ACSI

Cyber Security Defense
Key Report

2020
企業資安防衛關鍵報告

2020

趨勢現況
資安威脅新樣貌

萬物聯網的時代，資安議題不只影響個人隱私，舉凡企業、政府乃至於公共安全層面都陷入潛在威脅，像是智慧城市包含的交通、醫療、電力基礎設施，未來經由5G連結之後，倘若遭受攻擊造成系統癱瘓，城市將瞬間陷入停擺。

數位趨勢下的資安風險與企業經營

資安風險殷鑑不遠！2015年，烏克蘭電廠因為駭客透過釣魚郵件取得登入權限，再經由遠端登入電廠系統，一一啟動斷路器截斷電力，導致全國大停電，並且故意更換密碼，使電廠員工無法重新登入啟動電力，引發全球各國對關鍵基礎設施安全性的重視。

近20年來，互聯網成功驅動各行各業快速發展與轉型，後繼的大數據與人工智慧技術，也藉由數以萬計的連網裝置，將全球緊緊牽繫在一起，於是提供駭客絕佳機會，利用這些特性在網路上發動惡意攻擊，使得數位轉型替社會與企業帶來便利及商機，卻同時引入不容小覷的破壞風險。

根據網路安全公司賽門鐵克(Symantech)2018年發表的《網路安全威脅報告》，台灣在2017年承

受全球5%的「針對性攻擊」，僅次於美國、印度與日本，次數高居全球第4名。如果數位化已是無法阻擋的明確未來，那麼「資安」勢必是不可或缺的關鍵要素，台灣企業該如何才能對抗詭譎多變的資安威脅？

安碁資訊總經理吳乙南

已然雄踞台灣資安市場翹楚地位的安碁資訊便表示，大多數企業雖然都體認到資安的重要性，但仍然僅抱持防禦降損的消極心態，建議企業應該將資安交托專業團隊管理，並且視資安為「必要投資」而非花費，做好資安防護才能確保企業競爭力像安碁資訊的服務核心，即是讓企業客戶安心於本業，外在威脅則由專業團隊協助解決，進而幫助企業未來進軍全球市場時，能夠符合各國資安要求。

新舊網路攻擊模式

需要專業資安團隊作為後盾，是因為科技日新月異，駭客手法也多元演進，並且主要針對高獲利大企業下手，光是跟去年上半年相比，2019年威脅數量就成長265%、勒索案例也飆升319%。如今在台灣，平均每天發生5起企業勒索求助事件，其中二成為重大損害事件，導致業務或生產停擺，因此安碁資訊強調現在是「新舊風險並陳的環境」，安全隱私顧慮有增無減。

像是個資洩漏事件仍然層出不窮，就是罪犯藉由掌握網路上的巨量身分資料（big data），能夠針對大量通用格式的個資實施大數據分析，例如分析出哪些人經常旅行，再透過其個人檔案如公司電子郵件、任職單位等相關資訊，在臉書或LinkedIn等社群媒體上拼湊出個人背景輪廓，進而販售謀利，因此形成惡性循環。

另外，普及率越來越高的電子商務與線上購物，讓罪犯可以在網頁植入惡意程式碼，竊取信用卡資訊，過去兩年這類型攻擊數量激增，舉凡英國航空公司、Home Depot 和 Target 等國際知名企業都是受害者。美國 F5Labs《2019 年應用報告》檢查760份資料洩漏報告，便發現表單劫持攻擊（Formjacking）占2018年所有網路資料洩露事件的71%，2019年至今也有83起表單劫持攻擊，導致近140萬張信用卡資訊外洩。

當然還有越來越頻繁的雲端跳躍網攻(Operation Cloud Hopper),2017年有8家全球主要電腦服務供應商遭到駭客入侵,而挖礦綁架轉向Docker主機以及進階持續性滲透攻擊(APT)更是防不勝防,影響層面涵蓋金融、教育、醫療等產業,顯示企業無論大小,資安事件偵測能力都有必要持續提升強化。

從IT蔓延至OT的企業資安隱憂

2018年,台積電傳出遭病毒攻擊產業線停擺,短短兩天蒸發52億台幣,消息一出令人咋舌,試想如果連台積電這樣的大企業都難以防堵,其他企業該如何自保?

安碁資訊表示,企業面臨資安新舊風險並陳的環境,不少廠區大量使用OT(Operation Technology操作科技)與ICS(Industrial Control System 工業控制系統),加上近年IT(Information Technology資訊科技)的資安威脅正蔓延到OT領域,不只影響高科技製造業的自動化產線,也危急國家關鍵的油、電、水基礎設施,一旦運作中斷,必然帶來極大影響。

安全研究中心Ponemon Institute於2017年10月所做的調查,顯示全球利用殭屍網路(Botnet)以自動化方式惡意登入與日俱增,尤其針對憑證填充攻擊次數就增加54%。資訊工業策進會資安科技研究所所長毛敬豪表示,許多OT是根據普渡(Purdue)模型設計,當OT與IT相結合之後,ERP(Enterprise Resource Planning,企業資源計劃)、檔案伺服器等系統若遭受駭客攻擊,會連帶威脅OT環境,並且在行動裝置普及化、物聯網應用進入工控環境之後,駭客入侵的管道將會更加變化多端。

安碁資訊也提出警示,供應鏈廠商的資安漏洞,是許多企業經常忽略的關鍵環節,倘若上下游未能做好資安防護,讓病毒透過網路進入公司網路系統,嚴重程度將癱瘓生產線,因此想要落實資安,勢必要從資產盤點與風險評估著手,一旦發現容易遭受駭客攻擊的資安弱點是重要資產,必須優先處理,同時加強OT人員的資安概念,且針對高階主管進行資安教育,透過偽冒監看數據回應,來認識如何滲透測試與修補。

安碁資訊資安長顧寶裕

因此在可見的未來,肯定會有越來越多樣型態的資安要求,企業思考下一步營運計畫時,無論想擴大業務量或是站穩世界舞台,資安防衛都是至為關鍵的一役。

實際案例
國內外資安企業案例，以金融業為例

台灣平均每772人擁有一台ATM，密度之高堪稱全球第一，替民眾帶來高度便利性的同時，卻也引發資安隱憂，像2016年7月，竟有駭客自英國倫敦發動攻擊，遠端遙控台北與台中共22家第一銀行分行內的41台ATM，吐出超過8,300萬新台幣現鈔，輿論一片譁然。

國內外資安實例

近年來，世界經濟論壇（World Economic Forum, WEF）固定發布的「全球風險報告」中，「數據詐欺或竊取」與「網路攻擊」項目經常高居前5名，因為對於積極擁抱數位轉型的企業來說，這些資安風險已經是普遍事實，特別是大手筆投入Fintech發展的金融業者，感受到的衝擊最為明顯。

所以回顧國內外發生的重大資安事件，不難發現許多「苦主」都是銀行、券商等金融業者，受害清單涵蓋ATM遭駭、DDoS（分散式阻斷服務）攻擊、SWIFT（環球銀行間金融電訊網路）入侵、個資外洩等。

其中，在ATM遭駭部分，最有名的是2013年3月20日，南韓發生史上最大駭客攻擊事件，癱瘓了近48,000台電腦，也造成全國ATM故障、網路銀行與信用卡交易停擺，影響層面難以估算；時

至2016年10月，印度多家銀行ATM遭受入侵，導致320萬張簽帳卡資料外洩；2018年1月，國際駭客鎖定美國舊型ATM，偽裝成廠商安裝惡意程式，遠端控制大量吐鈔；2018年3月，印度Cosmos銀行ATM伺服器遭駭，被設置虛假代理伺服器進行授權交易，幾小時內約9.4億盧比(約4.1億新台幣)被盜。

2013/03
南韓駭客攻擊事件

造成ATM故障、網路銀行與信用卡交易停擺

2016/10
印度ATM疑遭入侵 320萬張簽帳卡資料外洩

駭客透過惡意程式感染Hitachi支付平台，再駭取用戶金融資料，多家銀行及金融機構合計約三百二十萬筆Debit金融卡資料遭竊取

2018/01
國際駭客鎖定美ATM進行攻擊

美國遭感染機種為Diebold已停產舊機型(Opteva500、Opteva700)，駭客偽裝成廠商安裝惡意程式遠端控制吐鈔

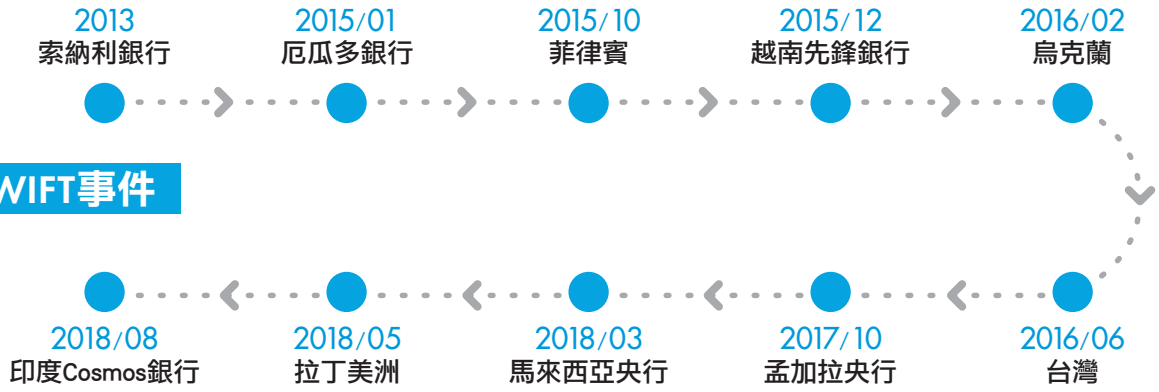
2018/03
印度Cosmos銀ATM伺服器遭駭

駭客設置虛假代理伺服器進行授權交易幾小時內約有9.4億盧比(約台幣4億1241萬元)被盜。

至於DDoS攻擊一直沒有停止過，過去四年，每一年都有台灣券商接獲勒索信件並遭受流量攻擊，雖然根據卡巴斯基實驗室的研究報告，2018年的DDoS攻擊活動比起2017年減少13%，但也顯示平均攻擊時間增加2倍之譜，加上網路可以輕易搜尋到相關教學影片與攻擊測試工具，所以金融業者務必及早做好防護準備工作。

2016/09 證券業遭寄發勒索信並遭到攻擊
2017/02 證券業再度接獲勒索信並遭到攻擊
2017/04 數家證券業收到勒贖信件要求支付比特幣
2017/08 國內券商再度遭到駭客流量攻擊
2018/04 國內金融業網站又遭受到攻擊
2019/10 國內金融業及券商再度接獲勒索信並遭到攻擊

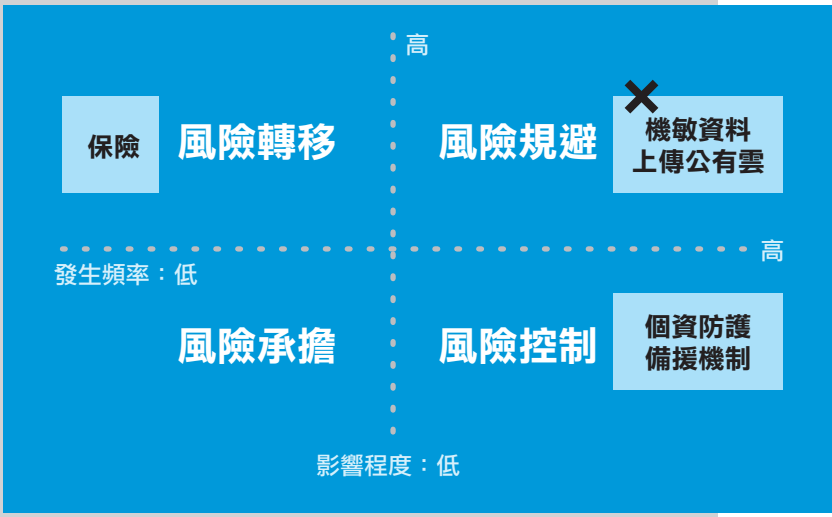
而SWIFT入侵和個資外洩，造成資金損失的事件更是屢見不鮮，最廣為人知莫過於2016年2月孟加拉中央銀行被駭客攻擊，成功盜領8,100萬美元，以及2019年美國第一資本銀行（Capital One）逾1.06億名客戶個資大規模外洩，損失估計1至1.5億美元，當然相關災情也曾在台灣發生，2017年遠東國際商業銀行的SWIFT系統就遭到駭客入侵，盜轉匯出18億新台幣，經事後調查，用來取得轉帳權限的惡意程式，居然悄悄潛伏數月未被察覺。



金融業資安管理重點

基於新科技導入伴隨各種資安風險，以及各國監理機關對管理面向的要求跟罰金越來越高，彰化銀行副總經理陳斌分享寶貴經驗，建議金融業者應該先行建立三道防線、組成風險管理架構，第一道防線是成立資訊處營業單位，第二道防線是成立專責管理的資安單位、法遵單位或風險管單位，第三道防線則是強化內部稽核。

接著，盡量將風險控制在可容忍範圍以內，並且選定適當的風險移轉、規避、承擔等對策，包括利用PDCA（循環式品質管理）持續改善，再藉由風險管理過程保持資訊的機密性，完整及可用性，例如由組織最高管理階層給予承諾及支持，建立明確的風險準則，就能透過識別、分析及評估資安風險，選擇適切處理選項並制定處理計畫，倘若量測指標、內部稽核及管理審查時，發現有不符合標準的地方，便可以立即改善與調整。



※為控制風險於可容忍範圍內，選定適當風險對策

當然也別害怕善用新興科技，包含人工智慧、雲端服務、生物辨識、IoT設備、區塊鏈、社群網路等應用，為金融業的服務、產品、組織、效率帶來實質改善，實現普惠金融的願景，即使新興科技不當使用，可能帶來詐欺、洗錢、資料外洩等資安風險，但只要透過各種資安檢測及演練作業，持續不斷改善，就有助於降低外部威脅風險程度，提高資安防護能力。

陳斌副總經理強調，邁入數位金融時代，實體銀行開始弱化，越來越多資料會被送上雲端網路，尤其金管會已經宣布「金融機構可於境外雲端儲存客戶資料」、「開放純網路銀行之申設」、「Open Banking三階段開放措施」等三大開放政策，可想而知數位金融服務勢必紛紛推出，將加速開放混合雲端應用並形成第三方生態圈，需及早建立資訊安全意識。

加上金管會規定管理資產達一兆新台幣的銀行，必須獨立設置法遵與資安部門，金融業者不妨尋求像安碁資訊這樣經驗豐富的資安公司合作，在安全與便利間做好弱點控管，包含導入新世代防火牆、入侵防護系統(IPS)、安全存取系統、資安分析和惡意軟體防禦等完備資安技術，不僅可作為堅實後盾，更可搶先一步戰勝網路攻擊，為企業與客戶部署進階防衛。

企業解方
資安防衛新思維

微軟(Microsoft)發布的亞太資安研究報告指出，2017年台灣因資安攻擊造成的經濟損失高達8,100億新台幣，相當於GDP總值的5%，但台灣企業超過9成以中小企業為主，並沒有足夠的風險意識，編列適當預算做好資安防護，容易身陷危機而不自知。

弱點管理與資源配置

企業要防堵資安意外其實不難，工研院產業科技國際策略發展所分析師鍾銘輝指出，有5大方法可以協助加強弱點管理與資源配置，包括採用終端防毒系統、優化內網防禦、定期風險評估與預測、提升員工資安意識，以及著重快速復原。

首先，隨著硬體效能的進步，企業可以尋找終端設備上的防禦方案，避免病毒入侵與執行，再透過設定管理規則，禁止非正常運作程式在機台中被開啟與執行，例如採用「應用程式白名單」，只有允許的應用程式才能執行與更改，即使出現病毒程式，沒有允許也無法執行，自然不會影響工廠正常運作。

第二，企業必須有效地將內網分割成更小的「區塊」，使負責不同職務的員工團隊各自獨立運作，並且內網安全防火牆可建立異常流量的監測機制，限制病毒、惡意程式碼的側向移動與快速散播，抵禦端點對端點的跨網路威脅。

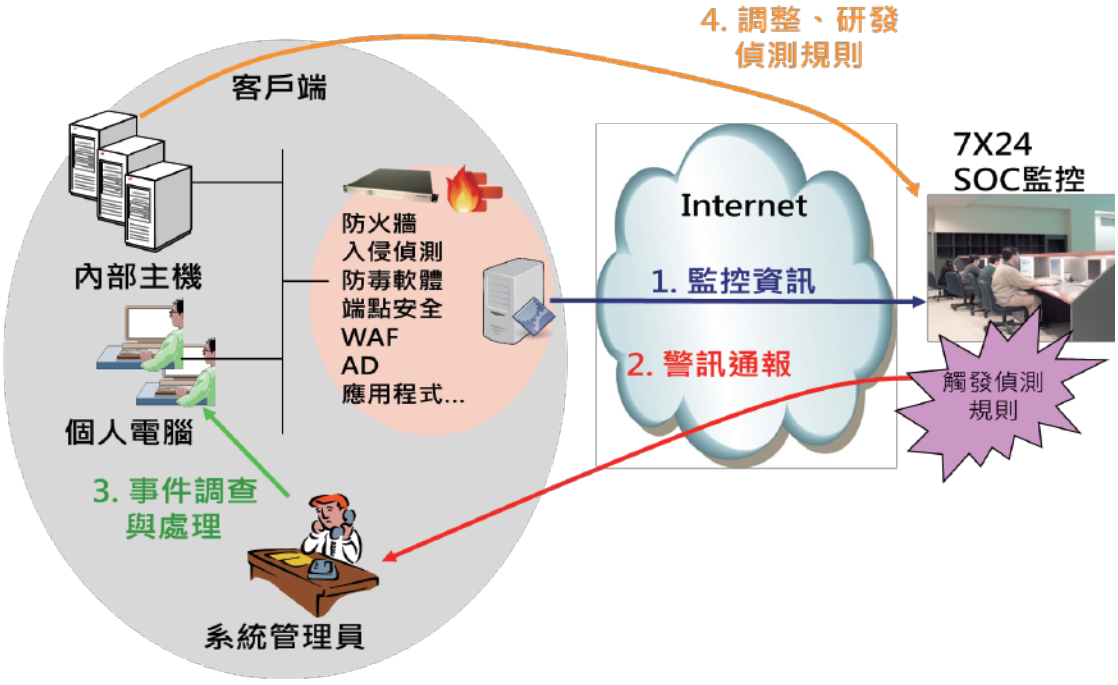
第三，有時候企業遭受勒索病毒攻擊，是因為廠房使用舊作業系統、防毒軟體來不及更新，甚至是系統老舊無法安裝防毒軟體，導致惡意程式輕易感染與擴散，所以應該定期進行風險評估與預測，適時更換或修正軟硬體設備。

第四，資安意識不只有IT人員需要知道而已，目前大多數生產管理與廠務部門人員，對資安防禦的概念並不熟悉，應該讓負責機台設備的單位加強資安教育訓練，儘快建構功能完整、簡單易用的資安防禦體系，避免隨時可能發生的安全事件。

最後，企業可以導入快速復原系統，因為一旦機台發生問題，假如維護人員必須經過多道程序才能進入無塵室，導致無法第一時間到場解決，產能停擺影響與金錢損失將難以估計，所以有了提供遠端連線管理功能的機台安全解決方案，只要一個程式上的操作，便能趁早復原降低傷害。

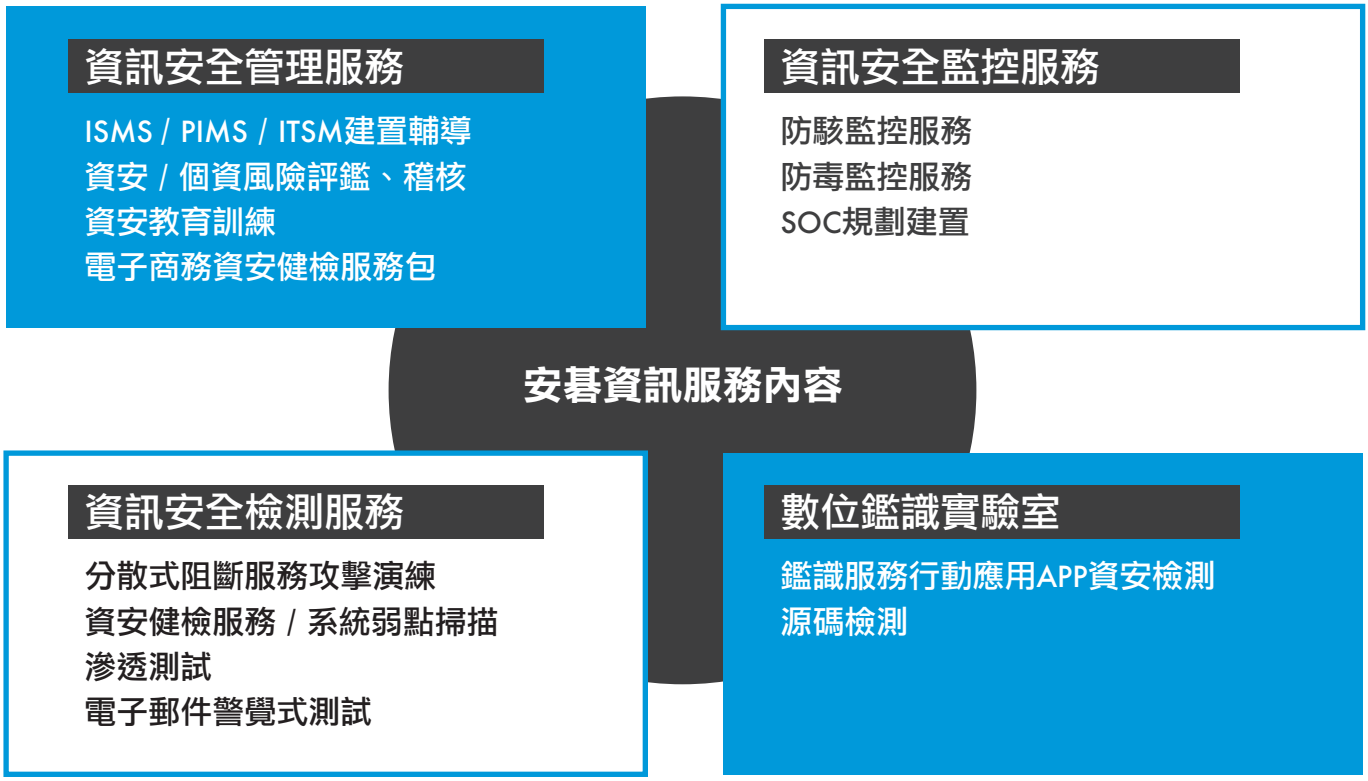
SOC資安服務趨勢

為了對抗多元類型的資安威脅，企業打造自有或使用委外SOC(Security Operation Center，資通安全防護管理平台)已成為另一股新趨勢，所謂SOC是指在建立防火牆、防毒軟體等基本防禦之外，還需要導入資安數據收集、安全事件分析等手法，進一步架構精準的警訊通報機制SOP。



創立於2000年的安碁資訊，是目前台灣最大的政府部門SOC服務商，當年投入資安市場第一步，即是從美國引進創新SOC營運技術，打造國外廠商難以比肩的在地服務團隊，先爭取到行政院國家資安會報的NSOC（National Security Operation Center，國家資通安全防護管理平台）標案，再憑藉專業服務與良好口碑，陸續成為中油、台電、台水等政府機關的合作夥伴。

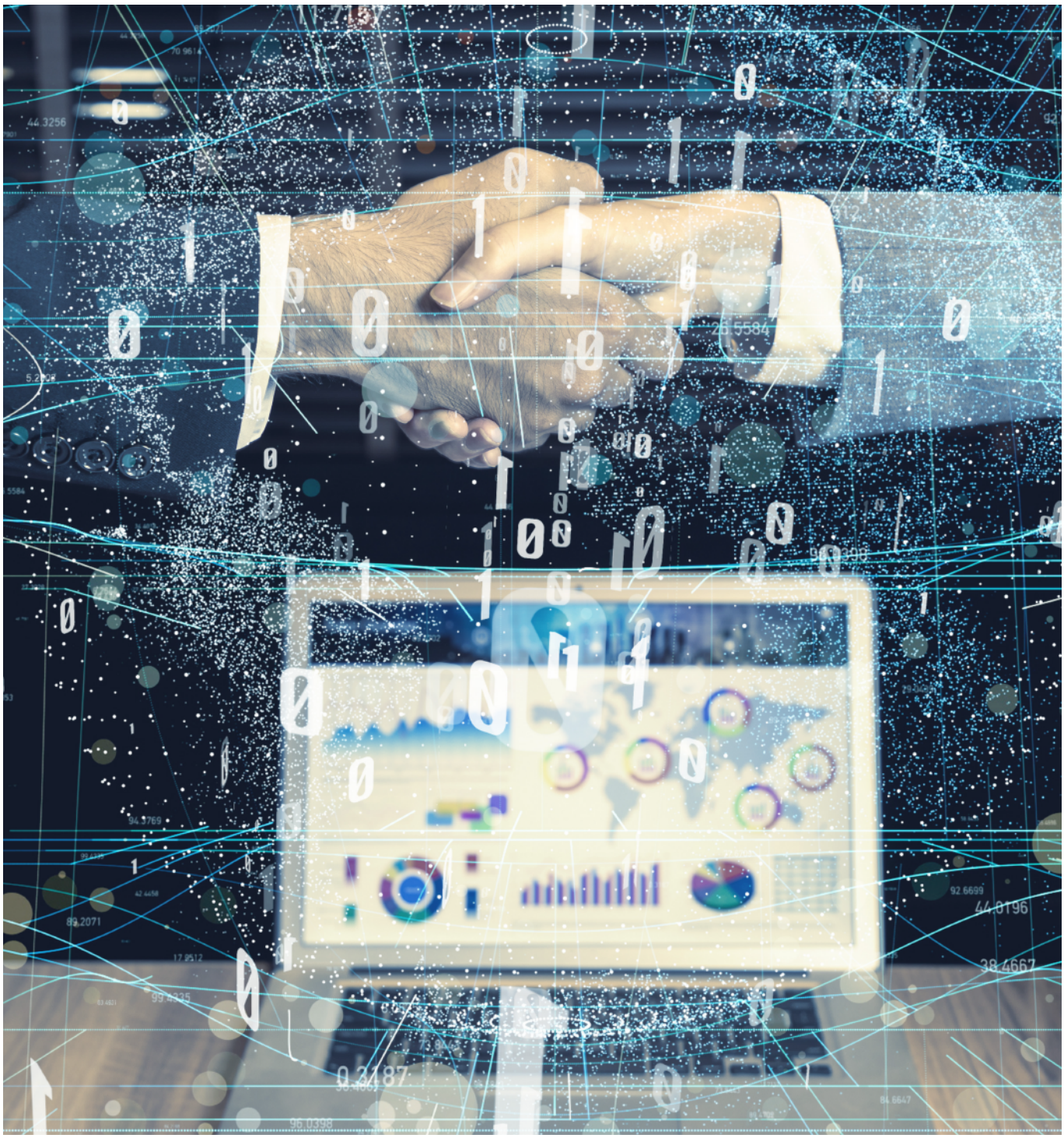
加上安碁資訊2017年大手筆斥資成立數位鑑識中心實驗室，不僅成為台灣最早取得ISO17025「鑑識科學」與「行動應用APP基本資安檢測」兩項國際技術認證的資安廠商，也讓提供政府機關與企業的24小時不間斷SOC，能夠與應變處理的各項數位鑑識工具無縫接軌，強化整體服務能量，如同正是有了ISO17025認證，安碁資訊才能扮演關鍵角色，協助台積電處理2018年電腦中毒事件。



安碁資訊提供台灣企業健全的資安服務

至於SOC展現哪些資安聯防具體效益，安碁資訊特地舉實例說明，幾年前發現某部會首長辦公室的電腦被駭客控制，經由SOC追查之後發現，竟是一個軟體工具的原廠，遭到駭客入侵所導致，以往類似的資安事件，只靠電腦防毒偵測是無法找出真相，但SOC能夠知道駭客是誰，從全球駭客行為的監控、個別客戶的受攻擊行為中建立規則，進而做出可廣泛套用的「數位防駭疫苗」，像2013年國家檔案局的電子公文交換系統，遭到駭客植入木馬程式，中央各部會與地方政府各機關廣受影響，安碁資訊便在偵測後立刻提報主管機關，並將因應措施迅速推送給各個客戶手上。

隨著2018年5月立法院三讀通過《資通安全管理法》，要求政府部門擴大資安防範規模，從中央層級部會到地方政府機關，都必須符合這項法律要求，所以未來舉凡資安健檢、滲透測試等服務需求將會越來越多，尤其中央跟地方政府都紛紛有了「區域聯防」概念，SOC趨勢肯定持續增長，預計也能給中小企業起了帶頭示範作用，加緊腳步規劃SOC建置，讓資安成為數位資產的重要一環。



企業資安的推進者

想了解更多企業創新轉型的致勝關鍵
請造訪安碁資訊

安碁資訊股份有限公司
Acer Cyber Security Inc.