網路韌性：數位時代的核心能力

蔡永信

中華民國 114 年 7 月

作者任職於中央銀行資訊處，本文內容純屬個人意見，與服務單位無關，如有錯誤概由作者負責。

摘　要

隨著數位轉型的浪潮席捲全球，企業營運模式與服務型態日益仰賴資訊科技與網路系統，如雲端運算、大數據、物聯網及人工智慧等技術的廣泛應用，帶來前所未有的效率與創新，也使企業面臨更複雜且多變的網路安全威脅。以往的安全策略主要聚焦於防禦，較易忽略攻擊突破後的快速應變與復原能力，因此企業必須轉向強調「韌性」（Resilience）的策略，強調在遭遇攻擊時能迅速偵測、有效應變並快速恢復營運的能力。

網路韌性是系統在遭遇攻擊、故障或其他突發事件時，能夠持續保持核心功能並迅速恢復正常運作的能力，具備持續性、迅速恢復與自我調適 3 項特性。美國國家標準與技術研究院(NIST)網路韌性工程框架，結合系統安全工程與風險管理，開發出能夠在面對不利條件、攻擊與壓力下，依然持續、復原並調適能力的可信任系統，當無法完全防止攻擊時，仍能確保任務持續與快速恢復。

網路韌性的關鍵成功因素包含企業管理面因素，如管理階層的支持與治理結構、養成重視資安的文化、專業資安團隊與資源投入，以及零信任等新資安解決方案的採用，並透過持續演練與改進資安措施，打造動態韌性體系，以應對不斷進化的網路威脅，如 AI 驅動的深度滲透攻擊，克服新興科技帶來的安全挑戰，如量子破密等。未來網路韌性發展將朝系統全生命週期安全管理深化，從系統安全設計開始、運營階段持續監控，到事件回應與恢復，並於事後回饋與檢討改進。

投資於網路韌性建設不僅能有效降低風險與經濟損失，還能提升企業品牌形象、吸引投資並增強市場競爭力，成為當今數位時代，企業長期穩定發展的重要戰略支柱。

目次

壹、前言

隨著數位轉型的浪潮席捲全球，企業營運模式與服務型態日益仰賴資訊科技與網路系統，如雲端運算、大數據、物聯網及人工智慧等技術的廣泛應用，帶來前所未有的效率與創新。然而，伴隨而來的是日益普及且複雜的網路與數位設備，使得網路攻擊與安全威脅變得愈發多樣且高強度，企業正因此面臨更複雜且多變的網路安全挑戰。

根據全球網路設備大廠思科（Cisco）2022 年的報告指出，超過半數受訪企業在過去 2 年內遭遇過網路安全事件，並影響其業務營運，而最常見的事故類型為勒索軟體（49.1%）、分散式阻斷服務攻擊（DDoS，45.5%）、內部人員權限濫用（41.8%）及系統中斷（38.2%），這些事件不僅造成 IT 與通訊中斷，還嚴重損害企業品牌聲譽與客戶信任（資安人編輯部(2022 年 12 月 7 日)）。國際資安公司 Sophos 也指出，勒索軟體攻擊使近半數企業無法在一週內恢復正常運作（Sophos (2023 年 5 月)）。此外，市佔率居領先地位的端點偵測與回應軟體 CrowdStrike，其更新異常引發大規模藍白畫面事件，造成全球電腦大當機，更凸顯供應鏈依賴帶來的危機（羅正漢(2024 年 9 月 6 日)）。

一、台灣公司資安事件公布數量逐年成長

有鑑於資安事件對於台灣上市櫃公司營運的影響日趨重大，證交所與櫃買中心在 2021 年 8 月公告更新，有關上市（櫃）公司重大訊息的查證暨公開處理程序，將資通安全事件納入重訊發布的條件，其後更在 2024 年 5 月及 7 月，進一步說明資通安全事件之重大訊息定義，有關資安重訊發布條件主要是指「公司之資通系統、官方網站或內部文件檔案資料等，遭入侵、破壞、竄改、刪除、加密、竊取、服務阻斷攻擊（DDoS）等，致無法營運或正常提

供服務，或有個資、內部文件檔案資料外洩之虞等情事等」，不僅讓資通安全事件公告有更明確的標準，也能彰顯台灣上市櫃公司面臨的資安風險狀況。

因此，資安顧問公司勤業眾信在分析近 3 年(民國 111 年至 113 年)的所有重大訊息內容後(陳盈州、周哲賢與洪玉珊(2025 年 1 月 2 日))，發現民國 113 年資安事件重大訊息數量已超過民國 111 年與 112 年 2 年數量的總合，且資安事件數量從民國 112 年 11 月時就已開始上升(如圖 1 所示)，尤其是民國 113 年3月及5月證交所擴大重大訊息發布條件後，更呈現顯著上升趨勢。另外，由近 3 年的資安事件重訊統計可看出，每年資安事件的成長率皆翻倍式成長，其可能原因包含（1）上市櫃公司對於揭露資安重大訊息的意願上升；（2）整體上市櫃遭受攻擊的比率增加。

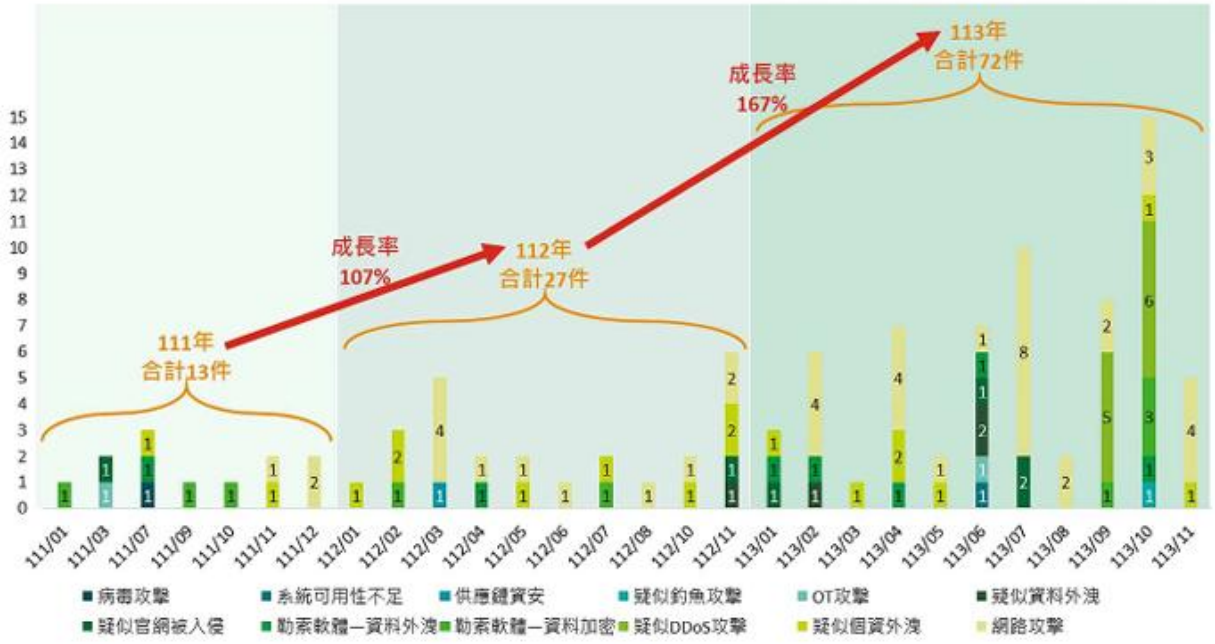

圖 1: 民國 111 年起至 113 年台灣上市櫃企業資安事件公告數量與成長率

二、安全策略的轉變

以往的安全策略主要聚焦於防禦，較易忽略駭客攻擊突破後的快速應變與復原能力，導致業務中斷及巨額財務損失，難以應對日益嚴峻的威脅。因此企業必須轉向強調「韌性」（Resilience）的策略，強調在遭遇攻擊時能迅速偵測、有效應變並快速恢復營運的能力。

網路韌性（Cyber Resilience）(或稱為網路安全韌性)已成為現代企業不可或缺的核心競爭力。它不僅是技術層面的強化，更涵蓋組織文化、風險管理、資源配置及持續改進的全方位策略。唯有建立完善的韌性架構，企業才能在瞬息萬變的數位環境中抵禦各種網路威脅，保障關鍵資產安全，維持業務連續性，並在危機中轉危為機，實現永續發展（范姜中岑(2024)）。

貳、網路韌性簡介

網路韌性的概念源於自然界的生態韌性（Holling, 1973），其強調系統在遭受劇烈擾動後仍能保持核心運作並自我調適。此概念後經 Holling (1996) 拓展至工程領域，主張系統應能迅速恢復並進行再組織。資訊安全領域的網路韌性，即是借鑑此核心精神，將安全策略從單純防禦，發展到全面應變與復原。

一、網路韌性特性

根據 Björck 等人（2015）進一步的研究與探討後，認為網路韌性是系統在遭遇攻擊、故障或其他突發事件時，能夠持續保持核心功能並迅速恢復正常運作的能力，並提出一個實用的定義：「在面對不利的網路事件時，仍能持續提供預期的結果的能力」。該定義超越了僅依賴防禦技術層面的思考，也可適用於不同的層級，包括：超國家（如歐盟）、國家、區域或城市、組織、商業功能（如業務流程）、技術系統（如 IT 架構），因此，網路韌性不

僅關乎 IT 系統，更關係到業務目標的達成、利害關係人的信任維護，以及關鍵資產的保護，並強調應變、復原以及持續自我優化的重要性。

Björck 等人（2015）強調網路韌性應具備以下三點特性：

●持續性（Continuity）：即使系統部分受到影響，關鍵服務仍保持運行；
●迅速恢復（Rapid Recovery）：在事故發生後，系統應以自動化或半自動化方式盡快恢復正常運作；
●自我調適（Self-Adaptation）：通過定期演練與數據分析，系統不斷學習並優化應變策略，進一步提升未來面對新威脅的能力。

有鑒於網路韌性非僅靠單一技術便能達成前述特性，而是需透過系統化與整合性地解構策略目標，藉此統合影響前述 3 項特性的技術與方法，美國國家標準與技術研究院(NIST)因此發布了網路韌性工程框架，旨在提供一套工程化的指南，以確保系統能夠有效地展現上述韌性特質。

二、網路韌性工程框架

NIST 針對如何建立具備網路韌性的系統，提出一套網路韌性工程框架(Cyber Resiliency Engineering Framework)(NIST SP 800-160 Vol. 2 Rev. 1)，該框架聚焦於網路韌性工程，即所謂的系統安全工程方法(System Security Engineering, SSE)，SSE 框架結合系統安全工程與風險管理，開發出能夠在面對不利條件、攻擊與壓力下，依然持續、復原並調適能力的可信任系統，強調當無法完全防止攻擊時，仍能確保任務持續與快速恢復。

SSE 框架可應用於各生命週期階段，包括新系統設計、升級、維運或系統下線，並且其設定的網路韌性應具備以下 4 大核心目標：

●預警準備(Anticipate)：維持「對逆境有充分準備的狀態」

此處逆境（adversity）包括自然災害、基礎設施故障（如停電）、高效能負載、網路攻擊、進階持續性滲透攻擊(Advanced Persistent Threat, APT)等，且應有完善的應變計畫，涵蓋威脅緩解、事件調查、供應鏈風險處置，而威脅情報更是預警準備的關鍵要素。

●承受能力(Withstand)：在面對逆境時，仍可持續執行核心任務或業務功能

即便未能偵測到攻擊，也應具備持續運作能力，尤其是 APT 攻擊活動可能未被察覺，或誤判為使用者錯誤。此外，需預先識別關鍵任務與其支援系統，並評估其重要性與可用性可能隨時間變動。

●復原能力(Recoer)：在逆境期間與之後恢復任務與業務功能

系統功能與資料的恢復可以是逐步進行的，困難點在於判斷恢復過程中的信任程度，且可能有其他威脅干擾恢復，APT 攻擊也可能藉混亂再次滲透系統，我們應有完善的應變計畫，涵蓋威脅緩解、事件調查、供應鏈風險處置。

●調適能力：因應技術、作業或威脅環境的預期變化，調整任務、業務功能或支援能力

預期變化可能為戰術或策略層級，需調整相對應的流程、程序或技術，而技術變化則有如 AI、5G、IoT 的出現。此外，企業組織作業環境的變更則可能來自於政策、法規或業務流程改變，故需進行這些變化的影響分析，以判斷是否改變攻擊面或引入威脅弱點。

SSE 框架是由目標、目的、技術、實作方法、設計原則，5 個構面所組成(如表 1)，具體說明如下：

●目標面是最上層的構面，定義系統在面對威脅與逆境時應達成的高層次能力。

●目的面是用來支援並落實每個目標的具體行動方向。

●技術面是指支援目標與目的的戰術手段與作法，如多樣性技術是指提升架構異質性，避免共同弱點、欺敵技術是指混淆、誘導或誤導攻擊者、非持續性技術是指動態配置資源、降低可攻擊面。

●實作方法面是用來實現每項技術的方法，方法需依據系統類型、威脅情境、任務需求而調整，如「欺敵技術」可實作誘捕系統蜜罐（honeypots）、虛假帳號、誘導性流量等。

●設計原則面可區分為策略性與結構性原則，用來支援架構設計與風險決策，如安全設計原則(Secure by Design)，指安全不是附加功能，而應從一開始就納入架構與設計決策中、縱深防禦原則，指採用多層次、多重機制來防止單一失效點造成整體崩潰、安全預設(Fail－Safe Defaults)，即系統在發生錯誤或未設定時，預設行為應為最安全狀態（如預設拒絕訪問），減少因配置錯誤或未預期情況導致的資安漏洞、模組化原則要求系統應分為獨立模組設計，降低相依性與影響範圍，以便於更新、隔離問題區塊、快速復原與彈性調整。

框架構面	說明
目標 （為何做）	預警準備、承受能力、復原能力、調適能力
目的 （要達到什麼效果）	共 8 項，包括避免、準備、持續、限制、重建、理解、轉型、重構
技術 （可採取什麼手段）	共 14 種，如多樣性、欺敵、非持續性、動態配置等
實作方法 （如何具體落實技術）	每種技術可對應不同實作方法，依情境彈性調整
設計原則 （提供設計思維）	安全設計、縱深防禦、最小權限、安全預設、模組化

表 1:SSE 框架構面整理表(Ross et al., 2021)

此外，美國國土安全部也開發網路韌性評估自我評量框架(Cyber Resilience Review, CRR），用以評估企業組織的網路韌性能力，該框架強調營運持續性與流程成熟度，而不僅是資安技術，其涵蓋準備、識別、保護、偵測、因應及復原六大面向、10 個領域，且每個領域會分成 5 個成熟度。企業組織可依據這些標準與框架進行自我評估，找出網路韌性不足之處，制定改進計畫，持續提升網路安全韌性(Cybersecurity and Infrastructure Security Agency. (n.d.))。

三、網路韌性與傳統資訊安全差異

以往的資訊安全策略多聚焦於防止入侵與阻止攻擊，強調如何確保網路安全，網路韌性則強調在不可避免的攻擊中維持業務連續性與快速復原，即

要求企業不僅建構堅固的防禦牆，更要建立快速偵測異常、有效回應與恢復的能力，確保關鍵業務不中斷。

我們可從目標、意圖、方法、架構與分析範圍來比較網路安全與網路韌性的主要差異(如表 2 所示)，網路韌性強調業務交付、容許失敗並恢復、從內部建立安全性、多層次防禦，並以企業組織間相互交織起的網路，作為分析資訊安全策略的範圍。

面向	網路韌性	網路安全
目標	確保業務交付	保護 IT 系統
意圖	容許可控失敗並恢復(Safe-to-fail)	避免失敗(Fail-safe)
方法	從內部建立安全性	從外部加以保護
架構	多層防禦與恢復機制	單層保護
分析範圍	從組織間的整體網路作為分析範圍(生態系觀點)	著重單一組織或系統的分析

表 2: 網路安全與網路韌性比較表(Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015))

四、網路韌性的多面向議題

NIST 新版網路安全框架 v2.0 強調，網路韌性是企業風險管理的核心，治理層應將資安風險與財務、聲譽等其他風險並列考量，依組織風險承受能力制定策略，網路韌性不僅是技術問題，更涉及組織文化、流程與治理。

因此，網路韌性是有多個面向的，技術層面有端點防護、網路安全等議題；組織層面則有治理結構、資安文化等；作業流程層面則有事件應變計

畫、災難復原等；人員層面則含括教育訓練、資安演練等，所以將各個面向有效率的整合，是提升企業組織整體抗壓與復原能力的關鍵。

參、建立網路韌性的關鍵成功因素

有鑑於企業組織的資源與人力有限，知道哪些因素對於建立網路韌性具有關鍵決定性影響，將使企業組織在建立網路韌性時更有效率，並且提升整體資源運用效能。

一、企業管理面

思科 2022 年研究報告《安全成果研究第三卷：實現網路安全韌性》，提到企業網路安全韌性的關鍵成功因素，成功因素不僅是技術問題，也強調組織領導、企業文化、資源安排與組織韌性，這些因素共有 7 大項(Cisco Systems(2022))。

(一)管理階層的支持與治理結構

管理層的積極參與與資源投入是提升韌性的首要條件。管理層應明確資安責任，將韌性納入企業治理與績效考核，確保跨部門協作與資源充分配置。建立跨部門資安治理架構，設置CISO職位，成立資安委員會，定期審視資安策略與風險評估，確保策略與業務目標一致。

(二)養成重視資安的文化

養成高度重視資訊安全的企業文化，能有效提升員工資安意識與行動力，降低企業內部威脅風險，且應定期舉辦資安教育訓練與模擬演練，建立相關激勵機制，以鼓勵遵守資訊安全的行為。

(三)專業資安團隊與資源投入

企業組織應擁有專責資安團隊與足夠資源，方能快速偵測與回應事件，進而縮短停機時間，並降低整體損失，除此之外，也應與外部資安機構保持合作關係，藉以獲取最新威脅情報，以及技術支援，提升企業網路安全準備的妥善率。

(四)雲端策略與混合環境管理

混合雲環境(使用至少 1 個地端環境或私有雲，和 1 個公有雲)管理複雜度高，企業應採用統一管理平台與自動化工具，降低錯誤與漏洞風險，提升環境一致性與安全性，且該報告顯示若混合雲環境複雜度高，會使企業網路安全韌性評分下降 8.5%至 14%。

(五)採用零信任架構

零信任架構強調「永不信任，始終驗證」，實施多因素認證、微分段網路與持續監控等機制，能有效防止內、外部威脅的橫向擴散與損害擴大，該報告顯示，採用零信任架構，可提升企業網路安全韌性評分達 30%。

(六)採用延伸偵測與回應

延伸偵測與回應(Extended Detection and Response, XDR)是一種將多個安全技術整合在一起的資安解決方案，該方案整合多端點、網路與雲端資料安全等多種技術，利用 AI 與自動化提升威脅偵測與事件回應效率，該報告指出使用 XDR 的企業，網路安全韌性評分將提升 45%。

(七)採用安全存取服務邊緣架構

安全存取服務邊緣(Secure Access Service Edge, SASE)一種架構模型，將網路連線與網路安全功能整合於雲端平台，企業能夠為任何位置的使用者，提供更簡單、安全和統一存取控制與威脅防護，並支援遠端與混合辦公環境，該報告指出企業組織採用 SASE，可提升網路安全韌性評分 27%。

二、持續演練與改進—打造動態韌性體系

隨著網路攻擊手法日新月異，企業組織應透過定期資安演練，檢視相關應變能力是否足夠，以期在網路攻擊事件發生時，能迅速反應並有效處置。此外，我國國家資通安全研究院近年亦推動關鍵基礎設施攻防演練場域的建置，透過模擬演練，提升關鍵基礎設施資安人員的實戰能力。

(一)演練的重要性與目標設定

為使資安演練能達到預期效果，有效增進企業組織對於資安事件的應處能力，演練的核心目標應放在：

- 強化團隊協作與溝通效率。
- 檢視現有應變計畫的可行性與漏洞。
- 提升員工對資安事件的警覺性與實戰能力。
- 測試技術系統的恢復速度與穩定性。

透過演練有助於跨部門溝通、快速決策、減少錯誤判斷，並驗證資安事件應變與處置標準作業程序的可行性，其中定期演練能提升資安團隊與高層應變信心，更能有效縮短資安事件回應時間，從而降低營運中斷的風險。

(二)多元演練類型與設計原則

企業面臨的威脅面與內部運作複雜度各不相同，故必須從自身真實需求考量演練類型，透過風險評估與組織規模分析，在演練目標、資源投入與難度設定上取得平衡，避免「一刀切」或「過度動員」的情形，演練類型可分為：

●桌面演練：以會議討論的方式，模擬資安事件流程，檢視決策與溝通，適合跨部門策略協調練習。

●實地演練：模擬真實攻擊場景，檢驗技術與人員反應。

●無預警演練：測試團隊突發事件反應能力，發現潛在漏洞。

●紅藍隊演練（Red Team/Blue Team）：紅隊演練不僅是測試防禦機制，更是協助藍隊發掘潛在弱點的關鍵手段，透過攻防對抗，提升藍隊防禦與偵測能力。

演練設計原則應遵循「逼真性」，模擬情境應高度應還原真實攻擊，增加應變的真實度、「安全性」，演練過程不得影響營運系統之可用性與業務連續性、與「可評估性」，演練必須便於後續分析與評估（如回應時間、偵測率、復原效率），並能產出具體改進報告，實施改善措施，如此一來，方能確保演練既具挑戰性又不危害業務運作，達到演練效益。

(三)演練流程與評估機制

演練前需制定詳細計畫，包括目標、範圍、角色分配與溝通機制。演練中，應即時記錄事件處理流程與問題點。演練後，召開回顧會議，分析成功與不足，制定改進計畫並納入例行管理（Ctlm (n.d.)）。

(四)持續改進與文化培養

演練不應是一次性活動，需將其納入企業治理體系，形成持續改進循環。透過定期演練與教育訓練，培養全員資安意識，建立安全文化，提升組織整體韌性。

肆、挑戰和未來發展

雖然網路韌性強調「在受到攻擊的情況下，仍能自我回復能力」，看似雲淡風輕的一句話，實則要能預期諸多可能發生的攻擊情境，建構出相對應的回復能力，即需考量可能面臨的威脅與挑戰，因此，了解網路威脅與未來發展趨勢，才能有效應對這些挑戰，提升建立網路韌性的效能。

一、網路威脅趨勢與韌性挑戰

隨著網路攻擊的自動化、快速化、與複雜化，新科技供應鏈攻擊日趨嚴重，國際資安合規要求日趨嚴謹，適格的資安人才短缺，新威脅與架構需求增加企業組織成本，影響韌性策略持續性，於此種種都對網路韌性帶來諸多嚴峻挑戰。

(一)AI 驅動的深度滲透攻擊威脅

2025 年，人工智慧（AI）技術已成為網路安全領域的雙面刃（Check Point. (2025)、INSIDE (2025 年 2 月 28 日)），一方面，駭客利用生成式 AI（GenAI）製作更具迷惑性的釣魚郵件、深偽影片及語音偽造，使 AI 成為社交工程攻擊的核心動力，並從輔助工具進化到能自主發起釣魚、勒索與深度滲透攻擊，對企業安全造成更大挑戰。同時，AI 也被廣泛應用於威脅偵測、行為分析與自動化回應，極大地提升企業對複雜攻擊的辨識與防禦能力，透

過融合雲端、邊緣與多雲防護於單一平台，將 AI 自動化威脅情報與風險評估機制導入其中，方能因應 AI 驅動的複雜攻防戰。

(二)新興科技帶來的安全挑戰

新興科技帶來的安全挑戰中，以量子計算技術帶來的威脅最大，在後量子運算時代的威脅，隨著量子計算技術的逐步成熟，現有傳統加密技術的安全效能將受到嚴重挑戰。企業必須提前進行技術轉型，部署抗量子加密演算法，確保設備或系統的加密敏捷性(Cryptographic Agility)，以確保在未來新型計算環境中關鍵數據依然獲得可靠保護。

(三)供應鏈攻擊與韌性建設

駭客透過軟體供應鏈、服務供應商等弱點發動攻擊，造成大規模影響，供應鏈攻擊成為全球資安事件的主要威脅之一。因此，企業必須加強第三方風險管理，建立多元供應商策略，並推動供應鏈透明化與持續監控，提升整體供應鏈韌性。

(四)法規合規與數據主權

全球資安法規日益嚴格，如歐盟 NIS2 指令、DORA 法案、美國 PCI DSS 4.0 標準及英國網路韌性法案等，皆要求企業強化資安防護與韌性措施。另一方面，資料主權議題將促使企業將部分資料移回本地端，以確保合規與風險控制（CipherTech, 2025），資料可用性與資料主權的拉扯張力，將使韌性規劃更加複雜。因此，企業結合法律、技術與流程，建立完善的合規管理體系，以降低法規風險的同時，也要能確保網路韌性。

(五)資安人才短缺

資安人才短缺已成為全球挑戰，企業除了須投入更多資源，進行資安教育與培訓，打造跨領域團隊，更要在如此激烈競爭的市場環境中，招募、培訓與留任相關專業人才，勢必增加企業運營成本，也可能帶來難以快速擴充或升級安全能力的負面效果。

二、未來網路韌性發展趨勢

(一)全生命週期安全管理深化

隨著網路攻擊日益頻繁與多樣化，企業需將安全管理從「事前預防」提升至「全生命週期」範圍，其範圍如下：

●設計階段安全：在產品與系統設計之初，嵌入威脅模型與韌性需求。

●運營階段持續監控：透過 AI/ML 強化異常行為分析，實時調整防禦策略。

●事件回應與恢復：結合資安協作自動化應變(SOAR)與自動化備援，縮短平均復原時間並不斷優化流程。

●事後回饋與檢討改進：建立 PDCA(Plan, Do, Check and Action)循環，將資安演練與異常事件教訓融入下一輪設計。

(二)安全存取服務邊緣與零信任的整合

安全存取服務邊緣理念，是將網路與安全功能融合至雲端平臺，實現「任何用戶、任何設備、任何地點」的安全瀏覽，而零信任資安策略，是動態授權與持續驗證替代傳統邊界防禦，兩者結合，透過雲原生安全技術，將安全功能隨服務遷移至雲端，以提升可擴展性與敏捷性，可有效提升網路韌性能力。

(三)人工智慧自動化的廣泛使用

未來網路韌性體系將更加倚賴 AI 與自動化。在自動化更新管理方面，AI 預期將能達到自動檢測漏洞並推送修補，縮短弱點曝險的時間。其次是人工智能運維方面，自動故障預測與自我恢復機制，將降低人工干預需求。

(四)供應鏈與生態系統韌性

隨著供應鏈攻擊頻繁發生，網路韌性勢必需拓展至企業組織的生態系統，以確保整體企業組織網的安全，這需要評估供應商的網路韌性，將供應商納入韌性指標體系，定期審計以達成企業組織網的安全。透過進一步建立行業聯盟，跨企業甚至是跨國協同合作，共享威脅情報與應急資源，以提升整體行業生態系的網路韌性。

伍、結語

網路韌性作為數位時代中維持系統核心功能安全的關鍵能力 ，其核心在於系統遭受攻擊、故障或其他突發事件時，仍能持續運作並迅速恢復正常 。本報告深入探討了其基本特性、NIST SP 800-160 工程框架所提供的具體技術與管理措施 ，旨在建立一套全生命週期的韌性體系，以有效應對不斷演變的網路安全威脅。總結來說，可分為以下幾點：

●全生命週期管理不可或缺

面對日益複雜的攻擊環境，僅依賴事前防禦無法有效應對風險，企業必須通過全周期管理實現快速復原與持續優化。

●跨部門與跨國合作至關重要

全球資訊安全威脅的跨國性要求建立統一標準與資訊共享平臺，形成協同防護的聯合作戰體系。

●前瞻性技術與動態調適策略

AI、量子計算、IoT 及 5G/6G 等新興技術的迅速發展，要求企業提前部署前沿技術並結合動態調適策略，確保網路安全體系能夠動態應對新型攻擊。

●企業競爭力與永續發展的基石

投資於網路韌性建設不僅能有效降低風險與經濟損失，還能提升企業品牌形象、吸引投資並增強市場競爭力，成為企業長期穩定發展的重要戰略支柱。

透過達成網路韌性這一戰略目標，企業組織在數位時代中便能確保其系統核心功能的安全性，進而在變動的環境中保持領先地位與競爭優勢。

參考文獻

資安人編輯部(2022 年 12 月 7 日)。網路安全韌性成台灣企業首要考量：7 大成功要素。資安人科技網。取自 https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10227

Sophos (2023 年 5 月)。The State of Ransomware 2023。取自 https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf

羅正漢(2024 年 9 月 6 日)。 CrowdStrike 軟體更新出包導致大量電腦當機。IThome。取自 https://www.ithome.com.tw/news/164836

陳盈州、周哲賢與洪玉珊(2025 年 1 月 2 日)。統計上市櫃重大訊息 看資安對於內部控制制度革新之必要。Deloitte。https://www.deloitte.com/tw/tc/services/audit-assurance/perspectives/2025-outlook-audit-1.html

范姜中岑 (2024)。政府資訊系統數位韌性。國家資通安全研究院。取自 https://www.nics.nat.gov.tw/core_business/digital_resilience/Digital_Resilience_Materials/

Holling, C. S. (1973). Resilience and stability of ecological systems. Annual Review of Ecology and Systematics, 4, 1–23.

Holling, C. S. (1996). Engineering Resilience versus Ecological Resilience. In P. E. Schulze (Ed.), Engineering within Ecological Constraints (pp. 31–43). National Academy Press.

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience–fundamentals for a definition. In New Contributions in Information Systems and Technologies: Volume 1 (pp. 311-316). Springer International Publishing.

Ross, R. , McEvilley, M. and Oren, J. (2016), Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=922194 (Accessed June 29, 2025)

Ross et al.. (2021). Developing cyber-resilient systems : A Systems Security Engineering Approach.Retrieved from https://doi.org/10.6028/nist.sp.800-160v2r1.

Cybersecurity and Infrastructure Security Agency. (n.d.). Cyber resilience review (CRR). U.S. Department of Homeland Security. Retrieved from https://www.cisa.gov/resources-tools/services/cyber-resilience-review-crr.

Cisco Systems. (2022). Security Outcomes Report Volume 3: Achieving Security Resilience. Retrieved from https://www.cisco.com/c/en/us/solutions/security/outcomes-report.html.

Ctlm. (n.d.)。企業如何建構職災防護計畫？完整指南：風險評估、教育訓練與演練全攻略. 爵鼎企業顧。取自 https://ctlm.com.tw/%E4%BC%81%E6%A5%AD%E5%A6%82%E4%BD%95%E5%BB%BA%E6%A7%8B%E8%81%B7%E7%81%BD%E9%98%B2%E8%AD%B7%E8%A8%88%E7%95%AB/

Check Point. (2025)。2025 年網路安全報告。取自 https://engage.checkpoint.com/2025-cyber-security-report-tw/items/report-cyber-security-report-tw-202

INSIDE (2025 年 2 月 28 日)。預測釣魚行為、彌補資安人才缺口：Check Point 的 AI 網路安全攻防。取自 https://www.inside.com.tw/article/37662-ai-in-cybersecurity

CipherTech. (2025). 2025 年資料安全預測：將「保護」與「韌性」置於核心。取自 https://www.ciphertech.com.tw/all_news/products_news/imperva_news/data-security-predictions-2025/