從《資通安全管理法》看企業資安維護

文《李婉萍、陳宏志[1]》

圖／ unsplash

為迎接 5G 時代來臨和提升台灣資訊安全的實力，行政院已核定「國家資通安全發展方案（110 年 ~113 年）」，推動國家資安發展藍圖。

前言

隨著上網人口增加與資訊相關活動開展，現代社會對資通系統與網路的倚賴日深，針對資通系統與網路的攻擊行為也越來越多。我國於 108 年 1 月起開始施行《資通安全管理法》(以下稱資安法) 及其一系列子法，主要為使公務機關及其他對公共安全與民眾福祉有重要影響的特定非公務機關 (例如，某些特別關鍵的油、水、電、醫療、電信機構)，能更重視資通安全，並有系統的持續精進資安維護事宜。雖然目前適用對象不包括大多數臺商或其他一般企業，但是資安法要求之資通安全維護計畫或應辦事項，例如導入資訊安全管理系統、採行資通安全防護措施、提升人員認知等事項，都是因應資安威脅或建置管理機制的重要項目，可供企業研擬資安維護方針與發展、調整商業策略時參考。

《資安法》對機關資安維護有諸多項目要求，這些要求並非我國所獨具，例如美國國家標準與技術研究所 (National Institute of Standards and Technology, NIST) 也建議可以採用其推動之網路安全架構 (Cybersecurity Framework, CSF) 來進行資安維護。細究 CSF 的識別、保護、偵測、回應、復原等五大功能架構與細部內容，可以發現其重視之面向與《資安法》的規定意旨，若合符節。

以識別為例，CSF 包含識別資產管理、營運環境、治理、風險評估、風險管理策略等內容，都與《資通安全管理法施行細則》(以下簡稱施行細則) 要求機關之安全維護計畫應包括辨識核心業務、盤點資通系統、進行資安風險評估等相似。企業在發展資安維護作法時，可以選擇採取《施行細則》對資安維護計畫的架構，或採取 CSF 的框架，並在具體細節上參考《資安法》的規定，關注《資安法》因應外在環境與執行狀況之修正[2]，持續精進自身的資安維護。

在一般的資安維護規定之外，《資安法》先前對於危害國家資通安全產品的明文，及近來實務上政府機關對使用中國大陸廠牌產品之節制，則呼應了國際對資安「乾淨路徑」(clean path)、「乾淨供應鏈」(clean supply chain) 的趨勢；此一趨勢也是臺商及其他企業在完善自身資安條件、調整商業策略時，所不宜忽視的。

《資安法》之防護基本要求與可供企業參考之作法

一、對組織資安維護計畫、應辦事項與資通系統防護基準之要求

《資安法》主要內容之一，係要求公務機關及特定非公務機關，須訂定資安維護計畫。依據《施行細則》第 6 條規定，資安維護計畫應包括諸多項目，首先是辨識與盤點，辨識與盤點的對象則包括機關核心業務、資安政策與目標、資通系統與資訊、相關風險等。參考這些項目規定，企業可以試著去辨識自身最重要的業務是那些，分析這些業務與支援業務的資通系統之對應與依存度，並從相關的業務流程與系統運作環節來找出可能的資安風險，評估其發生的可能性與嚴重性；此外還須思考在企業的資安政策與目標下，可容許之風險程度為何。

《施行細則》第 6 條亦要求資安維護計畫須包括對資安情資之分析與因應機制、資安事件之通報與應變機制、資通系統或相關服務委外時之監督管理，以及機關投入資安維護之人力與資源規劃等。這些項目在《資通安全事件通報及應變辦法》、《資安法》第 9 條及《施行細則》第 4 條對委外管理與監督的條文，及《資通安全責任等級分級辦法》(以下稱分級辦法) 均有更細緻的規定，企業可以參考其規定要項與精神，衡量自身資源與其他狀況，發展出自己的版本。

對企業的資安維護來說，適當防護措施的採取，可能是企業資安維護計畫裡最重要的一部分。可參考《分級辦法》附表一至附表八及附表十，對機關應辦事項及對資通系統之防護基準的要求來加以思考。

《分級辦法》附表一到附表八，依據機關之資安責任等級，分別從管理面、技術面，以及認知與訓練等三大面向規定各等級機關之應辦事項；例如，要求資安責任等級為 C 級之機關導入 CNS 27001 等資訊安全管理系統、每 2 年辦理核心系統之滲透測試、配置至少 1 位資通安全專責人員等。企業或許可以考慮依據自身不同業務的重要性，對應採取不同等級機關之應辦事項。

換言之，對最重要的業務及相關系統，企業或許可參考 A 級機關的應辦事項，對較不重要的業務，則採取 C 級或 D 級機關之應辦事項。同樣，企業可以在盤點出自身資通系統後，仿《分級辦法》附表九的精神，依各該系統於機密、完整與可用性等面向的重要性，對企業之資通系統依其

圖／歐新社

許多公務機關使用中的中國大陸廠牌監視器，已被要求限期汰除。

註 1、作者任職於行政院國家資通安全會報技術服務中心，本文為該中心「國際資安組織與法制政策研析」研究成果。

註 2、例如，於今年 (民國 110 年) 8 月 23 日，資安法之多項子法修正條文，方由行政院發布施行。

圖／總統府

今年 5 月 ， 蔡英文總統出席「CyberSec 2021 臺灣資安大會」，致詞中表示資安就是國安，也是台灣產業發展必須把握的關鍵領域。本次盛會共有超過 200 家國內外資安品牌參加，報名人數超過 1 萬人。

防護需求的高低加以分級，並參考《分級辦法》附表十的規定，對不同分級的系統採取不同的防護措施。

若企業對如何著手或落實執行尚無頭緒，行政院前已提供包括資通安全維護計畫範本等參考文件[3]，企業可以參考並依據自身需求修改後，據以執行。

二、與委外管理監督相關之規定

本文在上一節，提到《資安法》第 9 條及《施行細則》第 4 條對資通系統或服務委外，有要求委託人對受託人進行管理與監督之規定。 由於部分企業可能誤會委外後相關資安維護責任即轉嫁至受託人，針對這部分，本文在此稍作說明。

由於專業分工的趨勢，在資通訊領域內將業務委外十分常見，如網站代管、客戶服務委外等。不管是否為受《資安法》所規範之機關，凡屬組織業務，其相關之資安維護責任就會落在組織身上；在委外之情形，則必須由組織去管理、監督受託人，以確保受託人在受委託業務相關範圍，符合委託人之資安維護義務與要求。執行上，建議企業務必將相關管理監督之作為詳載於委託契約中，以避免日後執行時之爭議與困難。

關於委外監督，要特別提醒的是，倘若企業本身是受《資安法》上公務機關或特定非公務機關委託辦理資通業務之承商，則更須注意上述《施行細則》第 4 條的規定。機關可能會要求承商配合機關之監督稽核或其他監督作為 (此項要求通常會直接寫明在招標文件及雙方的契約文件內)；而受託業務之實際執行內容可能涉及國家機密時，機關會要求對承商執行業務人員進行犯罪紀錄等適任性查核；此外，企業如係受託客製化開發資通系統時，可能被要求對系統進行安全檢測或提交來源證明等。

對資通產品採用之特殊規定

資通產品或服務琳瑯滿目，即使有完善管理制度，若不慎採用了危害資通安全的產

註 3、行政院國家資通安全會報，範本文件，https://nicst.ey.gov.tw/Page/7DDA83CEE9EAB67E (最後造訪日 110 年 8 月 19 日)。

品，仍不免有機敏資料遭竄改、竊取之風險。 因此，今年 8 月 23 日修正前之《分級辦法》附表一至附表八，曾有一項針對公務及特定非公務機關「限制使用危害國家資通安全產品」的規定；此外，行政院針對公務體系 (包括公務機關及公營事業等) 另行要求禁用中國大陸廠牌產品的規定，均可供企業規劃資安維護或商業策略時參考。

以下就「原則禁用危安產品」與「原則禁用中國大陸廠牌產品」摘要說明如下：

一、原則禁用危安產品

修正前之《分級辦法》附表一至附表八之應辦事項中，均有一項關於禁止採用危害資通安全產品之規定。依據該規定，除非無替代產品且為業務所必須者，得另專案處理外，否則不得採購或使用危害資通安全產品[4]；企業也宜參考此措施之精神，購置較無風險疑慮的產品。

另一方面，企業如欲銷售或代理產品，且所規劃之銷售對象是公務機關或受資安法規範之特定非公務機關時，更務必留意對此類產品之認定。即使臺商銷售的對象不是上述機關，產品或服務一旦曾被認為是危安產品即相當於被認定有資安疑慮，顯然也會影響產品之銷售，日後甚至可能出現產品瑕疵或其他法律爭議，不可不慎。

二、原則禁用中國大陸廠牌產品

行政院於 109 年 12 月 18 日曾函請各公務機關於 110 年底前，完成汰換所使用或採購中國大陸廠牌資通訊產品作業[5]，先前已採購而未能立即汰換者，則須列冊管理並原則禁止與公務環境介接[6]。至於所謂中國大陸廠牌，指廠牌係屬依大陸地區法律設立登記之公司、合夥或獨資之工商行號、法人、機構或團體所擁有者而言；此分類係依據工程會 107 年 12 月 20 日工程企字第 1070050131 號函中針對「大陸地區廠商」的定義說明而來。

而資通訊產品，依《「盤點大陸廠牌資通訊產品」注意事項》之說明，則不限於硬體，亦包含軟體及服務[7]。依據上述注意事項，硬體方面只要「具連網能力、資料處理或控制功能者皆屬廣義之資通訊設備，如個人電腦、伺服器、無人機、印表機、網路通訊設備及可攜式設備及物聯網設備」均屬之；軟體方面，則包含套裝軟體與客製化系統；至於服務，則包括客服及軟、硬體資產之維護服務等。從上述說明歸納可知，盤點之產品係指機關本身可以辨識之終端產品為主，暫未考量產品內部之構成元件。

結論

由《資安法》而來的規定雖然不會直接適用於多數臺商與一般企業，但其資安防護的基本精神與作法則可供企業參考；透過了解法規要求之管理制度或相關措施之內容，調整並於企業內部施行，結合不斷精進的管理循環，應足以一定程度保護企業之資通系統或核心業務，避免事故發生或降低事故的不良影響。

臺商或企業若屬《資安法》規範之對象之承商，或主要銷售、代理包括軟、硬體及服務等中國大陸廠牌資通訊產品，則宜對於危安產品，以及針對公務體系的中國大陸廠牌產品禁用規定等，加以留意、提早因應。

最後，雖然《資安法》相關規定未針對一般民生用品加以限制，但因對危安產品等的認定及其衍生效應，及國際上對「乾淨供應鏈」的需求趨勢，企業之業務若包括銷售或代理此類產品時，勢必要留意，適時調整經營策略。

註 4、針對此一規定，行政院並另針對公務體系發布《各機關對危害國家資通安全產品限制使用原則》，以利相關機關執行時有更具體之依憑。

註 5、行政院國家資通安全會報，資通安全網路月報 (110 年 3 月)，110 年 4 月 20 日，https://nicst.ey.gov.tw/Page/8770AD7511CB8DC9/fd432cc0-8dab-4412-8d60-87fa3fd57105 (最後造訪日 110 年 8 月 19 日)。

註 6、行政院國家資通安全會報資通安全作業管考系統，「盤點大陸廠牌資通訊產品」注意事項，https://spm.nat.gov.tw (最後造訪日 110 年 8 月 19 日)。

註 7、同前註。