資通安全宣導資料

紐約時報專欄作家 Firedman 在其著作「世界是平的」中，描述了一個預料之外的科技與社會變動，強調網路拉平了世界，也打破疆界藩籬，並提示我們，資訊時代網路使人們無所遁形。隨著現代武器系統的數位化與網路化，我們除了必須面對實體的敵人，也必須面對網路平台上無遠弗屆的敵人，所以，做好資訊安全的工作就是做好戰場經營，這是身為科技時代的我們須有的認知與覺悟。

既然「資訊安全」已成為重要的議題，那麼足以威脅資訊安全的因素有哪些呢？

1. 天然災害：占所有威脅因素的 17%至 19%，舉凡水災、火災、風災、地震、雷擊等均屬之，它可能會對電腦系統造成一定程度的影響或損壞。
2. 設備故障：由於資訊系統的運作主要是靠軟體、硬體及網路設備來達成，所以軟體錯誤、硬體故障或網路斷線等，都將造成資訊系統的損害。
3. 蓄意侵害：人為的蓄意侵害行為是資訊安全工作上最難預防的威脅因素，亦占了資安威脅因素的 81%至 83%，例如單位內部人員利用職權之便，對電腦系統之軟硬體設施進行破壞與非法使用，或外部駭客的入侵，進行各種破壞或竊取資料等。
4. 人為疏失：人為疏失為威脅資訊安全最重要的一項因素，而資安問題又主要出現在「人」的問題，這是一種存有便宜行事或好奇心作祟的心態，例如作業員輸入錯誤、電腦操作員誤置檔案或私自下載網路上免費的小遊戲、美女圖，或開啟來路不明的郵件而衍生駭客入侵等問題。

既知資訊安全可能面臨的各種威脅，那麼又該如何有效防範呢？「風險管控」提供了我們在危安事件發生前，即建立健全的安全防險觀念和運作機制，這是預防危安事件發生的關鍵。

管理學中有個「破窗理論」可以說明風險管理的重要，若有一幢建築物的窗戶破損而不馬上修復，就會有更多的窗戶被人打破，而且這幢建築物很快就會成為犯罪的溫床。這個理論是由美國政治學者威爾遜和犯罪學家凱林首先提出，前紐約市長朱立安尼即將此理論應用於整頓紐約治安上，他從維護紐約的犯罪溫床—地鐵著手，讓紐約的治安大幅改善，也因為朱立安尼而使此一理論聲名大噪。

其實，做好資訊安全的風險管控就是一種防患於未然的管理工作，網路上有句名言：「網際網路的時代，有誰知道坐在螢幕前的是一條狗或是病毒？」這句話即是提示資安風險管控的重要，唯有建立資安憂患意識，並做好風險管控，隨時提高警覺，始能免於受「駭」。

以下提出三個案例，期能警惕並強化國人對於資安的保密認知：

一、使用公務電腦處理私務：

某單位同仁利用公餘就讀「在職專班」，某日因公務電腦資料遭竊，經調查始知，該員因貪圖便利，私自將課堂提報資料及論文以隨身碟儲存後利用公務電腦作業，該電腦雖未連接網路，但仍遭植入木馬程式致公務資料遭竊。

研析：一般人以為只要電腦不連接網路，在隨身碟的公務資料就不會外洩，或認為只要先將網路線拔除，於處理公務資料後，再將資料刪除、連網，就不會有問題；事實上，只要家中電腦被植入木馬程式，即便是在隨身碟中作業，公務資料仍會被複製到電腦中，只要一連上網路，這些隱藏在電腦的資料就會自動經由中繼站傳到駭客電腦。

二、貪圖免費使用非法軟體：

春節期間民航局開放上網訂購返鄉機票，某位民眾使用「訂票自動搶票系統」非法軟體，影響訂票系統正常運作遭

檢調單位查獲。
研析：該位民眾因資安法紀觀念淡薄，貪小便宜隨意下載非法軟體使用，造成訂票系統當機，影響其他民眾權益，觸犯「刑法第 36 章—妨害電腦使用罪」第 360 條「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金」。

三、好奇任意下載不明程式：

日前報章刊載，民眾檢舉網路上流傳清涼美女圖，經查為某單位警局流出，復經查證，係因某位警員因好奇下載來路不明郵件，並將信件轉寄，致遭駭客入侵。

研析：據調查發現，中共常藉由網路，針對我政府機關、國軍人員或高科技業者進行網路情蒐，在取得相關電子郵件帳號後發送色情圖片（其間夾帶病毒或木馬），或假冒學校、政府單位寄送含有惡意程式之電子郵件，使用者開啟後，即遭植入木馬致資料遭竊，或淪為駭客做為攻擊他人的中繼站。

「保密安全，人人有責」，由以上案例得知，資訊安全工作是一項防患於未然的風險管理過程，而建立正確的資安素養更是現代人必須具備之基本常識；尤其在資訊化、數位化、網路化的今日，機密資訊的保護難度相對提高，唯有積極提升國人保密習性及資安素養，並落實風險管控，資通安全才得以確保。（摘自清流月刊－作者劉秀貞）