資安趨勢與發展藍圖

■行政院資通安全處處長　簡宏偉

資安的概念就是風險管理的概念。通常人都會認為資安應該是要做到滴水不漏，沒有發生任何資安事件，才是好的資安，但是就如同網路長城一樣，再怎麼強大的防護，攻擊方總是可以找到漏洞，進而侵入系統。一個好的資安管理應該是以風險管理為核心，經由審慎地評估與辨識，找出整個環境中最應該保護的核心系統，並經由管理的強化和新技術的導入，而將風險降到最低，讓受保護的標的在完整性、可用性，和機密性的考量下，能維持正常地運作，在受到入侵時即能正確感知，同時更進一步地化為主動防禦。

「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、通報應變，一直到協處改善等四個階段，而這四個階段也是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，藉由即時迅速的通報機制，將所發的資安事件情形，藉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，更能經由即時地通報，讓其他機關可以有警覺，並能進行防禦，而且經由快速的通報機制，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是大範圍的攻擊，這對於資安防護都有重要的影響。

例如以今年的 WannaCry 勒索病毒為例，經由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即時地回報，讓行政院資安處可以掌握最新的情形，將影響降到最低。而在事後，TWCERT/CC 也將相關的訊息經由國際連結管道，傳遞給其他國家，透過國內政府機關內的縱深防護，到跨機關的資安訊息交換，乃至跨國間的資安聯防，使得資安事件的影響可以降到最低，不致造成重大的損害。

我國資安推動四大策略

我國因政治情勢特殊，曾經在一個月內遭受到超過 2 千 4 百萬次來自境外的攻擊，這些攻擊樣態的樣本數遠多於其他國家，同時境外惡意組織經由攻擊我國所累積的經驗，進一步調整及優化後，轉而攻擊其他國家，因此許多國家都很希望和我國在資安方面進行合作，希望能取得並分析這些攻擊的行為與模式，而這也是我國長期累積經驗所取得的優勢。但是也由於我國內需市場中的資安產業規模不足，以及缺乏長期的資安人才培育制度，使得不管是政府或是民間產業，都有資安人才不足的危機，而這也是政府必須以整體面來思考，從資安通識人才的培育、到資安專才的養成、職涯的發

展、以及高等資安技術的研究等進行規劃與推動。也就是說從教育體系、研究體系、國防體系、政府體系，以及就業體系等，必須有一長程且完整的規劃，以培育資安人才。

目前行政院已經規劃了第5期的國家資通安全發展方案，期程從106年到109年，希望以打造安全可信賴的數位國家為願景，並以厚植自我防護能量，保衛數位國家的目標，逐步建構一個安全可信任的數位基礎環境。為達成這樣的願景與目標，我們擬訂了四大推動策略，分別是完備資安基礎環境、建構國家資安聯防體系、提升資安產業自主能量，以及孕育優質資安人才等策略。

在完備資安基礎環境部分，考量每個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，我們將建立資安治理成熟度的框架，律定風險管理架構，經由4個構面19項評估原則，由機關依據實際需求，逐年提升資安治理成熟度。在建構國家資安聯防體系的部分，經由組織內的縱深防禦、擴大到跨機關的聯防、並進而擴張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，並以會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、通訊傳播、交通運輸、緊急醫療、金融與經濟、高科技園區，

以及中央與地方政府等八大關鍵基礎設施，建立資安訊息分享及聯防機制，以保護並維持國家的基礎運作。而在提升產業自主能量的部分，我們希望能建構資安的生態鏈，讓資安產業和產業的資安需求能夠銜接，再藉由關鍵基礎設施的場域，使國內資安業者有機會發展新型態的資安顧問與諮詢服務。最後也是最重要的是人才培育，希望經由學校、研究單位、業界和政府的合作，為我國培育資安產業所需的資安人才，解決各方欠缺資安人才的問題，並完善國內資安自主產業生態鏈，確保各政府機關及關鍵基礎設施之自主性。

結論

資安即是國安，新型態的戰爭中，無實體攻擊所造成的破壞遠遠超過傳統實體攻擊所造成的破壞，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，資訊系統一旦出了問題所造成的影響，將導致社會的運作不穩定，而國家的防衛也難以為繼，因此資安不再只是個人或是組織的安全防護而已，更涉及到國家整體的安全及生存。

我國資安未來的發展藍圖，將打造一個安全可信賴的數位國家為願景，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，期望經由此四個推動策略環環相扣，讓民眾在安全無虞的環境下，安心使用科技所帶來的便利與服務。

（※本文摘錄自法務部調查局 106 年 11 月份清流雙月刊）