國家資通安全研究院
院長
何全德

跨領域整合　建構安全網

從資安防禦打造企業韌性策略

COVID-19加速各產業數位轉型，建置資安環境、打造數位韌性成為企業邁向數位永續的重要課題。國家資通安全研究院院長何全德過去曾在行政院研考會任職30多年，一手草擬政府資安管理制度，並建置電子化政府基礎建設，從政策制定者到擔任總統府第二局局長，負責資安實務，對資安工作有深刻的觀察與體會。

口述／國家資通安全研究院院長何全德　整理／張維君

政府投入資安制度的建立及部署已近30年，近年又受到《資通安全管理法》的規範，相信這些累積的資訊科技（IT）安全管理經驗能作為製造業在導入營運科技（OT）資安制度時參考。

網路攻擊愈來愈猖獗，企業必須提防供應鏈攻擊、物聯網及加密貨幣等風險，也是今年主要的資安趨勢。

以資安打造產業及數位韌性

AI、5G等數位科技，可以說是未來10年改變產業樣貌，同時帶來機會的重要力量，而資訊安全則是攸關數位科技究竟是阻力，還是助力的關鍵。近年產業，特別是製造業、半導體產業，面對地緣政治、供應鏈重組的風險，或是國際間對淨零永續的要求，都凸顯出數位科技對強化產業韌性的重要性，而資安作為科技基磐的角色更是無須贅言。

企業營運挑戰不只上述這些，由於臺灣向來是製造業重鎮，而製造業OT產線大多有不能斷線的需求，因此在面臨勒索軟體等各種網路攻擊時，企業擔心停工造成更大損失，可能會選擇支付贖金，這也是我們看到臺灣近年屢屢成為網路攻擊目標的原因之一。根據趨勢科技調查數據顯示，除了政府之外，製造業在駭客攻擊前五大目標中位居第二。

網路攻擊之所以如此猖獗，主要是網路犯罪已經商業化，犯罪集團不需要具備很高深、專業的駭客技術，在暗網已有很多的網路攻擊工具包在販售。加上AI人工智慧與機器學習等新技術的應用，或是API的使用增加也帶來新的入侵風險，例如利用AI協助找出軟體開發的漏洞，都能被駭客不當利用。此外，企業也必須提防供應鏈攻擊、物聯網及加密貨幣等風險，都是今年主要的資安趨勢。

最大風險就是「不知道有風險」

對製造業的作業現場來說，OT已IT化，許多機台設備已連網，安裝愈來愈多的感測器，並導入AI系統進行模擬分析，除了整個基礎設施數位化，包括使用者行為也已改變，工程師從現場機台操作轉為遠端連網操作。

製造業工廠在數位轉型的同時也暴露出許多弱點與風險。首先，在網路連線管理方面，許多業者未積極管理網路接口，沒有完整的盤點網路架構中有哪些連網設備。其次，由於產線設備的作業系統老舊，軟／韌體很少或無法更新，也都是安全隱憂。第三，遠距連線權限未能妥善管理。雖然在正常情況下不開放遠端連線，但發生緊急狀況時，可

能權宜允許合作廠商遠端連線進行故障排除，但排除後若未能恢復原先設定，經常因此產生入侵破口。

在物聯網方面，如今工控環境非常複雜，包括有各種主製程產線、製程數據感測系統、生產率回報系統等，但機台設備供應商通常不會開放最高存取權限，不允許企業安裝安全防護軟體或工具，雖然減少感染惡意軟體的機率，但卻導致無法安裝防毒等防護軟體。此外，工控系統設計初期可能缺乏身分認證和基本的加密防護功能，容易產生入侵漏洞。而製造生產系統的軟體更新速度較慢，且企業未能及時更新也很常見，或是基礎設施供應商以維持生產穩定為原則，偏好進行微小更新。另一項需要注意的是，許多工具韌體使用開源套件開發，這些套件往往存有過多弱點，導致用戶受駭。總體來說，最大風險就是「不知道有風險」。

製造業的作業現場，現在已有許多OT改為IT化，機台設備連網，安裝愈來愈多的感測器，並導入AI系統進行模擬分析等。

工控資安策略應參考國際標準

由於網路攻擊事件頻傳，為了鼓勵企業通報並快速掌握情資，金管會已要求上市上櫃公司需在重大資安事件發生後，在「次一營業日開盤2小時前」發布重大訊息。而金融業則須在重大資安事件發生後，30分鐘內通報金管會。因此，企業必須制定一套資安策略，並逐步落實。

在擬定策略之前，企業必須以風險管理的角度來看資安。資安不可能做到絕對百分之百零風險，而是須考量投入成本，思考投入多少資安預算能把風險降到最低，或是能接受的程度。一旦發生資安事件，企業要如何快速偵測、應變處理及復原，把損失降到最小，人力以及管理流程，都必須妥適規劃。而在風險評估方面，應該以資安事件發生機率高中低，以及事件發生時對資產影響程度高中低進行風險評估，事件發生機率高且衝擊影響高者優先處理，以抓大放小為原則來管理風險。

實際在擬定資安策略時，應參考國際標準，並且可以從攻擊方的角度來檢視企業本身防禦部署的強度以及偵測弱點所在，並評估人員技術及系統防護是否足夠。建議可參考非營利組織MITRE針對工業控制系統所推出的MITRE ATT&CK for ICS Matrix，這是以駭客思維來設計防禦策略，同時也可參考OWASP Cyber Defense Matrix

企業要轉換心態，將資安防禦視為打造企業韌性策略的一環，而非只是符合法規要求。

資安框架，以更全面地擬定防禦策略。

而經濟部也制定《工控物聯網共通性資安指南》，是以工控系統普渡模型Level 0－Level 5檢視OT／IT風險所在，並制定安全計畫、緊急應變處理等，同時也對應國際標準，如ISO 27001資訊安全管理系統、IEC 62443工控安全標準等，以上都是企業在制定對策時可以參考的標準與指引。

資安不是一個人的江湖

在OT資安策略制定上，儘管資訊長或資安長可能需要肩負80%的責任，其他落在廠長及OT人員身上，但是「資安不是一個人的江湖」，需要跨領域整合及協作，與供應商及其他部門單位共同努力，而取得企業高階領導的支持更是成功的關鍵。

俗話說：「格局決定布局，布局影響結局」，希望企業能轉換心態將資安防禦視為打造企業韌性策略的一環，而非只是符合法規要求。例如半導體龍頭大廠台積電的資訊安全宣言即強調，將資安與機密資訊保護視為對客戶、股東、合作夥伴及員工的承諾。從該公司的資安組織架構也可見其對資安的重視，其企業資安組織直接對總裁底下的資訊科技及資材暨風險管理資深副總負責，同時也對董事會底下的審計委員會報告。

對資安長來說，從落實法遵、人力籌劃與運用、經費配置、委外管理、組織資安治理，到新興科技風險管理等都是職掌範圍，亦需向董事會報告、對主管機關說明，以及在資安事件發生時決策建議要不要停機，挑戰可說非常重大。

數位韌性對企業或政府組織來說，已經是標配而不是選配，唯有建立起資安治理新思維，包括將資訊安全的流程設計，盡可能移到軟體開發前期，也就是所謂的「安全左移」概念；從源頭軟體品質做起，以駭客思維設計防禦工事，採用紅隊演練來檢視企業資安韌性，建立零信任資安架構以及公私協防等，才能充分發揮數位科技戰力，協助企業再新的世代轉型躍升。