數位發展部
Ministry of Digital Affairs

數位經濟：資安產業
2024-2026 資安產業人才需求推估調查

【調查執行單位】資策會數位教育研究所

數位發展部數位產業署

112 年 12 月

目 錄

一、調查範疇

本年度調查對象包括在臺灣提供資訊安全產品和服務的廠商，參考 IEK《2021 年臺灣資安產業調查報告》及《2022 年臺灣資安產業產銷調查與現況》之定義，將臺灣資安產業分為三大類，包含資安防護、資安營運與資安支援。本調查旨於瞭解國內資安產業在資安專業人才之需求，以建立適切的人才培訓計畫，降低國內廠商對於專業人才的需求落差。

表 1 資安產業調查範疇表

行業標準分類代碼	6201 電腦程式設計業、6202 電腦諮詢及設備管理業、6209 其他電腦相關服務業、6311 入口網站經營業、6312 資料處理、主機及網站代管服務業、6390 其他資訊服務業
調查產業說明	本調查根據 IEK 定義之《臺灣資安產業範疇與分類》，以臺灣提供資安防護、資安營運及資安支援等資安相關產品及服務之廠商為調查對象。
問卷調查說明	總計回收 90 份有效樣本（含中華資安國際、神盾、華電聯網、數位資安系統、光盾資訊科技等企業），回收率 25.71%，調查樣本營業額約佔總體營業額約 18.62%。
深度訪談說明	深度訪談廠商共 8 家，分別為互聯安睿、中華龍網、趨勢科技、捷而思、網擎資訊軟體、中華資安國際、安碁雲架構服務、大同世界科技訪談對象為董事長、執行長、總經理、副總經理等。

資料來源：行政院主計總處，本計畫整理。

二、產業趨勢對人才需求影響

近年來，數位經濟的快速發展帶動了各個產業迎向跨世代、跨境、跨領域的趨勢，物聯網、人工智慧等數位創新科技的廣泛應用已對生活各層面，甚至整體經濟活動產生重大變革，然而，數位技術的新興發展也伴隨著嚴重的資安挑戰。

駭客利用人工智慧增強其攻擊手法，以及物聯網裝置應用的複雜性使得資安防護變得更加困難，此外 5G 網路的廣泛部署帶來了新的網路安全挑戰，加劇了資安威脅的嚴重性。資訊安全已經成為一個至關重要的議題，不僅對個人、企業，也對政府機構產生重大影響。這增加了我們對資安專業人才的需求，以應對這些新興威脅並確保各方的數據和資訊得到適當的保護，因此，培養和招聘資安專業人才是當前的迫切需求。

正因如此，無論是公部門、民營機構、大型企業或中小型企業，對於具有資安專業知識和技能的人才皆有迫切需求，期望這類型的專業人才協助規劃、建立和維護有效的資產和資訊安全防護措施，以確保各組織能夠有效地應對不斷增長的資安挑戰。

有鑑於此，本計畫透過展開臺灣資安產業人才需求調查，以了解資安人才現況、關鍵職務職能、培訓需求及未來應用發展等。本調查報告背景說明部分，主要分為全球資訊安全發展趨勢與概況及臺灣資訊安全發展趨勢與概況，敘述如下：

（一） 全球資訊安全發展趨勢與概況

根據國際調研機構 Gartner 的調查，2023 年預計全球資安與風險管理產品和服務的支出將超過 1,950 億美元，增長幅度達 11.8%，此強勁的增長趨勢表明，資安在當今全球商業環境中的重要性正在不斷上升。值得特別關注的是，雲端安全被預計成為未來兩年增長最強勁的資安類別之一，這反映出企業日益依賴雲端基礎架構來支持其業務運營，同時也面臨著新的雲端安全挑戰。

此外，Gartner 的調查亦指出，企業在環境、社會和治理（ESG）等方面的關切，以及對第三方風險、資安和隱私風險的重視，將推動綜合風險管理（IRM）市場實現兩位數增長。其中 IRM 市場的增長意味著企業為確保其業務的長期穩健發展，將越來越關注整體風險管理，在這個過程中，資安服務、基礎設施防護、網路安全設備以及身份訪問管理等相關資安類別的支出將持續增加[1]。

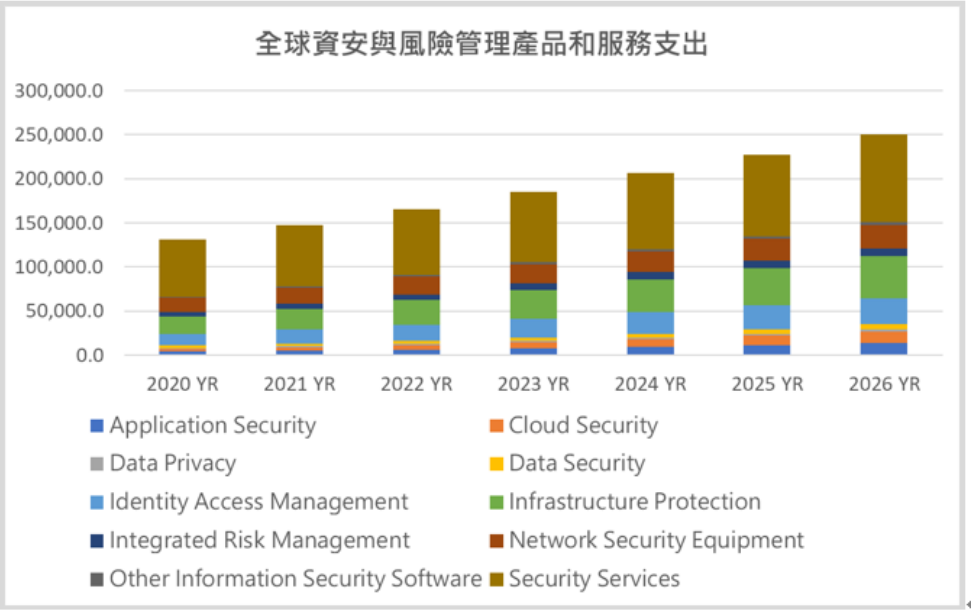

圖1　全球資安與風險管理產品和服務支出

資料來源：Gartner；工研院產科國際所（2023 年 3 月）

網路安全業者 Check Point 針對 2023 年的網路安全趨勢提出了四種主要類型，包括惡意軟體與網路釣魚、駭客激進主義、新興政府法規以及安全整合。由此可見，針對網路安全領域的不斷演變和升級，凸顯了資安專業人才更需不斷跟進新的挑戰和法規要求的現實。其中網路安全趨勢中的新興政府法規，更是反映了政府對於資料安全和隱私的關切，這需要企業遵守更嚴格的法規要求，以確保個人資訊和數據的安全。此外，安全整合趨勢顯示了企業需要將不同的安全措施整合在一起，以建立綜合的安全架構，應對多元化的資安威脅[2]。

全球的資安發展趨勢均一致顯示在現今數位環境中，資安已成為全球商業環境中不可或缺且關鍵的一部分，因此企業和組織皆必須持續投資於資安產品和服

務，以應對不斷變化的資安挑戰，確保其業務和資訊的安全，此外，了解和遵守新興政府法規，並實施安全整合策略，將成為確保資安的關鍵步驟。

（二） 臺灣資訊安全發展趨勢與概況

根據趨勢科技公布 2023 年上半年的資安總評報告，指出生成式 AI 工具不僅在合法領域內有著爆炸性的成長，也正被網路犯罪集團大量利用，AI 工具成為歹徒簡化詐騙流程、自動過濾目標以及擴大攻擊規模的利器，造就了各種新的犯罪型態；另也特別提到，臺灣在上半年內檢測到大約 4,400 萬筆惡意連結，位居全球第三，僅次於日本和美國[3]。

另參考工研院《2022 年臺灣資安產業產銷調查與現況》，提供臺灣資安企業為主體的現況調查，文中指出臺灣資安產業以中小型企業為主，59.6%的資安業者具有自主資安產品服務與專業服務，40.4%為專業經銷代理，其中超過 3 成的資安自主業者主要提供「網路安全防護產品」和「資安顧問服務」，反映出企業和機構對於網路安全的關切，以及企業需要資安專業顧問的需求，來確保其資安策略的有效實施。目前臺灣資安產業之企業客戶中以「高科技及電子相關產業」為主要銷售對象，其次為「關鍵基礎設施相關產業」及「傳統製造業者」，主要原因為臺灣身為全球重要的供應鏈夥伴，在供應鏈資安防護上具有發展優勢，由於供應鏈攻擊事件增加，企業對於供應鏈資安的需求將大幅提高，因此帶動 OT 資安、軟體及產品安全的商機和市場機會[4]。

關於企業對於各項資安新興議題因應情形，參考圖 2，觀察資安業者在未來的投入方向，主要將專注於協助企業遵循「國內資通安全管理法合規」的相關產品和服務，佔比達 60.9%。其次是「雲端服務安全應用，佔比為 57.0%，以及「WFH 遠端存取控制安全應用」，佔比達 45.7%。這顯示資安業者除了需應對政府法規要求外，也要因應雲端安全、網路存取和零信任等資安需求的提升，預計未來，資安產業的應用領域將維持多樣化發展的趨勢。

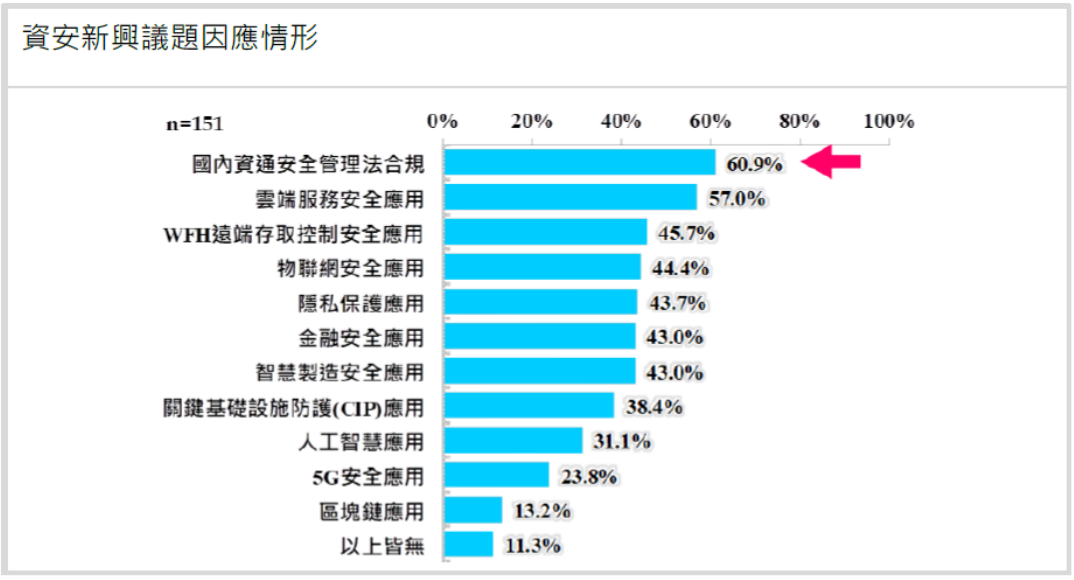

圖2　臺灣資安企業投入研發狀況

資料來源：工研院產科國際所（2022 年 12 月）

為了確保產業能夠有效應對快速變化的資安挑戰，並保護關鍵資訊和數據免受潛在的風險和威脅，因此本計畫展開國內資安產業人才需求調查，有助於企業釐清與掌握人才職能需求、協助政府更加掌握資安人才現況及企業面臨的問題，並提供建議措施，以確保資安人才培訓及供給能夠滿足產業實務需求，並為臺灣數位經濟安全持續發展提供堅實的基礎、促進其持續發展。

。

三、人才需求量化分析

本調查從業人數之推估方法為經濟合作暨發展組織（OECD）於 1960 年代建立之「地中海區域計畫人力推估法」，從經濟學上投入、產出的觀點來決定需要多少勞動供給，以達到某特定經濟成長目標。根據工研院產科國際所之 2022 年臺灣資安產業產銷調查與現況統計顯示，2022 年臺灣資安產值預估為 688.3 億，2023 年將成長至 744.4 億元，年成長率高達 8.15%。另從近期調查之人均產值成長趨勢推估，人均生產率每年平均以 1.1%的速度增長。依上述資料預估 2024 年資安產業人才需求數的樂觀值約為 2,510 人，持平值約為 2,280 人，保守值約為 2,050 人（詳見表 3）。

表 3 資安產業人才需求之量化推估表

年度	2024 年			2025 年			2026 年		
景氣情境	樂觀	持平	保守	樂觀	持平	保守	樂觀	持平	保守
新增專業人才需求(人)	2,510	2,280	2,050	2,710	2,460	2,220	2,930	2,660	2,400
景氣定義	樂觀=持平推估人數* 1.1 持平=依據人均產值計算 保守=持平推估人數* 0.9 ※本調查已將最後需求推估數字，四捨五入至十位數呈現，僅供參考。								
廠商目前人才供需現況	表示人才充裕之廠商百分比：3.8% 表示供需均衡之廠商百分比：38% 表示人才不足之廠商百分比：58.2%								

資料來源：本計畫整理。

四、人才需求質性分析

本調查彙整出資安業者八大關鍵職缺之人才需求條件與相關資訊，彙整如下表 4。

表4 資安產業人才質性需求分析表

所需專業人才職務	人才需求條件				招募情形	
	工作內容簡述	最低學歷/學類科系	能力需求	工作年資	招募難易	海外攬才需求
資安專案經理	負責資安需求訪談與確認，協助資安產品及專案之規劃、執行及進度控管，協助團隊溝通協調與整合專案團隊，滿足資安應用整合及技術支援需求。	大專/ 1. 資訊技術細學類 2. 資料庫、網路設計及管理細學類 3. 軟體開發細學類	1. 產品知識 2. 領域知識 3. 資通安全概論	**2-5年**	困難	無
資安產品研發工程師	掌握企業在資安防護上的弱點及駭客的攻擊手法，針對較新技術領域(如：5G、VR)進行情蒐及研究；根據 Road Map 及 PM 需求，進行資安產品開發規劃、需求規格撰寫、新產品開發建置、建立 CI/CD 流程、UI/UX 介面設計，解決研發過程中技術問題。	大專/ 1. 軟體開發細學類 2. 資訊技術細學類 3. 資料庫、網路設計及管理細學類	1. 程式開發與偵錯 2. 領域知識 3. 產品知識	**2-5年**	困難	無
資安產品檢測工程師	執行資安產品測試業務、驗證產品安全性；研析資安相關標準，確保部門發展之資安產品符合國際或國家法規規範。	大專/ 1. 資訊技術細學類 2. 資料庫、網路設計及管理細學類 3. 軟體開發細學類	1. 產品知識 2. 領域知識 3. 資安檢測	**2-5年**	普通	無

所需專業人才職務	人才需求條件				招募情形	
	工作內容簡述	最低學歷/學類科系	能力需求	工作年資	招募難易	海外攬才需求
資安維運工程師	負責監控資訊環境與網路系統，針對網路異常狀況或惡意程式進行分析，並製作相對應的分析報表、資訊防護計畫、分析與管理，亦包含防火牆、防毒軟體等資安設備的維護。	大專/ 1. 資訊技術細學類 2. 資料庫、網路設計及管理細學類 3. 軟體開發細學類	1. 作業系統管理（含操作、監測及維護） 2. 領域知識 3. 產品知識	**2-5年**	普通	無
資安檢測與鑑識工程師	負責滲透測試、弱點掃描及漏洞改善建議、紅隊演練、軟硬體資安檢測及產出測試報告、協助資安防護工具與機制檢測；資安事件發生後負責分析與評估攻擊事件的使用工具、技巧與程序，提出避免攻擊事件持續擴散方針，協助資安事件數位鑑識調查，針對惡意程式進行辨識與逆向工程、持續改進惡意程式分析流程；釐清公司資安的現況，協助後續應變措施的提報。	大專/ 1. 資訊技術細學類 2. 資料庫、網路設計及管理細學類 3. 電算機應用細學類	1. 資安檢測 2. 領域知識 3. 弱點掃描、入侵偵測及滲透測試	**2-5年**	困難	無
資安架構師/管理師	評估企業現行系統資訊架構，設計與規劃符合企業利益、當地法規政策的安全網路資訊架構，並協助企業制訂網路安全標準、進行資安稽核、抽	大專/ 1. 資訊技術細學類 2. 資料庫、網路設計及管理細學類 3. 系統設計細	1. 領域知識 2. 產品知識 3. 資安方案部署及管理	**2-5年**	困難	無

所需專業人才職務	人才需求條件				招募情形	
	工作內容簡述	最低學歷/學類科系	能力需求	工作年資	招募難易	海外攬才需求
	查與檢視，及追蹤營運系統資安異常事項，提交建議改善措施並落實，協助公司營運相關資安議題及風險評估，提供資安及 ISO 諮詢服務及導入，並提供資安教育訓練。	學類				
資安產品支援工程師	負責資安產品上架與安裝、保固維護、提供售後客戶問題回覆與技術支援，並研究最新資安解決方案與資安產品發展趨勢。	大專/ 1. 資訊技術細學類 2. 資料庫、網路設計及管理細學類 3. 系統設計細學類	1. 產品知識 2. 作業系統管理（含操作、監測及維護） 3. 領域知識	**2-5年**	困難	無
售前規劃業務	介於業務與技術之間，主要工作在於將客戶的需求進行規畫並將問題與業務跟技術相互討論，確保符合案件需求與技術支持。	大專/ 1. 資訊技術細學類 2. 資料庫、網路設計及管理細學類 3. 電算機應用系學類	1. 產品知識 2. 領域知識 3. 資通安全概論	**2年以下**	普通	無

資料來源：本計畫整理。

五、人才需求綜合分析

本調查經由 90 份問卷調查結果暨 8 家代表性資安廠商之企業深度訪談，綜整出對國內資安人才需求的共通性問題，經過彙整、分析如下：

（一） 資安人力擴增需求增加，人才供給不足、缺乏系統化職能培訓機制

隨著資訊安全意識的提高，越來越多的組織和企業意識到了資訊安全的重要性，再加上國內法規面的要求，導致國內企業對於資安人才的需求急劇增加，並需要透過資安廠商提供資安專業人才來幫助他們建立和維護安全的數位環境，因此國內資安廠商專業人力持續成長，資安人才擴增需求明顯增加。

然而透過本調查結果可發現，資安產業的初創企業和中小型企業佔據市場的相當份額，進一步凸顯了資訊安全人才的緊迫需求，以及企業在資訊安全領域的專業人力不足的現實狀況。

故建議深化在職培訓、建立資安人才職涯發展藍圖，加強員工所需專業知識，並鼓勵員工獲取資安專業證照，確保團隊擁有最新的技術和知識，提高資安防禦能力。

（二） 畢業生缺乏資安實務經驗、產學落差大

在資訊安全領域，實務經驗是最為關鍵性的條件，因為資安領域的複雜性和不斷變化的威脅，故會要求專業人才具備實際應對問題的能力。然而，企業注意到目前國內大專院校的資安教學內容，較無法真實對應業界痛點與需求，畢業生缺乏足夠資安實務經驗，因此新鮮人進入職場後，除了需要一段時間來適應實際工作環境，亦需要花時間掌握最新的技術和資安解決方案。

另本調查結果亦提到企業透過產學合作所培訓學生於畢業後可能受大廠吸引，或其他職涯規劃而無法長期留任的比例甚多，增加企業重新招募和培訓新鮮人的成本，也影響資安廠商投入資本於產學合作的意願。

故建議應檢視過往資安人培與產學合作培育成效，精進產學合作模式，並以業界需求為導向規劃教案及培訓師資，提高資安人培成效及提高人才留任率。

（三） 國內資安就業環境不佳，自主研發廠商難發展，人才流失率高

資訊安全產業一直以來都是競爭激烈的領域，且隨著技術的不斷發展，資安人才需求急劇增加。然而，國內資安廠商在薪資條件及福利難以與國際大廠競爭，再加上資安產業的特性，使得員工在工作中難以迅速獲得成就感且工作壓力大，故國內資安廠商刻正面臨高度人才流失的現象，且臺灣資安廠商多為代理商，無法建立與拓展臺灣資安產品與服務價值亦是國內資安產業面臨到的困境。

另外，目前國內資安實務競賽和相關活動在培養駭客思維方面發揮了積極作用，幫助參與者了解攻擊者的策略和技術，提高了對潛在威脅的警覺性。然而防禦方面的資安專業人才，才能夠幫助企業建立健全的資安措施，檢測和阻止潛在攻擊，並在發生安全事件時有效應對，也因此了解駭客思維固然重要，但對企業實務而言則更需要防禦方面人才

故建議扶植國內自主資安研發廠商，激勵企業和專業人才積極參與資安研發領域，提高產業競爭力，並改善資安專業人才的就業環境與工作氛圍，以吸引和留住優秀資安人才。

六、參考資料：

[1] Gartner（轉引工業技術研究院），臺灣資安新創前景可期 布局國際市場，2023.03，取自

https://ictjournal.itri.org.tw/xcdoc/cont?xsmsid=0M208578644085020215&sid=0N08149673221060814 6

[2] Check Point（轉引立法院），國際資通安全發展趨勢，2023.08，取自

https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=46362&pid=230858

[3] 趨勢科技，2023 年度網路資安報告，2023.08，取自

https://www.trendmicro.com/zh_tw/security-intelligence/threat-report.html

[4] 工業技術研究院，2022 年臺灣資安產業產銷調查與現況，2022.12，取自

https://ieknet.iek.org.tw/iekrpt/rpt_more.aspx?actiontype=rpt&indu_idno=3&domain_id=66&rpt_idno=932910852