如何做好資訊安全防護工作

資訊安全是什麼？資訊安全防護的內涵有哪些？資訊安全工作應如何推展與落實？這些問題不論政府機構或企業組織向來十分重視，但相關的電腦安全、網路安全，甚或是網際空間安全等資安議題，卻很少有人提出有效的方法論。

資訊安全防護工作絕不僅止於保護重要機敏單位，甚或某一組織階層內電腦網路上所儲存的資料，惟有擴及整個網路基礎建設包括確保網路節點、路由器、領域名稱伺服器及網路交換器等設備均能正常的運行，同時資料能正確及可靠的傳輸，則資訊安全工作始能落實。因此在此前提之下，我們不禁要問：完整的基礎建設包含什麼項目？網路安全會面對什樣的威脅？防護措施如何部署才能發揮最大的成本效益？而這三個問題的核心卻在於如何精確地定義所謂的「資訊安全」。

「安全是一切的基礎，沒有安全就沒有一切」，這句耳熟能詳的話不僅適用在建軍備戰，同時也適用於資訊安全的領域，本文將跳脫資訊科技複雜的技術層次，直接由管理者的觀點切入，從安全需求、安全政策及安全機制等三個構面剖析資安防護的具體內容與步驟，以使大家對資訊安全防護工作有更深刻的認識。

一、資訊安全需求：

資訊安全的特徵雖在保護資訊之機密性、完整性與可用性，但企業組織與軍事單位卻因需求不同而使得要求重點各異，如一般企業組織採用資訊系統之目的在使其員工或研發人員能有效率作業，因此資訊存取與分享至為重要，所以可用性的確保為第一要務；反之在軍事機敏單位，則強調機密性與完整性，因為機密資訊如遭未授權人員讀取而導致洩漏將危及國防安全，因此與其資料被解讀毋寧檔案因無法讀取而遭到刪除，以有效避免機敏資訊之刺探或蒐集，因此明確的律定單位的資訊安全需求是落實資安防護工作的第一步。

二、資訊安全政策：

安全需求為電腦系統之某些存取動作提供允許或不允許的指導原則，而安全政策則進一步的規範系統處於什麼樣的狀態是被允許，什麼樣的狀態是不被允許。假使系統一直停留在允許狀態，而使用者所執行的存取行為也是被允許的，則這個系統是安全的；如果系統能轉換至不允許的狀態，或使用者可以執行不允許的動作或行為，則這個系統就是不安全。這部分在國際及國內均有相關的規範可供遵循，如 BS7799、ISO17799、CNS17799、CNS17800 等標準，只要藉著計畫（Plan）--執行（Do）--檢查（Check）--行動（Act）的 PDCA 循環程序反覆檢驗即能達成。

三、資訊安全機制：

只有安全政策是不足夠的，需輔以安全機制的配合，安全政策始能落實執行，因為安全機制可以保證系統不會進入不安全的狀態。安全機制可以是技術，如加密、防火牆、入侵偵測系統的運用，也可以是一套控管的程序，如機敏資訊分持及讀取權限之設計。但有時候技術性的機制並無法滿足政策的需求，如校園內雖禁止使用非法的 mp3 音樂，而系統管理者也經常實施檢查，但聰明的學生往往會採取更改副檔名、加密或隱藏等方法，因此即使管理人員使用一般的搜尋工具仍無法有效的查察，這時在技術上無法有效達成資安控管目標的部分，則採用程序或政策卻能有效的加以禁止。

而由前述的分析我們可以清楚的了解，沒有任何一種方法或機制可提供系統絕對安全的保證，但不同的方法則能提供不同程度的防衛能力，惟有依照需求綜合運用而整體安全防護始能確保；此外，評估安全也不能僅依賴系統所採用的機制或方法，有時使用者環境也是影響安全成敗的重要因素，因此必須納入考量。

資訊安全的構成元件包含需求、政策及機制等三者，「需求定義安全的目標」，它說明什麼樣的安全是你所預期的；「政策定義安全的意涵」，它說明達成安全目標的步驟有哪些；而「機制則能強化政策」，他說明採用什麼樣工具、程序或方法可以保證達成資安防護的目標，因此三者相輔為用，缺一不可；因此當政府機構或企業組織在建構資訊系統時，除應優先考量作業系統本身的安全性之外，更需將前述資安的三個元件整合在整個軟體發展生命週期的每一階段當中，使得安全政策能滿足組織的需求，而安全機制可有效強化政策之執行，如此則在安全無虞的環境下使用資通網路環境不再是一個遙不可及的夢想，而落實整體資安防護工作的目標也於焉達成。

轉錄自清流月刊 93 年 12 月號作者吳文進