

資安即國防，防護核心戰略產業

臺灣資訊安全協會秘書長 洪伯岳

近年來層出不窮的資安災害不可被忽視

2020 諧音愛你愛你，卻對世界及臺灣而言都是辛苦的一年，面對傳染病肆虐的全球經貿變局，美中貿易戰及香港政治情勢發展，對臺灣既是挑戰，也是機會。雪上加霜的是臺灣近年來面臨層出不窮的資安攻擊事件，2018 年國際大廠台積電安裝新機台時遭受勒索病毒攻擊導致當機，影響無法估算；2019 年知名企業廣達電腦遭到冒用名稱領取貨款，合作廠商 Facebook、Google 等大廠皆遭受重大損失；而今年初台塑、中油等多間重要能源及科技公司也遭受來自中國駭客組織「Winnit Group」的勒索病毒攻擊並揚言將會持續進行。層出不窮的資安問題持續發生，誰都不能置身事外，必須盡快建立起安全的資訊防護，而這需要政府、企業及人民共同的努力。

中小企業為主體的臺灣需要建立自己的資安防護

從 1970 年代開始，臺灣的製造業、電子業蓬勃發展，為臺灣經濟帶來精彩的一頁，然而不同於很多大國以世界大廠為主支撐整個國家（如韓國），小而堅強的中小企業一直是臺灣經濟主力，而這些撐起臺灣 GDP 的大小企業，近年來卻不斷面臨資安攻擊的問題，但我們卻無法像國外這樣以國家之力保護少數大型企業。當對岸以舉國之力針對我們時，這些為數眾多的中小企業該如何自保，是我們該思考的課題。臺灣有許多製造出口產業，彼此間為供應鏈的型態，環環相扣，牽一髮而動全身，而在各產業蓬勃發展時，科技的進步也帶動駭客攻擊行為的轉變，從前只是點對點單一對象的

攻擊，現已演變成爲計畫性的面狀式攻擊；從前很多無法獲益的攻擊行爲，現在因爲虛擬貨幣、比特幣等的出現，駭客金流的管道更佳的暢通，所能勒索的利益更大，毫無疑問的將會對臺灣整體的產業帶來更嚴峻的衝擊，而我們該有不同的政策方式來保護自己，也保護臺灣。

資安問題是災難，資安即是國防

國家的基礎建設中，水、電、天然氣等都是不可或缺的能源，這些生活中無所不在的能源產業都已有完整的防災 SOP，能源業者也有自身的防護措施，畢竟出了一點小問題都可能影響到舉國的民生，除此之外還有完善的災害應變方案，而這些都是臺灣慢慢的從每一次災害中學習，一步一步建立起來的。現在這些重要的基礎建設正面臨嚴峻的資安問題，不只是資訊安全本身，其中也有很大一部分的政治因素。一般的駭客不會去攻打基礎建設，沒有太大收益不說，自身安全怕也會面臨很大的考驗，但當國與國的政治立場不同，在國際間產生摩擦時，某些背後有靠山的駭客組織就會開始這種行爲，那將不單單是資訊安全受到挑戰，而是國家安全整體面臨挑戰，由此看來：資安問題是災難，而資安即國防，這是大家都該有的共識。

分級的資安解方，建立資安國防

除了有共識之外，也必須一起商討該如何完善臺灣的資安國防，應由資安專業人員協助政府或者各產業間的政策決議，設計出完整的防護政策；不單單只是使用資安產品，而是需要加上整個流程的資安服務，建立資訊安全災害專屬的 SOP 應變方案，比如事前就須先做好資料備份及異地備援，將備份資料加密，以及災害發生的當下，防止病毒持續擴散，盡快關機斷網，保留證據讓鑑識單位分析，以求將傷害降至最低，並快速回復原本該有的運作。例如：使用天然氣這項產品，其實就是使用了背後龐大的天然氣產業以及其產業消防安全的防護，資安產品也是一樣的，除了外力的攻擊外，自身的使用不當也會產生資安問題；建立起完整的解決流程，包含產品、服務以及災害發生時的通報、聯防，最後人才的培育，都是缺一不可。

此外，整體產業的服務機制也相當重要，如天然氣的檢測流程、巡檢人員皆有分級分工一樣，資安產業亦需要分級分類的方式，藉由政府的幫助，在政策上幫助產業分級，並建立一個完整的產品分級規章，方便人民識別。金融產業有龐大的金流，與

第一線的零售業所需要的資安等級一定是不相同的，而如何能讓所有企業主都清楚知道，並找到適合自己的產品及方案，是臺灣現在急需研究的計畫。

資安產品不是應用產品，而是基礎建設

建立起完整的分級制度後，還必須有一套政府定義的防護網，此後各產業的整體運作及分級間的整合，都須仰賴於此。好的基礎建設分為很多層面，很多時候我們會學習國際間的良方，知己知彼，進一步設計成適合臺灣的模式；產業間與政府的合作也十分重要，與政府一起合力商討相關金融方案及保險方案等，並且研究推動產業的法規辦法；最後，十分重要的人才培育計畫也需擬定。以上都有所完善之後，資安產業的整體發展、產業間的整合及推動、臺灣的資安基礎建設也會隨之提升。以更長久的益處來說，臺灣的資安實力本來就堅強，如果能在臺灣先完善資安基礎建設，也更有利於我們向外推廣國際，讓世界看見臺灣。

有科技的地方就有資安，防護核心戰略產業

資安問題除了是新聞報導的重大事件之外，也與生活息息相關，只是大家未曾發覺。國家間的科技發展被駭客攻擊固然是資安災害，企業間使用視訊會議時，也會產生資安疑慮；甚至個人的一通視訊電話都存在資安問題。在科技跟生活息息相關的現今，資訊安全跟我們息息相關。由於世界資安事件頻傳，各國現也紛紛提高各產業的資安標準，要求建立完善資安評分制度，如德國汽車工業聯合會（VDA）推出了一套有多數成員認可的資訊安全評估流程，而評估結果需上傳至 TISAX 平台，以求保障產業的安全。如此戰戰兢兢就是因為汽車產業為垂直的供應鏈，稍有不慎，資安漏洞變就會成為嚴重的人身安全問題。

臺灣除了保守訂定資安防護網之外，也可主動出擊，將多數產業結合資安，如：提升臺灣既有的 OT 產業產品的資安水平，協助通過國際認證，進而提升產品的質量，提高國際出口的機會，將危機變成轉機。推行各產業產品的資安認證，進行公司企業的資訊安全檢測等等；經由增強自身安全防護，同時提高自身穩定度等等，都是在國際上加分的要件。所以，臺灣在核心戰略產業上需要運作的，不單單是個別企業的防護，而是整體產業供應鏈都非升級不可。今年是 5G 元年，其所帶來的網路高速流量，勢必成為下一個重大資安挑戰，做好資安規劃，才是最能有效防堵駭客攻擊的做法。🌀