淺談資安風險管理：以遠距視訊為例

金門縣政府政風處專員　陳大中

摘要

資安風險管理為資安防護之基礎，唯有完善的風險管理，方能逐步建構更臻妥適之資通安全防護網。

全臺上網人數已突破 2 千萬

依據財團法人臺灣網路資訊中心「2019 臺灣網路報告」，推估民國（下略）108 年全國 12 歲以上曾上網人數達 1,898 萬人，而全國上網人數（包含未滿 12 歲）已達 2,020 萬，整體上網率高達 85.6%，為歷年最高 1。換言之，我國各項資訊科技及網際網路不僅日益普及，更有快速發展之趨勢。

公私部門因資安破口，遭受鉅大損害

然隨著網際網路及其他資通科技之迅速發展，亦帶來資訊安全危機，如：銓敘部 108 年 6 月間經報導指出超過 24 萬筆個人資料遭外洩，台積電於 107 年 8 月初設備遭電腦病毒 WannaCry 感染，該次中毒事件影響台積電營收估計新臺幣 25.96 億元（依台積電 107 年第三季財報數據），足堪為我國史上損失最大的資安事件。今年 5 月間不僅國內多家重要能源及科技公司接連遭勒索軟體攻擊，甚至爆發位列資通安全責任等級最高級 A 級之總統府電腦也遭駭客入侵事件。

視訊軟體 Zoom 之資安隱憂

全球因受新冠病毒蔓延影響，遠距視訊軟體開始廣泛使用，其中 Zoom 視訊軟體資安疑慮遭連環踢爆，先是該視訊軟體將加密金鑰存

放位於中國大陸的伺服器，有遭駭客竊聽之虞。隨後爆發英國金融時報記者藉由竊聽其他報社運用 Zoom 視訊軟體召開的會議，刺探其他報社之新聞訊息。不僅如此，香港中文大學使用 Zoom 視訊軟體進行遠距考試，系統被不明人士駭入，考試時透過該軟體分享個人電腦螢幕，播放色情成人片、舞曲 MV 等，Zoom 的各種資安事件接踵而來地發生。因此，電動車大廠特斯拉、美國國家航太總署及英國國防部等機構陸續宣布禁用 Zoom 軟體。

資安風險管理步驟

為免更多公、私部門或個人因資安破口，遭受鉅大損害，我國亟待正視資安防護問題，然資安防護沒有百分之百，不同資通環境，都存在不同的弱點與威脅，只有透過不斷精進，確實做好風險管理，才能將資安風險降到最低，因此，無論是公、私部門或個人，都應確實認識強化資安風險管理，管理步驟有四：

首先，應先識別風險，不論是公務機關、私人機構或個人，均應對其本身及所屬部門之資安風險全貌確實掌握，雖然各部門業務、作業差異甚鉅，可能潛存的風險因子不盡相同，然仍應審酌不同業務屬性，做出可識別的異質性資安風險因子，做好風險識別，是管理的基礎，也是最重要的一個步驟。

其次，進行風險評估，針對資訊資產可能存在的每個資安風險，逐一分析，分析要項包含評估曝險係數、發生可能性、發生時之影響程度、損失預期範圍及處理之優先順序等，確實風險分析與評估，以為後續有效之管理與因應。

第三，深入檢視風險成因，瞭解可能之外在威脅與本身潛存之弱點，透過確實認識可能造成資訊設備、系統危害或威脅之外在影響因素，如系統內容遭駭或遭植入惡意程式，致機密資料遭竊取、竄改，或造成原有之服務不得不中斷等；以及掌握資訊系統或資訊設備本身

可能存在的弱點，例如硬體設計存有缺陷、無防火牆設備、軟體測試不足、內部控制未確實等，唯有全方位檢視風險成因，清楚分辨外在可能危害之威脅與內在潛存之弱點，才能進行有效之相應安全管控或對策，避免損害發生或擴大。

第四，提出最適切之風險因應，當風險經識別出來及評估後，須提出相應之處理計畫，處理方式大致上可區分為避免風險、轉移風險、降低風險及接受風險。我們須先思考有無方式避免風險，如無法避免，退而考慮能否轉移風險，若無法避免又無法轉移，就審酌有沒有辦法降低風險可能帶來的影響與衝擊，最後，如果無法處理或需處理成本過於巨大，接受風險，也算是一種選擇。

使用遠距軟體之風險管理

以遠距軟體為例，使用前應提前做好風險管理，

其一，選購本身較無資安疑慮之產品，不論公、私部門在使用遠端視訊產品前，均應由資安管理單位或請專業之資安人員，協助全面盤點遠端視訊之同質性產品，了解產品是否符合《資通安全管理法》等相關規定，是否存有將資料回傳至特定地區之伺服器的疑慮，汰除有資安風險之產品，擇優選用符合規定之遠端視訊產品。

其二，進行遠端視訊會議或教學前，應修改密碼，避免使用弱密碼，更不得便宜行事，取消密碼。進行安全性及相關環境設定，落實人員管控，非屬該次會議或教學之第三人，未經同意，不得進入。

其三，針對遠端視訊產品之操作人員做好教育訓練，以利視訊之正常進行，遇有狀況，方得以迅速處置。

其四，凡機密、敏感議題或資料，均不宜於遠端視訊會議或教學使用，避免不慎洩漏，造成重大損害。透過完善資安防護措施，減少外在威脅及內在弱點，讓風險因子降到最低，持續落實資安風險管理，讓遠距辦公或遠距教學，更加安心踏實。

資安即國安

資訊安全不僅是安全與便利的取捨，更關係整體國家安全與國家利益，近年政府為強化資安工作，陸續完成相關法制作業，然徒法不足以自行，若要達到有效資安防護，就須做好妥善之資安風險管理，並逐步落實資安環境的改善，減少風險的存在，並培養資通使用者之資安觀念及敏銳度，提升其資安防護之素養與能力，如此方能建構更臻完妥之資通安全防護網。