裝備自己。

Android 是採用 Linux 內核，近年被手機廠垂青，設計出近百款智能手機，功能多、款式多，價錢比 iPhone 和 iPad 便宜，並大行其道，銷量超越蘋果和微軟。各廠家再接再勵，陸續推出幾十款全新 Android 平板電腦，港幣兩三千元，媲美 iPad，易用、方便、安全，是精明用家之福。

簡錦源
香港Linux商會主席