論述 》專論 · 評述

關鍵基礎設施的數位韌性挑戰與因應之道

當前臺灣關鍵基礎設施高度依賴數位技術，雖提升效率與服務品質，卻也暴露於日益複雜的網路威脅。面對勒索軟體與供應鏈風險，組織須建立動態風險管理制度，導入 ISO 22301 等國際標準，並透過預防、應變與恢復三階段的系統化演練，強化營運持續能力。韌性再進化不僅仰賴技術升級，更須跨界合作與創新思維，共同打造安全、彈性的數位未來。

邱述琛、廖彥鈞、宋玫蓁（安侯企業管理股份有限公司執行副總經理、執行副總經理、協理）

壹、前言

臺灣關鍵基礎設施依功能屬性區分爲八大領域：能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關及高科技園區，皆日益依賴數位技術來提升效率、降低成本並提供更優質的服務。然而，這種對數位化的依賴也帶來了前所未有的風險和挑戰，例如：醫療院所、政府機關、金融業再到台灣中油股份有限公司（以下簡稱中油公司）都持續受到勒索軟體攻擊的威脅，我們必須正視這些挑戰，並採取果斷的行動來強化關鍵基礎設施的數位韌性。

貳、數位轉型下的關鍵基礎設施：脆弱性暴露

一、效率與脆弱並行

數位化轉型，如同雙面刃，爲關鍵基礎設施帶來效率提升的同時，也暴露了其潛在的脆弱性。過去，這些基礎設施往往採用物理隔離的系統，網路攻擊的風險相對較低。然而，隨著物聯網（Internet of Things, IoT）設備、雲端計算和大數據分析的廣泛應用，關鍵基礎設施系統正變得越來越互聯互通，雖然提高了運營效率，

但也擴大了攻擊面，使之更容易受到網路攻擊。

二、新興技術與攻擊手法的演進

隨著AI（Artificial Intelligence）技術的發展，網路攻擊的威脅日益嚴重，攻擊手段更是日趨複雜，不法分子甚至無須高深技術即可造成嚴重威脅，而針對關鍵基礎設施的攻擊正在全球升溫，駭客不斷尋找和利用關鍵基礎設施系統的漏洞，一旦攻擊成功，就可能導致服務中斷與重要數據洩露，進而對社會造成嚴重影響，例如，2015年烏克蘭電網遭受駭客以惡意軟體攻擊，導致數十萬人斷電；2020年我國中油公司遭到綁架勒索軟體攻擊，服務大規模中斷，這就是十分令人警醒的案例。

三、眞實案例警示：攻擊的社會影響

關鍵基礎設施面臨的數位韌性挑戰中，供應鏈風險也是一個不容忽視的問題。關鍵基礎設施系統通常依賴複雜的供應鏈，涉及眾多供應商和承包商。任何一個環節的安全漏洞都可能影響整個系統的穩定性。例如，如果某個供應商的軟體被植入惡意程式，可能會感染使用該軟體的關鍵基礎設施系統，造成大規模的故障，並且惡意程式可能橫向擴散至所有與關鍵基礎設施相關連之主機及系統。

參、數位韌性建設：從防禦到快速應變與營運持續

一、建立動態風險管理制度：數位韌性的核心支柱

組織建立一個全面的風險管理制度是提升數位韌性的基石。這不僅僅是一份文件規範，而是一個持續進行的過程，須要對關鍵基礎設施系統定期進行風險評鑑，識別潛在的威脅、漏洞和弱點，並制定相應的應對措施，並且須確保執行風險評鑑前已針對最新的威脅情資進行更新，以便及時發現和應對新出現的風險，這個過程不應是靜態的，而是應該根據內外部環境的變化不斷調整和完善。

二、轉變思維：恢復營運持續能力

面對日益複雜和頻繁的網路攻擊，我們必須承認，百分之百的安全是不存在的。因此，我們必須轉變思維，建立快速恢復營運持續的能力，確保即使在遭受攻擊的情況下，關鍵基礎設施也能以最短的時間和最小的損失恢復正常運營。

提升關鍵基礎設施的數位韌性，不能再僅僅局限於傳統的「築牆式」防禦，而必須轉向一個更全面、更動態的策略，涵蓋從預防、偵測與告警、應變到恢復的整個生命週期。

（一）預防及偵測準備階段

首先，必須提前完善

備援系統或建立替代服務方案，並且設計「人工處理流程」，一旦發生緊急事件時，可立即啓動相應的備援計畫，確保服務不中斷。其次，對於資訊系統而言，定期進行系統漏洞掃描與入侵偵測是非常重要的。這能幫助我們及早發現潛在的安全威脅，應對日益猖獗的駭客攻擊和服務中斷風險。最後，當備援架構和流程規劃完善後，須根據事先制定的切換步驟，將標準作業流程（SOP）提前演練熟悉，不只資訊相關人員，更應涵蓋所有相關部門的員工，讓大家都知道應該如何應對，一旦眞正發生中斷時，能有效避免手忙腳亂。透過跨部門的協作訓練與事前演練，不僅能提升整體的應變能力，也能確保在危機時刻快速且有序地反應。

（二）應變階段

在「應變」階段，核心重點在於快速反應與明確分工，確保在事件發生的當下能立即採取有效行動。成立專責的應變小組是關鍵，包括技術修復人員，負責迅速定位並解決系統故障或安全事件；內部協調人員則負責統籌資源、訊息溝通，確保各單位間協作順暢；對外聯絡人則負責與合作夥伴、媒體或民眾溝通，維持企業形象與訊息透明。同時，還須要安排負責緊急疏散的團隊，以保障人員安全。透過明確角色分工與協同作戰，才能在危機中迅速掌控局勢，最大限度減少損失與影響。

（三）恢復階段

在「恢復」階段，首先，進行服務與系統的修復與驗證，確保所有資料完整、系統功能正常，恢復正常運作；其次，評估事件所造成的影響，不僅要考量對內部的影響，同時也必須衡量對民眾、企業以及社會秩序所帶來的衝擊，以全面了解事件的整體影響範疇；最後，進行改善與強化措施，包括進行系統升級以提升防護能力、優化應變流程，並擴大演練範圍，以降低類似事件未來再次發生的風險，確保組織的韌性持續提升。

三、提升數位韌性：導入國際標準與系統化演練

爲提升關鍵基礎設施的數位韌性，可同時參考國際標準 ISO 22301 的營運持續管理系統（Business Continuity Management System, BCMS），在制定和落實營運持續策略時，務必要將人員安全放在首要位置，確保在危機發生時能提供全面的保護與支援。同時，演練的規劃也要充分考慮資源的調度與分配，以確保在緊急情況下，能迅速動員人力、物資和設備，達到最佳的應變效果。系統化且符合國際標準的演練，不僅能有效提升組織的韌性，讓整體應變能力更具彈

性，也能保障業務的連續進行與人員安全。透過定期且符合國際標準的演練與持續改進，有助於建立一個更具彈性與應變能力的組織架構，有效降低風險影響，並確保在突發事件中能快速反應、及時應對。整體來說，這種標準化的管理流程與實務演練，既能提升組織的整體抗壓能力，也有助於達成長期的風險管理與持續改善目標。

肆、數位時代的基石：韌性再進化

在數位浪潮席捲全球的今日，關鍵基礎設施不僅是國家運作的命脈，更是經濟發展與社會穩定的根基。面對日趨複雜且難以預測的威脅，我們必須拋棄過往單純仰賴防禦的思維，轉而擁抱「韌性再進化」的理念，這不僅意味著技術及軟硬體層面的升級，更需要思維模式的徹底轉變，也須要持續學習與適應，如今的時代攻擊手法不斷演變，今日有效的防禦措施可能明日就已過時，因此鼓勵創新，支持新興安全技術的研發與應用，也是提升韌性的關鍵。

關鍵基礎設施的韌性再進化，更須要跨領域的合作與協作，政府、企業、學術界與廣大民眾都應積極參與，共同構建一個全方位、多層次的數位安全生態系統。政府應制定明確的政策與標準；企業應加大對安全技術與人才的投資；學術界應投入更多精力於研究與創新；而民眾則應提升安全意識。

「數位時代的基石：韌性再進化」不是一個口號，更是一種責任與承諾。讓我們以更積極、更開放的姿態，迎接數位時代的挑戰與機遇，共同打造一個更具韌性的數位未來。

參考文獻

1. 資通安全署－關鍵基礎設施資安防護，網址：https://moda.gov.tw/ACS/operations/ciip/650
2. 國家資通安全研究院－共通規範，網址：https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Common_Standards
3. 安華聯網－如何100％提升客戶信任度　導入ISO 22301循序落實企業永續經營目標，網址：https://www.onwardsecurity.com.tw/resource_blog-detail/iso22301_certificate❖