我國資安人才發展藍圖

彭俊能 2019/04/03

引言

資訊對任一組織而言是屬於敏感資產，針對此資產的保護即為資訊安全，猶如日常的交通、金融、產品安全等，皆需透過一系列的規劃，以避免外在因素造成故障或損壞。資訊安全除軟硬體設施的架構外，最大的因素在於人，依據 iThome 2019 年企業資安大調查[1]中顯示，企業資安風險 Top25 顯示，人員疏忽與欠缺資安意識為第一名，在企業無法面對資安攻擊時，以人員資安知識與意識不足佔大宗。顯示人們的動機與行為將間接或直接影響到安全機制的建構，因此資訊安全人才的培育應以政策、技術及管理等三縱面，以及企業供給與需求為剖面來著手，分別規劃培育初階、中階及高階資安人員。

網路威脅大幅提升，企業資安人才需求增，但缺人才供給

全球資訊網(World Wide Web, WWW)自 1989 年誕生，至今約 30 年，整體的應用發展，已從最初的電腦連線擴展成現代的物物相連。而網路威脅也從電腦病毒、蠕蟲等單點威脅，發展到結合殭屍網路的大規模攻擊行動；攻擊對象也從不特定對象變成針對性的攻擊，攻擊的範圍由電腦主機、手持裝置到物聯網設備。雖然網路安全的防護，已從過去的單純的掃毒與防火牆，演進至今日的內容過濾、防毒系統、入侵防禦等資訊安全設備，但是多樣化的攻擊手段除了讓一般企業難以透過資訊安全設備外，也讓資訊安全產業所提供的產品或服務難以契合所有產業的需求。主要的原因，正是資安人才難以培養且供不應求，除了必須具備資訊相關的技術能力外，還必須有能力洞察可能的資安威脅，並運用自身的專業來消彌這些威脅。前述資安能力，除長期的專業技術的學習，亦需要多年的實戰經驗累積，對於我國資安發展現況僅數十載看來，這二方面的規劃應要依照短中長期之規劃加速進行，。

美國因關鍵基礎設施資安需求，制定網路安全勞動架構

以美國的關鍵基礎設施為例，整體關鍵基礎設施民營化的比重高達 85%[2]，如何協助這些民營企業獲取資訊安全人才、建立防護體系，成為美國政府的重要目標。2013 年美國總統歐巴馬要求美國商務部「國家標準技術研究所」（National Institute of Standard and Technology, NIST），研議提升關鍵基礎設施資通訊安全之架構（Framework to Improve Critical Infrastructure Cybersecurity）[3]。隔年，NIST 開始進行資安人才培育的相關規劃[4]，也就是現在的 National Initiative for Cybersecurity Education (NICE)計畫。NIST 透過 NICE 的運作下，整合政府、學術界與私部門的意見，於 2017 年 8 月公布了網路安全的勞動架構(Cybersecurity Workforce Framework, CWF)[5]，從職務名稱、職務內容、到專業技能三個面向，建立職務標準框架，提供企業與資訊安全從業人員作為職務媒合的參考。

依據 CWF 建立的資安職能地圖，協助勞工規劃職涯，幫助企業建立人才

在 NICE 的運作下，彙整了全美資訊安全職務的輪廓，依據初階、中階與高階職務，歸納出了 10 種核心職務，分別為資安專員、事件反應小組、資安稽核與數位鑑識員 4 個初階職務，滲透及漏洞測試人員、資安分析師和資安顧問 3 個中階職務，以及資安工程師、資安架構師、與資安經理 3 個高階職務[6]。本文以這 10 種核心職務為基準，考量所需具備的認證，將職務縮減為 8 類，初步建立了 **資安職能地圖** (詳參圖 1)。從職能地圖中，資訊專業人員可以依據各種認證所形成的路線，規劃自己的資安職涯，政府或企業亦可以透過獎勵取得認證的方式，引導有意願的員工往單位需求的人才發展。

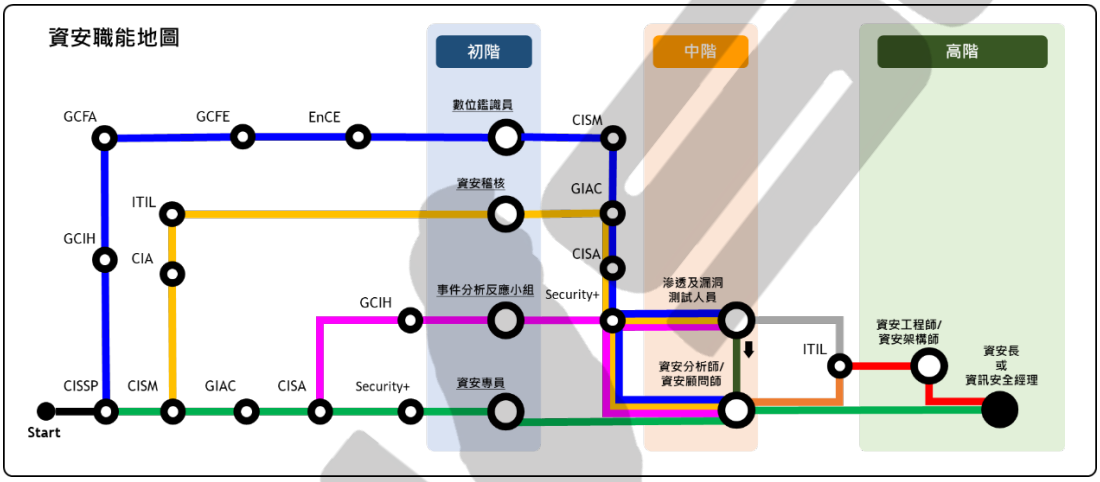

圖 1 資安職能地圖

依地圖發展國家級初階資安人員認證系統 因應關鍵基礎設施的資安需求

無論是 106-109 年的國家資通安全發展方案(核定本)[7]，或是 107-114 年的資安產業發展行動計畫[8]，發展優劣勢分析都指出資安人才的缺口，並強調政府與產業皆有快速補足的需求。本文建議政府可以參考本文彙整的資安職能地圖，在擁有相對應的認證後，輔以法律及資訊倫理的課程，便可發給初階人員國家級的認證。一方面可以借助民間培訓機構的力量，提供相當程度的認證訓練，避免與民爭利，另一方面也可以快速的收攏已具有相關認證的資安人才，因應關鍵基礎設施所需求的基層資訊安全人員。

中高階資安人員應採時效性認證制度 以維持資安人才的專業度

對於中高階人員的認定，除了專業知識與技術之外，相關的資訊事件的處理經驗也是相當重要的，不妨參酌國內專門職業的發給執業執照的標準，舉例來說，除認證之外，必須在資安產業工作滿 2 年，或是非資安產業但擔任資安相關職務滿 5 年，才發給國家級認證。此外，中高階人員除了管理責任之外，亦肩負資訊安全整體規劃的要務，必須時時掌握資訊安全發展脈動。緣此，建議

針對已發給國家級認證之中高階人員，每隔一定期間(例如 2 年)必須回訓一次，以延續國家級認證的效力。

---

1 資料來源 ：iThome Security 資安專刊：2019 臺灣資安年鑑

2 黃俊泰(2018 年 3 月)。美國關鍵基礎設施威脅資訊分享框架簡介。清流雙月刊，14，4-9。取自 https://www.mjib.gov.tw/FileUploads/eBooks/7142c018bd2a4c5ca62d35e7dd5a924b/Section_file/06e85973c1234f948ff5cdd96fbf18cf.pdf。

3 Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” Federal Register 78, no. 33 (February 19, 2013): 11737–11744.

4 Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (2014).

5 Newhouse B., Keith S. S., Witte G. (2016). NICE Cybersecurity Workforce Framework. Gaithersburg, MD: National Institute of Standards and Technology.

6 資料來源：https://www.cyberseek.org/pathway.html。

7 國家資通安全發展方案(106 年至 109 年)核定本，2017 年。行政院國家資通安全會報。

8 資安產業發展行動計畫(109 年至 114 年)，2018 年。行政院國家資通安全會報。