資通安全之防範及經費編列

◎行政院主計處電子處理資料中心

壹、前言

隨著電腦科技的發展，個人電腦的普及網路的盛行，使得資訊的傳播無遠弗屆，政府部門無不卯足全力利用電腦網路之方便性，提供多樣化之網路服務，期望民眾「多用網路，少用馬路」，以減少社會成本，提高服務績效；民間企業也積極利用電腦網路的便利，提高企業競爭力；如何確保資訊安全，已是資訊提供者及使用者最關切的問題，因此編列資安相關經費做好資安防護有其必要。

貳、現況分析及檢討

回顧這幾年的資安事件，有個人資料外洩、病毒危害及駭客攻擊等，事件發生來源，有外部使用者透過網路進行未經授權之存取或破壞機關對外之網路服務，及內部員工對外洩漏資訊或疏忽造成系統服務中斷等，其實大部份之資安事件是可預防的，只要使用者落實執行各項資安規定。

參、未來及改進方向

各單位推動資安工作，首須訂定資安作業規範，可就人員、系統、設備、網路、資料及委外等分別制訂保護措施，茲簡要摘述如下：

在人員方面：設定優質帳號(由文、數字及特殊符號組成，最少七個字元，且每三個月要定期更換)、簽署保密協議、定期接受資安訓練、定期審查存取權限、人員異動即時取消其使用帳號及權限。

在系統方面：設定使用權限、定期備份、作好系統變更管制及文件管理。

在設備方面：設防火牆、防毒軟體、即時修補系統漏洞及更新病毒碼、可攜式設備加強管理、注意設備環境安全(機房門禁、電源、纜線)。

在網路方面：對外網路服務採原則關閉、例外開放之管理政策，內外網路作區隔管理，重要網路服務具身份鑑別機制。

在資料方面：依機密性、敏感性作分級標示及管理，重要資料採實體隔離及建立使用者身份認證機制、加密儲存、定期備份。

在委外方面：資安規定納入合約、與委外廠商簽署保密協議、釐訂廠商資安權責。

爲促使各單位員工確實執行各項保護措施，因此實施資安內部稽核是必要的，因應上述措施可能失效或受到巨大災變時，確保系統能永續運作，其營運持續管理計畫(含系統備援回復、緊急應變措施)便成爲最後一道防線，各單位應規劃建立並定期演練，以防萬一。

部份保護措施可藉助工具，如設防火牆 (視功能約在 30 萬元間)、防毒軟體 (每台個人電腦約在 600-700 元，如爲更新授權者約 235 元)、入侵偵測軟體 (約 30 萬元)、資產管理系統 (10 人版約 3 萬元)等，亦可委外辦理資安業務(所需經費依範圍及設備複雜度估算)；至於備援需求，須視資訊處理之即時性考量，備援方式可分同步備援(成立備援中心，設備援主機並作同步備援，成本最高)、熱備援(設備援主機，成本次高)、一般備援(檔案備份採異地存放，爲一般機關採用)；資安防範很重要，惟各機關仍應視處理資料之機密性、敏感性，選定符合成本效益之控制措施，並據以編列必要之資安經費。

肆、結語

資通安全爲大家所熟知，且爲機關所重視，倘資安工作不落實，其系統必定不安全，資安防護工作成功之關鍵因素，要管理階層實際的支持與承諾、有正確的風險評鑑與擬訂有效的控制措施、全體員工的認知與實踐、資安政策要定期審查及不定期的實施資安稽核等，資安工作永遠也做不完，建立「資通安全，人人有責」的觀念，希望大家將資安規定視爲例行工作，惟有貫澈執行，才能確保機關之資通安全。