

專訪數位發展部資通安全署署長蔡福隆

國家級防護戰略 落實全社會資安韌性

採訪／林振輝、施鑫澤 文／鄭宜芬

數位發展部資通安全署自 2022 年成立以來，做為臺灣推動資安政策與防護體系的核心角色，不僅承接國家資通安全發展方案的推動任務，同時也肩負修訂《資通安全管理法》、健全資安治理架構的重要使命，積極提升國家數位韌性。

資通安全署為數發部所屬三級機關，主要負責國家資通安全政策的規劃、執行與督導，包含政府機關與關鍵基礎設施的資安防護、演練與稽核，以及資安事件通報與應變機制的建置。

數位發展部資通安全署署長蔡福隆表示，政府推動資安政策的架構，於行政院設有「國家資通安全會報」，統籌協調各部會的相關資安工作。近期工作重點主要有兩大面向，一是推動國家資通安全發展方案，二是推動資安法修法。

他指出，今年規劃之第七期國家資通安全發展方案有三大目標：

一是強化全社會資安防禦韌性，建立國家型緊急應變機制；

二是豐富資安產業生態系，推動自主研發核心技術、驗證產品合規及促進產業規模化；

三是構築新興科技防禦技術，利用 AI 於防護及演練、並關注量子破解非對稱式金鑰加解密的衝擊。

隨著地緣政治風險與新興科技威脅加劇，臺灣的資安挑戰日益複雜。資安署透過跨部會協調、公私協力及國際合作，強化關鍵基礎設施的防護與演練，並積極導入 AI 與新興資安技術，建構多層次的資安聯防網路。

跨部門合作 強化跨域資安合作網絡

在跨部會與產官學合作方面，資安署依循「國家資通安全戰略 2025」，訂定「國家資通安全發展方案（114~117 年）」。

蔡福隆進一步說明，政策面規劃四大策略，包括：

一、建構全社會資安防禦韌性：系統性的擴大資安人才培育，逐步建構全社會資安防護網，以完善國家資安應變機制。

二、提升關鍵基礎設施（CI）資安防護及韌性：工控系統安全將是重要挑戰，將透過建立資安防衛體系，加強工控系統人員培訓，增加關鍵基礎設施構面專家，落實領域基準，以提升關鍵基礎設施工控系統防護能量。

三、壯大我國資安產業：透過政策與法規的完善來擴大國內業者商機及確保網通及資安產品安全，並與數產署合作來鼓勵業者自主研發資安產品或解決方案。

四、AI 新興資安科技應用及合作：將致力加速推動資安產業及產業資安的 AI 化等及深化國際資安合作、交流及結盟。

在法規面上，資安署修訂「資通安全管理法草案」，包含擴大稽核範圍，增訂納管機關對於危害國家資通安全產品有關下載、安裝或使用之相關規範，

數位發展部
資通安全署

Administration for Cyber Security, moda



數位發展部資通安全署署長蔡福隆表示，我國資安政策推動的架構，於行政院設有「國家資通安全會報」，統籌協調各部會的相關資安工作，主要透過兩個面向推動資安政策，一是推動國家資通安全發展方案，二是推動資安法修法，期以提升我國整體數位韌性。



蔡福隆從金融業轉戰全國資安政策推動的關鍵角色，主要負責制訂與執行資安防護政策，推動跨部門協調與相關法規修訂，以提升政府部門資訊安全防護能力。

以及增訂強化資安人員之專業知能及重大資安事件之調度支援等規定。

面對日益嚴峻的資安挑戰，資安署亦透過公私協力，與資安院共同營運**台灣電腦網路危機處理暨協調中心（TWCERT/CC）**，將國內外資安情資分享給會員，協助企業儘早防範資安威脅。並就重大資安事件，主動聯繫協助受駭企業，降低損害影響。

為提升現職公務人員具跨資安職能專長，加速擴增政府資安人力，資安署推動「**政府資安人力職能轉換訓練計畫**」，配合大專校院等訓練機構，辦理現職公務人員轉換資訊處理職系訓練課程，建構長期教育訓練政府資安人才能量。

尤其關鍵基礎設施（Critical Infrastructure；CI）是中國長年攻擊的目標，資安署推動跨關鍵基礎設施聯合防護，結合中央目的事業主管機關串連 CI 提供者進行領域資安防護，銜接國家層級進行橫向跨域聯防，形成「**三層式資安聯防架構**」，以減緩 CI 受資安攻擊致營運中斷的影響，強化整體國家安全。

目前已建置國內層級及各 CI 領域層級之**資訊安全監控中心（SOC）**、**電腦緊急應變小組（CERT）**及**資訊分享與分析中心（ISAC）**等聯合防護機制，以系統化及制度化方式，進行事前資安情資掌握及傳遞、事中通報及應處、事後情資整合分享與應用等，建構完整的防禦陣線。

關鍵基礎設施 打造多層策略與聯防體系

關鍵基礎設施做為國家維持運作所需的基本設施

與服務，是駭客長期潛伏攻擊的目標。「最弱的那一環，就是你最大的風險。」蔡福隆強調，關鍵基礎設施的防護不容許出任何差錯，資安防護策略與預警機制的多層面措施，包括檢測、三道防線策略、演練模擬、外部曝險檢測及防駭分工等。

首先，針對資安法納管機關之資安防護，包含 CI 提供者及業務涉及 CI 事項之公務機關，應符合其資通安全責任等及要求，訂定、修正及實施資通安全維護計畫，及辦理相關資安防護（如：資安檢測、布建資安設備與防毒軟體及威脅偵測理機制等防禦措施）措施、內部資安稽核、資通安全管理系統導入或協力廠商驗證等應辦事項。且依法規要求，亦應負有資安事件通報及受稽核義務。

資安三道防線策略包括：

第一道自我保護，如資料加解密、應用程式與作業系統安全、授權管理；第二道防火牆、IPS、WARF、監控系統、及微網段切割管理；第三道制度化，如 ISO 27001、內部控制規範等。

為提升防護效能與應變能力，主管機關及各 CI 領域主管機關依規應規劃及辦理相關演練，如社交工程演練、事件通報及應變演練、情境演練及網路攻防演練等。

萬一遭駭，據「資通安全事件通報及應變辦法」，資安法納管機關**知悉事件後一小時內**應依進行通報，且限時完成損害控制或復原作業，並持續進行資安事件調查及處理。

除此之外，整體資安聯防也至為關鍵。數發部偕同各 CI 領域主管機關整合資安防護資源，建立國家資訊分享與分析中心（ISAC）、資通安全通報應變（CERT）及資訊安全監控（SOC），並結合 TWCERT/CC 資源強化我國聯防體系，分享所接收之國內、外資安情資予各主管機關，掌握近期資安趨勢及資安事件預防與應處經驗，加強各域資安管理及防護作為，提升整體資安防護強度。

資安投資轉為企業競爭力

TWCERT/CC 跨域合作

過去企業主多將資安視為成本支出，歷經頻繁重大攻擊後，現已將資安做為企業經營的重要投資之

一，「現在若不投資資安，以後會付出更大的錢，要付贖金。」

蔡福隆表示，TWCERT/CC 為我國針對民間企業資安事件通報、事件諮詢及協助服務之窗口，鼓勵民間中小型企業加入。我國資安聯防體系透過與 TWCERT/CC 合作，交流各跨域威脅資訊、分享國內外情勢，並提供公私領域資安事件預防及應處經驗，加強各界資安管理及防護作為，鞏固公私領域資安聯防體系。

他進一步建議，企業應在法治環境下兼顧實際運作與資安投資責任，避免負面影響產業發展。如**臺灣企業資安投資抵稅**已於 2022 年上路，大型企業也可利用工會及供應鏈資安聯盟（如 SEMI E187）帶動供應鏈與整體產業資安提升；另外，企業也可將資安韌性列入 ESG；另可由金管會推動、證交所與櫃買中心所擬的管控指引，強化上市櫃公司的資安能力。

資安治理與管理並重 加速防護與演練升級

資安長作為企業資安治理的核心角色，必須依據董事會的指令，爭取資源、制定計劃，並進行跨部門協調。當發生資安事件時，如何快速因應，將風險降到最低，是這個高風險職位的重要責任。

「演練宛如招式，工具是武器，而治理就是內功。這種最基本的內功，如今已愈來愈受到重視。」蔡福隆指出，「**資安治理**」以風險導向與策略發展為核心，涵蓋資安工具、演練、防禦與資料治理；而「**資安管理**」則著重於日常監控與防禦，例如防火牆與 WAF 設置、駭客入侵監控，以及攻擊事件數量等 KPI 的管理。

他舉例，近年金融業頻繁遭受駭客攻擊，金融業必須以風險導向為基礎，因此建議企業採取資安預防措施與超前部署，確保能在事件發生前，提前一週甚至三個月前就有明確的布署與因應計劃。

此外，模擬真實情境也相當重要，必須在演練中藉由實際情境模擬降低突發風險。在面臨 DDoS 攻擊等資安事件時，需有完善的復原方案與 SOP。至於資安健診、弱點掃描與網路架構檢視等，各有其重要性，唯有兼顧各項檢測，才能全面強化網路安全。

資安政策藍圖 提升我國整體數位韌性

為推動政府機關資安治理制度，資安署除持續精進修正《資通安全管理法》及相關規範，全面提升各級政府機關資安防護整備，並依「資通安全責任等及分級辦法」規定及國家資通安全發展方案策略，資安防護等級 A 級、B 級公務機關及關鍵基礎設施提供者，每年應辦理資安治理成熟度評估作業。

然而，從最近一年評估結果發現，多數機關於推動資安治理過程中，在技術面的管理上尤其面臨較大的執行困難，蔡福隆歸納其尚需努力的共通方向如下：

- 一、建立明確且具體的方法或指引，藉此加強資通系統的源碼及 SBOM 安全管理；
- 二、針對資通系統的作業環境，明確區隔開發環境、測試環境及正式作業環境，藉此降低網路不當連通或權限管理不當的資安風險。

而為協助機關持續強化資安治理與管理措施，資安署將針對不同規模的組織，辦理職能訓練及增能訓練，完善資安人才教育訓練生態系，有效落實資安管理制度。

職能訓練部分，資安署推動「**資安職能訓練發展藍圖**」，開設資安職能訓練課程，協助各級公務機關資安專職人員建立所需之專業能力；增能訓練方面，每年透過資安人員專業訓練、稽核員訓練、實戰技術工作坊、菁英人才班等，助力政府機關與關鍵基礎設施提供者，強化資安人員的實務能力。

未來，因應國際資安標準規範發展趨勢，資安署偕同資安院院持續訂定相關資安參考指引提供政府機關與機構參考，以加強資通安全防護，確保資通系統與資料之機密性、完整性及可用性。

在具體措施上，如推動 AI 與量子技術於資安防護與演練中的應用研究；同時標準化技術檢測工具與流程，擴大檢測範圍；加速零信任安全產品的驗測與推廣，以建立更完善的資安生態體系，提升我國整體數位韌性。