資訊安全應達成的目標

◎王志銘

網際網路在 1990 年代以驚人的速度成長，從桌上型電腦、筆記型電腦，到現在的手機無線上網，都與網際網路連結在一起，使得病毒擴散與駭客攻擊更加頻繁。近年來常見的木馬程式、間諜軟體、釣魚郵件及垃圾郵件等，不僅造成鉅大的損失，也難以單一技術防禦。

網路沒有絕對完美的防禦，因此資訊安全是一種相對「取捨」的作為，應在有限的條件下，將資源投資在最容易受到攻擊或是對單位傷害最大的安全弱點上。例如，一間 10 位員工的小企業，最該做的是為每台電腦安裝防毒軟體，而不是花大錢建構一個安全營運中心。

完整的資訊安全應同時建設 3 個 P 的防護，分別是「人員（people）」、「程序（process）」、「產品（product）」；可以用一句話來整合三者的關係：人員都遵守資訊安全程序，產品（資安工具）才能發揮功效。單位規定電腦要設定複雜度 8 碼以上的登入密碼，同時機敏資料必須要加密，這就是一種程序規範，單位必須依照資訊獎懲規定進行宣導及獎懲，使所有人員都能正確地執行這個程序，唯有如此，單位所購買的作業系統、防毒軟體及端點防護系統才能發揮保護資訊的功效。假使一個單位都照規定做了，但若有些人卻由於記不得經常更換的密碼，就寫在鍵盤或螢幕上，儘管有安全的產品和操作程序，然而缺乏資訊安全意識就會功虧一簣，可見 3 個 P 的防護缺一不可。

單位推動資訊安全所要達成的目標有三項：一、預防，事先預防比事後處理容易許多，防火牆的建立及 Nessus 等偵掃軟體的運用，均可預防電腦或漏洞被違規使用；二、偵測，除了人員的資訊安全警覺性外，入侵偵測系統（IDS）及防毒軟體（SEP）合成區域聯防（ZDBS），將可達到偵測之目的；三、反應，平時必須經常演練及資料備份，將有助於資訊安全事件發生後的反應與復原。