零信任浪潮下
企業資安韌性的策略布局

Strategic Deployment of Corporate Cyber Security and Resilience in the Era of Zero Trust
ゼロトラスト前提のサイバーセキュリティモデル

文・圖／資策會MIC資深產業分析師　童啟晟

混合工作型態驅動企業信任邊界移動

COVID-19 疫情如同一場戰爭，衝擊全球的經濟、改變人類的工作與消費生活方式，企業生產形態也跟著變革，儼然形成人類社會發展的新常態（New Normal）。另一方面，企業資產大量轉換至數位賦能環境的現實狀況，更使得資通訊系統暨應用場景變得日益繁複；而萬物聯網亦提供了勒索病毒一個絕佳的進犯環境，及讓駭客攻其不備的機會。再加上資安攻擊態樣隨著防禦演變而改變，攻擊能見度愈來愈低，企業常有自己也看不到的死角，如異常登入行為、網路流量、惡意程式等。

此外，許多國外龍頭企業已紛紛採用混合上班的工作模式，但由於在公司上班與在家上班之間的界線逐漸模糊，資料外洩、VPN 的攻擊，層出不窮。然而隨著資料與服務雲端化、使用者行動化及存取裝置／設備多元化，傳統基於區隔為信任基礎的網路邊界已現資安窘況，實在難以滿足新形態工作需求。因此，企業的資安團隊必須採納屏棄傳統的單一面向解決方案，採取一套多層式（身分、裝置／設備、網路環境、應用程式、資料）的防禦計畫與策略，才能有效掌握任何潛在侵犯點，不讓駭客乘虛而入。

在今日的混合工作模式下，企業若假設所有內部流量都是安全的，就反而彰顯傳統網路疆域界定的資安困境。若能在 ICT 架構當中導入零信任的概念：「絕不信任、持續驗證（Never Trust, Always Verify）」，企業就能將未來任何網路攻擊的損害降至最低，而且不須犧牲使用者生產力，讓他們順利存取工作所需的企業資源。

企業提升資安韌性的方法與框架

美國國家標準與技術研究院（NIST）對「數位韌性（Cyber Resilience）」的定義：使用網路通訊資源或被網路通訊資源賦能的系統，在面臨敵對與不利的情況如壓力、攻擊、損害時，能夠預判、承受、適應及復原的能力。此能力旨在讓組織於競爭激烈的網路環境中，仍能實現其任與業務的目標。而大部分針對「數位韌性」的討論也常聚焦在承受及復原，即 NIST CSF（Cybersecurity Framework）框架所涵蓋的資安五大面向：識別（Identify）、保護（Protect）、偵測（Detect）、回應（Respond）及復原（Recover）。

而企業在真正著手打造數位韌性力之前，首先必須觀察所處的環境，即所謂的「衡外情」部分。其觀察的重點，

包括產業競爭的態勢如國際資安大廠與獨角獸／潛力新創所聚焦的資安解決方案；資安威脅的趨勢如跨域聯防、情資共享機制；主管機關法令政策的調整如上市櫃公司設置資安長暨專責單位與人力；及國際相關標準如資安治理（ISO 27002：2022）、軟體供應鏈安全（CMMC 2.0）與最佳實踐等，找出有哪些環境的變化可能對企業的營運造成衝擊，凸顯企業體質脆弱。

至於在所謂的「量己力」面向，可檢視企業內部的革新，例如從轉念意識（Awareness）至心態建立（Mindset）及執行訓練認知；再者轉骨，例如文化調適；最後為轉型：打造變革策略。而需要特別強調的是，這些徵候的原因或許有優先順序及強弱之分，例如產業競爭態勢與資安威脅趨勢的發生，會遠比主管機關訂定相關法令政策要來的早；但驅動企業改變建立韌性以應變的力量，卻遠比法令政策來的微弱許多。

數位轉型 vs 資訊安全，企業資安韌性策略

產業界多數認為的資安最佳實踐，涵蓋縱深防禦、合規要點及風控清單、縮小攻擊面，甚或擁有完善的資安產品暨服務等，都不能稱的上是所謂的策略。畢竟不錯的策略必須是可以衡量、可以清楚是否有朝著目標取得進展的計畫。以縮小攻擊面而論，當前網路環境中的任何裝置／設備都可能在未察覺情況下，被當作攻擊企業的資產，所以整個場景其實都是企業的被攻擊面，企業根本無從評估攻擊面是否已經變小了。

隨著更多企業將資產與關鍵資料移轉至雲端，倘若勒索病毒集團欲維持生存與獲利，勢必不得不隨之轉戰雲端。而前瞻2023年產業資安化趨勢，可以預見元宇宙（Metaverse）與非同質化代幣（NFT）的光環將會褪色；但其底層的區塊鏈技術，則勢必將成為駭客躲避追緝的避風港。過去Apache Log4j的漏洞事件，使得產業形成一朝被蛇咬，十年怕草繩的疑慮，對於開放原始碼軟體的信任依然存在著變數。

相對於企業的資安韌性的建構，不僅是將企業的資安防護不斷加強（防火牆如同河岸堤防的修築墊高），還得考慮遭受駭客攻擊之事實時，能做好事後的資安資源重新部署與再調配，及企業營運不中斷的「可持續性」（當堤防擋不住洪水時，沿河的居民要如何快速遷移，讓生活不因洪水而被中斷）。韌性關鍵即在於各產業資安的應變能力，沒有了資安，所有的韌性將無法在遭受變故時快速回復並提出因應機制（資安防護、資安管理、資安治理），可見資安對產業發展的重大意義。

許多企業的董事會已將資通安全視為業務風險，而非技術風險；但卻少有企業將資安防護看待為商業投資與布局。因此下個世代的資安防護核心，最終也將如同業務與資訊的數位轉型成為以資料驅動、AI賦能決策、軟體定義。同時也隱喻，資安長必須要與資訊長更密切的合作，思考如何搭配企業數位轉型的進程，將企業投資在數位轉型上的資源轉化運用於新世代的資安防護架構、發展及自動化作業上。

MIC AISP 網址：http://mic.iii.org.tw/AISP
著作權所有，非經資策會書面同意，不得翻印或轉讓。

以上研究報告資料係經由MIC內部整理分析所得，並對外公告知研究成果， 由於產業倍速變動、資訊的不完整，及其他不確定之因素，並不保證上述報告於未來仍維持正確與完整， 引用時請注意發佈日期，及立論之假設或當時情境，如有修正、調整之必要，MIC將於日後研究報告中說明。 敬請參考MIC網站公告之最新結果。