1月份公務機密維護宣導-資安趨勢與發展藍圖

資安的概念就是風險管理的概念。通常人們都會認為資安應該是去做到滴水不漏，沒有發生任何資安事件，才是好的資安，但是就類似於網路長城一樣，再怎麼強大的防護，攻擊方總是可以找到漏洞，首先入侵系統。一個好的資安管理應該做到風險管理為核心，經通過審慎地評估與核查，摸清整個環境中最應保護的核心系統，並進行全局管理的強化和新技術的導入，而將風險降到最低，讓受保護的標的在主體性、參與性、機密性的考慮下，能夠維持正常運轉，在受到侵犯時即能正確化認知，同時地化為能正確認知。

「情資分享」是資安事件處理中重要的一環

資安防護可以區分為早期預警、持續監控、應變，一直到協調處通報等四個階段，而這四個階段也以風險管理為核心理念進行循環，其中「通報應變」是最重要的一環，由即時迅速的通報機制，將所發的資安事件情況，由標準化的通報訊息，快速地傳遞給主管機關，不僅可以防止事件擴散，更能全球範圍的即時地通報，讓其他機關可以有警覺，並能進行防禦，而且各地快速的通報機制，也可以讓主管機關掌握事件的影響面，以確認是單一事件或者大範圍的攻擊，對於這個資安防護都有重要的影響。

例如以WannaCryle索病毒為例，大多數事前的通知及提醒各政府機關應注意的事項，再加上病毒擴散期間各政府機關及時通報，讓行政院資安處掌握最新的情況，將影響降到最低。而在事後，TWCERT/CC也將相關的資訊傳播國際聯絡管道，傳遞給國家，突破國內政府機關內部的縱深防護，到跨機關的資安資訊交換，因此跨國間的資安聯防，使得資安事件的影響降到最低，不致造成其他重大的損害。

我國資安推動四大策略

我國因政治情勢的特殊勢，曾經在一個月內受到超過2千4百萬次來自境外的攻擊，這些樣態的樣本數量遠多於其他國家，同時境外惡性組織攻擊我國所積累的經驗，進一步調整及優化後，轉而攻擊其他國家，因此許多國家希望和我國在資安方面進行合作，希望能夠取得併分析這些攻擊的與之模式，這也是我所取得的經驗優勢。資安產業規

模不足，以及缺乏長期的資安人才培育制度，使得無論是政府或民間產業，都有資安人才不足的危機，而這也必須政府以整體面來思考，從資安通知識人才的培育、到資安專才的培育、職涯的發展、以及高等資安技術的研究等進行規劃與推進。既從教育體系、研究體系、國防體系、政府體系，以及就業體系等，必須有長程完整的規劃，以培養資安人才。

在審查資安聯基礎環境部分，考量各機關的業務特性不同，所要保護的客體和風險管理的重點不同，我們將建立資安聯治理成熟度的框架，律定風險管理架構，全國4個構面十九項評估原則，由機關依據實際需求，逐年提升資安聯治理成熟度。部分，亞太組織內部的縱深防禦、擴大到跨機關的聯防、並推進跨境至跨國資安情資交換，讓資安防護從點到面，從內部到國際合作；此外，並以影響國家社會安定的關鍵基礎設施為優先，要求水資源、能源、通信系統傳播、交通運輸、醫療、金融與經濟、國家安全的關鍵基礎設施為優先，要求水資源、能源、通訊系統傳播、運輸而在提升產業自主能量的部分，我們希望能看到資安產業的生態鏈，讓資安產業和產業的資安需求能夠對接，再接由關鍵基礎設施的場域，使國內資安產業者有機會發展新型的資安顧問與諮詢服務。最後也是最重要的是人才培育，各個學校、研究單位、希望與政府的合作，為我國培育資安產業所需的資安人才，解決各方面欠缺資安人才的問題，並完善國內資安產業自主生態鏈，確保各政府機構及關鍵設施基礎設施之自主性。

結論

資安即是國安，新型態的戰爭中，無攻擊所造成的破壞十分嚴重超過傳統攻擊所造成的破壞，例如利用網路攻擊癱瘓金融體系、交通運輸，乃至水電的供應等，這對現代化國家而言，信息系統一旦引發問題所造成的影響，將導致社會的運作突然，而國家的防禦也難以為繼，因此我國資安未來的發展藍圖，將打造一個安全可信任的數位國家為願景，並以厚植自我防護能量，保衛數位國家安全為目標，從法規標準到資安聯防，建立自主資安產業到培育人才，期望全國這四個推動策略環環相扣，讓人民處於安全無憂的環境下，放心利用科技所帶來的便利和服務。

轉載自《清流》雙月刊