CIO Insight 調查解析（4）

產業資安聚焦、採購項目，以及零信任導入趨勢

CIO Insight 調查是台灣最接地氣、最多本土 CIO 大量參與的調查。本系列解析以 CIO Insight 調查數據為依據，並由最懂台灣產業，知識與經驗齊備的資策會數轉院金融科技中心分析師進一步解析。而資安是 2024 年度關注焦點，了解台灣產業對資安的的擔憂與對策，獲得跳脫危機環伺風險漩渦的可能。

調查／CIO Taiwan　解析／資策會數轉院金融科技中心

伴隨著新興數位科技應用的日益仰賴與增長，資安威脅亦是與日俱增，小如資訊外洩，大如駭客攻擊甚至惡意軟體綁架。資安威脅小致企業營運中斷、財物損失，大則損害公司信譽、造成企業經營危機，因此，該如何佈局資安策略仍是產業當今不可忽視的關鍵議題。

一、資安聚焦

所謂資安聚焦共分成三構面進行詢問，分別是「資安防護力自我評分」、企業認為「資安執行上所面臨的困難」、以及自覺「最擔心的資安防護破口」。

根據調查結果顯示，全產業在資安防護力上平均為 6.9 分，若以各產業進行細分，以金融業為首自評來到 7.7 分；服務業分數則最低為 6.5 分。

金融業本身經營受到高度監管，即便是資訊應用的合規法遵也有其高規格要求。加之服務客群涵蓋廣泛，掌握多數群體機敏資料，因此相比其他產業，金融業在資安防護力一直擁有較高的水準。

而服務業於疫情可控後陸續恢復實體店的業務

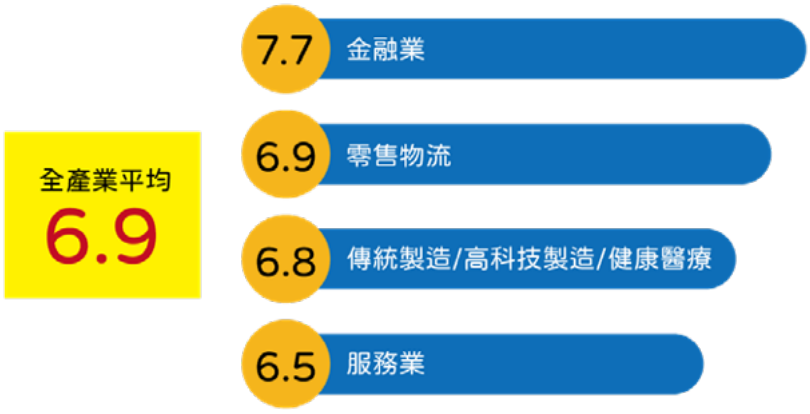

圖 1　產業自評資安防護能力。（資料來源：CIO Insight 調查報告）

活動，首要任務除使門市業務回到疫前的穩定，且須將疫情間的線上顧客導引至線下消費，眼下所面臨的營運挑戰主要為缺工議題。在減輕人力負擔之下，服務業多半透過資訊工具以降低對人力的依賴，如導入簡易的 QR 點餐系統，與服務型機器人補足外場人力。因此推斷服務業在持續強化營運發展相關資訊應用的同時，自覺其資安相關準備可能面臨新的挑戰與不足。（圖 1）

至於在詢問企業有關資安所面臨的困難中，總體來看，以資安政策未能嚴格落實執行（51.3%）為第一大困難，其次是無法隨時掌獲安全資訊動態（43.4%）與無法掌握發生資安事件後恢復正常營運的時間（33.2%）。（圖 2）

近年來企業資安事件頻傳，無論是機敏資料外洩或遭受惡意軟體綁架，皆顯示出企業內部對資安防範未具足夠的防護力。

在有關資安破口的調查上，以用戶端破口佔近 8 成，主要潛在因子恐為內部員工資安意識較薄弱，致使其資安水準不一致。其次才是有關硬體設備與軟體程式漏洞所造成的資安破口。進一步探討用戶端破口這個環節，用戶端安全佔比則將近 8 成。普遍而言，企業內部雖定期宣導及安排資安教育課程，但一般人員其風險識別能力仍較低，稍有不慎將落入社交工程與釣魚攻擊。而 IT 人員雖比一般同仁較有資安意識，但也因其在特權帳號上具特殊存取或管理權限的資格，致使其容易成為駭客的首要攻擊對象，使特權帳號安全為企業用戶的次要破口。（圖 3）

在軟體及程式漏洞中泰半以程式碼未考量安全性，與開放原始碼漏洞為企業 CIO 兩大隱憂（圖 4）。開放原始碼通常因穩定性高、能夠快速建立原型與具擴充性等優勢，成為當前不少企業在開發時的首要選擇。可開放原始碼也因其開放性緣故，讓駭客得以從原始碼中尋找漏洞，進一步對使用其原始碼的企業組織進行攻擊。

因此，為因應軟體面漏洞，產業接下來可朝 SBOM（軟體物料清單）投入與部署。透過 SBOM 來羅列軟體所涉及之元件、版本或其函式庫等詳細資訊，不僅掌握開放原始碼的使用狀況與透明度，也能夠強化產業對軟體的安全資訊。

若產業不幸發生資安事件，因 SBOM 以系統化方式建立軟體清單，除可幫助 IT人員快速追蹤漏洞並進行修補，同時加以防範第三方如軟體供應鏈的

在資安執行方面，面臨最大的困難是什麼？

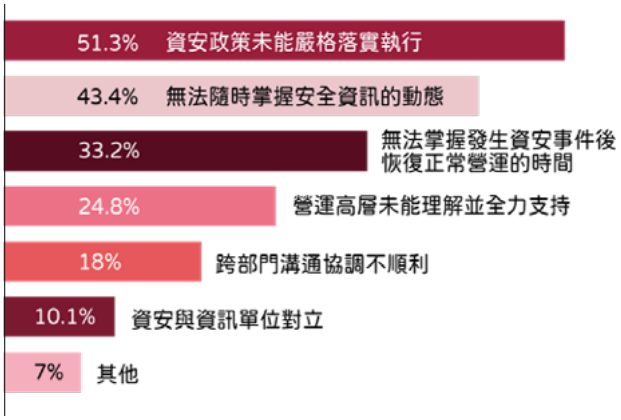

圖 2　資安執行上面臨的困難。（資料來源：CIO Insight 調查報告）

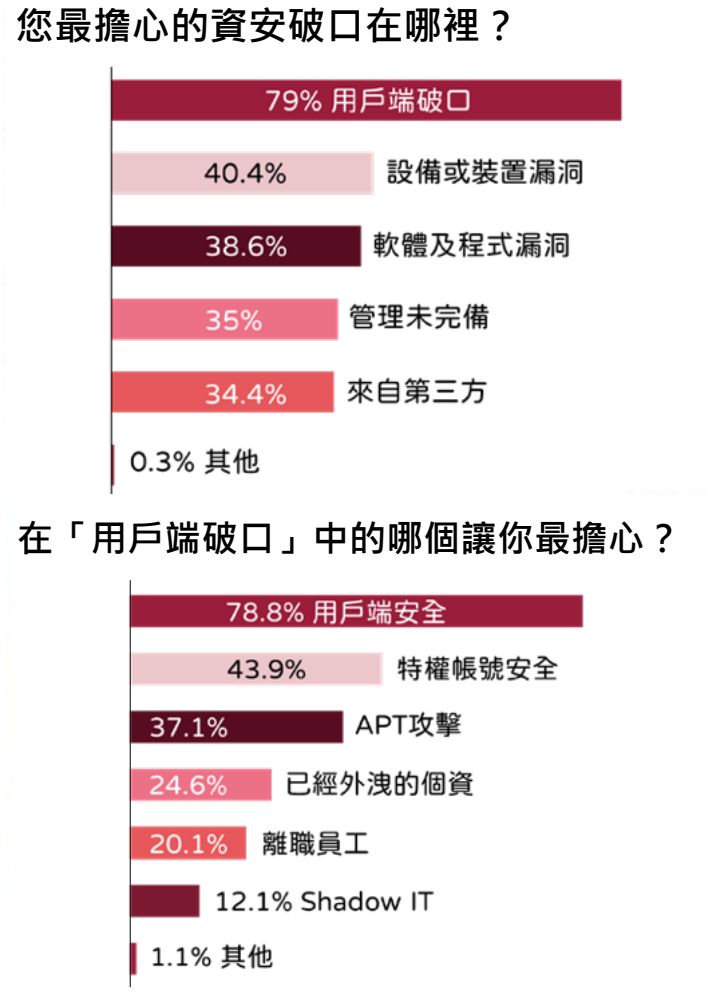

圖 3　資安破口以及用戶端破口調查。（資料來源：CIO Insight 調查報告）

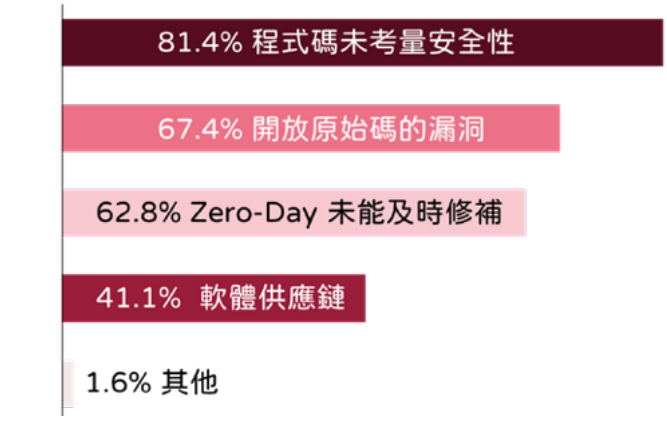

圖 4　軟體及程式漏洞調查。（資料來源：CIO Insight 調查報告）

攻擊。

二、資安採購項目

資安採購項目將以 ISO 27001 定義，共分為組織控制、人員控制、實體環境控制，與技術控制四項展開調查。由於企業 CIO 在破口面的擔憂以用戶及設備為重，由此可知在採購上也將偏向兩大部分進行因應。

在四項控制中，產業預計採購的資安項目確實其中涉及端點與防火牆，如端點偵測及回應、端點防護，以及網路防火牆和對防火牆管理等對設備裝置的防護力，可看出 CIO 仍以用戶與裝置作為資安第一道防線進行採購考量。

而現今在後疫情下所提倡的雲端與居家辦公逐漸成為一種新常態，企業面對的身分認證將不如以往僅有企業內部裝置。居家辦公浪潮下如員工個人的 PC、行動裝置或相關資料數據等，皆是透過私有網路進行登入與傳輸。

因企業無法透過內部網路進行控制與防範，故對身份認證的採購成為企業 CIO 次要的採購項目，此部分也可視為產業接下來對零信任的布局。

三、零信任架構

歷經重大資安事件與風險後，產業開始迎來資安零信任的轉型。不僅歐美國家發布相關指南，數發部也為提倡零信任架構，並於2022年開始遴選2個機關並預計逐年試行，以身分驗證、設備鑑別與信任推斷三階段，進行 A 級機關的零信任導入。

零信任架構係指在每次存取前，用戶皆要評估其安全性，在確認帳號、身份等來源安全前，該來源皆是不可信的。在是否導入零信任架構方面，全產

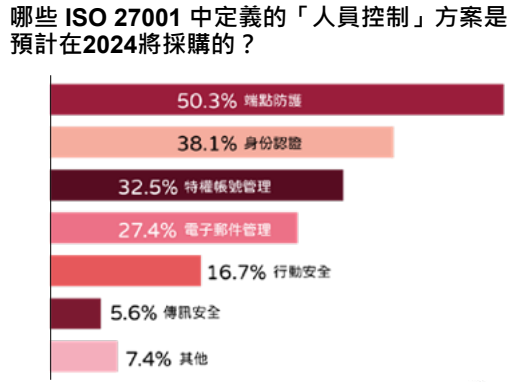

圖 5　人員控制下資安採購方案。（資料來源：CIO Insight 調查報告）

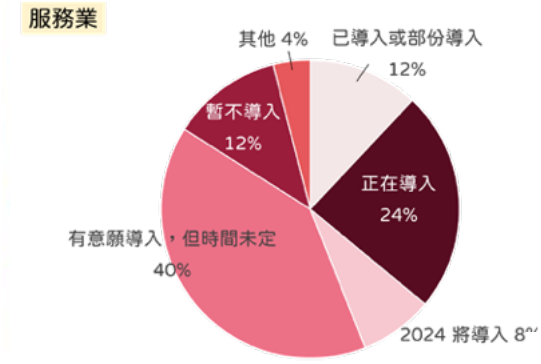

圖 6　是否導入零信任架構。（資料來源：CIO Insight 調查報告）

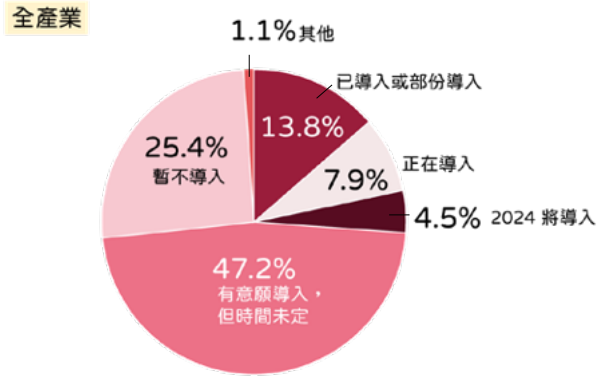

圖 7　金融業導入零信任架構。（資料來源：CIO Insight 調查報告）

業有 7 成對零信任持樂觀看法，其中 4 成為有意願導入，此外可發現 2 成的產業已導入（含部分導入）以及正在導入。（圖 6）

就其次產業討論，金融產業因金管會發布「金融資安行動方案 2.0」，其中提及因應疫情使企業採取居家辦公、內部資料與服務上雲，與內部用戶所存取的裝置多元化，故鼓勵金融業進行零信任的部署，以強化內部在連線的驗證與存取權的管控，使金融業對於規劃導入零信任的意願為高。（圖 7）

資安防護為全產業目標，尤其在歷經疫情洗禮與重大資安事件後，WEF 將網路犯罪與威脅列為全球十大風險之一，各主管機關也開始將資安列為產業的法規遵循要求，驅使產業在對用戶端安全、身份驗證及軟硬面漏洞皆有所共識。

未來，因應生成式 AI、營運上雲等趨勢，企業在應用新興科技提高生產力時，需隨時監控其潛在資安風險。因此企業可思考將導入零信任為資安防護的第一道防線，透過零信任原則以達到更好的資安治理，實現企業在數位彈性與韌性目標。

作者李震華博士，現為資策會數轉院金融科技中心副主任，及臺灣亞太監理科技協會秘書長。並兼任政大數位金融創新實驗室副執行長及臺北大學、東吳大學助理教授。李震華博士專長為新興網路與軟體技術、人工智慧、金融科技及區塊鏈加密貨幣領域，曾擔任技術研發經理、產業分析師、數位轉型顧問等職務。

掃描 QRCODE
至官網下載完整報告。