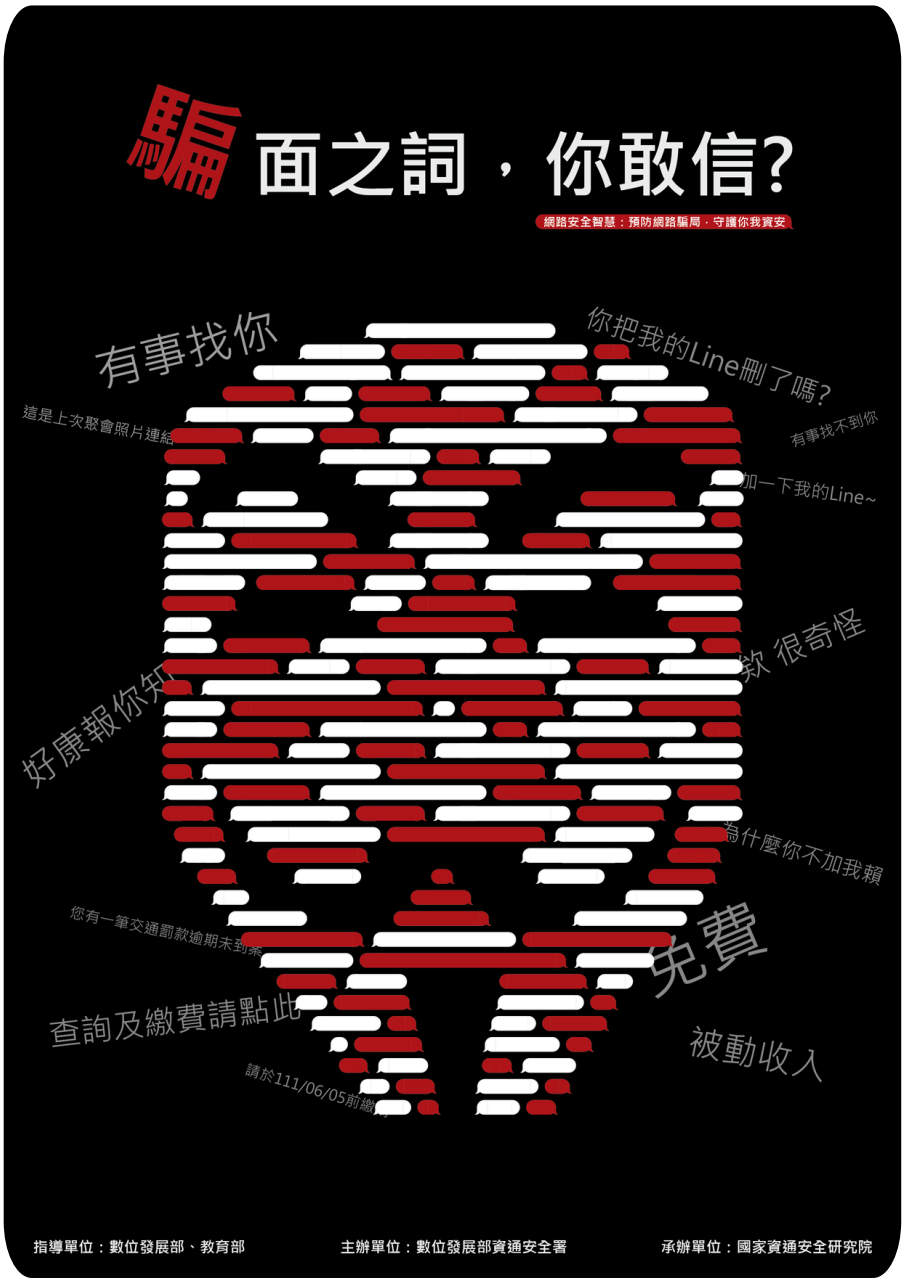
114年5月號

公務機密
資訊安全維護



林業及自然保育署
臺東分署

公務機密 資訊安全維護

目錄

資安時事案例

各機關被駭客入侵都不通報？資安修法定罰則 避免沈默共犯

今年馬偕醫院被駭客入侵，甚至造成1600萬筆民眾個資外流。圖/本報資料照片

2025-04-24 11:31 聯合報／ 記者馬瑞璿／台北即時報導

立法院交委會今（24）日審查「資通安全管理法」部分條文修正草案，立委對於政府機關資安人力、駭客入侵通報機制都提出不同質詢，尤其，許多醫院、企業被駭客入侵之後，都不會主動通報，今年馬偕醫院被駭客入侵，甚至造成1600萬筆民眾個資外流，都可能為民眾帶來潛在的新詐騙風險。立委要求資安法必須建立72小時通報機制，並提出差別性罰則，以避免沈默共犯。

台灣因為地緣政治關係，經常遭受駭客攻擊。根據國際資安業者Check Point統計數據顯示，2024年全球平均每周網路攻擊次數為1673次，較2023年增加44%，其中，台灣遭受攻擊的情況相當嚴重，平均每周遭受3993次攻擊，居亞太地區之首。但無論是政府單位，還是私人企業，資安人員的人力遠遠不足。

國民黨立委洪孟楷今日質詢，若是公務機關稽核都由資安署負責，人力究竟夠不夠？數發部長黃彥男指出，目前資安署每年要稽核的公務A級機關，包含台電、台水等，總共有96個單位，資安署的人力目前每年稽核約40個單位。

民進黨立委李昆澤質詢時指出，根據資安署統計，中央及地方依法應配置資安專責人員共1533人，但實際編列人員只有939人，占整體需求的61.25%，非正職人員（約聘、委外）共355人，即便加聘人力，公部門缺額仍達239人，等於有有近16%的缺口沒有填補。民進黨立委許智傑也指出，資安署成立至今，離職率為2.18%，遠高於近五年全國公務人員離職率的0.79%。

對此，數發部長黃彥男指出，部內有轉職訓練，預計會補400-500人，也有高考資安類課，希望能有更多人來報考；資安署長蔡福隆則表示，各個領域、部門都在競爭有限的資安人力，公部門待遇無法跟私部門比較，只能透過獎勵措施、加給才能留才，他也建議A級機關可以增加待遇來吸引人才。

共諜案近日引發關注。洪孟楷質詢時指出，外交部長助理職等沒有很高，但是經手外交部長行程，機密流出去不知道多少，在政府底下變成一個共諜，數發部也應該針對稽核人員進行查核，以免國家機密資料流出。蔡福隆回應，資安署中，不只是科長級要做特殊查核，只要是涉及業務機敏同仁，都會通報法務部調查局進行特殊查核，以保障機敏業務不外流。

另外，台灣資安事件頻傳，今年以來，國際駭客組織不斷攻打台灣醫院，從之前的馬偕醫院，到近期的長慎醫院，都被駭客入侵，也有不少駭客組織持續攻擊過內企業，但因為現行資安法沒有強制企業立即通報，也使得很多企業都有鴕鳥心態，能不通報、就不通報。

李昆澤質詢時指出，個資法對於通報時間規定相當籠統，缺乏通報時間跟處罰，國際上，美、歐、日、韓都明確規定24-72小時強制通報制度，他認為，台灣應該要建立72小時通報機制，被駭單位應該要在72小時內通報政府，並提出差別性罰則，以避免沈默共犯。黃彥男則回應，新修的資安法中，有規定1小時內要通報，不通報也會祭出罰則。

2000大企業表態重視資安
卻陷入誤區 「見招拆招 + 別著急做」 釀資安危機

2025/04/15 16:56:57/經濟日報 蘇璽文
2025年還沒過完第一季，台灣資安再度亮起紅燈。先是2月傳出北部知名醫院 500 台電腦遭駭當機與中部某醫院遭攻擊引發關注，3月初北部知名醫院病患資料遭加密勒索，1660 萬個資被駭客公開販售，恐已流入詐騙集團手中，各界無不譁然，以喚醒了台灣社會對重大資安事件的記憶。

如2016 年，某銀行ATM被駭入盜領 7000萬台幣，以及後續的十三家證券公司遭集體勒索、鐵路票務系統遭駭、加油站支付系統遭癱瘓、戶政資料 2357 萬筆遭兜售、某航空公司會員資料遭勒贖…等，以及北市衛生局、銓敘部、汽車租賃服務、知名百貨、旅行社等個資外洩事件，無不在當時震驚各界。

令人憂心的是，當今社會無論企業營運或民眾生活，雙雙走入數位化，相當於 24 小時暴露於資安風險的侵襲中，每一民眾都可能成為下一個待宰羔羊，而政府、企業、機構也都可能成為新的受害者。

8年大小事件下來 台灣不是沒有學乖

就連被外界認為資安嚴謹的一種科技大廠也不見得能倖免，在過去的8年間，陸續遭遇大小不同的資安攻擊。儘管政府與企業多次宣示加強資安力道、更在數位轉型、永續經營的浪潮下搖旗吶喊，卻仍顯力有未逮，也讓外界質疑，「資安即國安」的說法，是否正在延後兌現？！

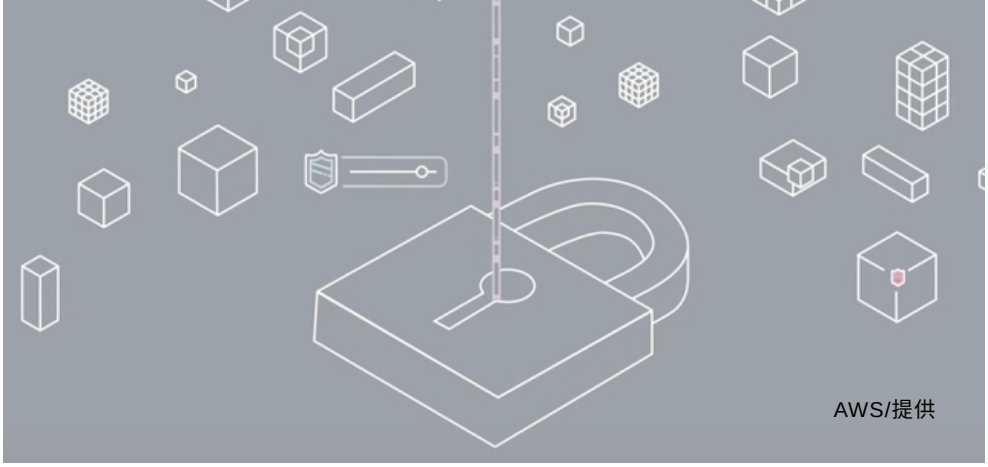
事實上，台灣企業並非沒有亡羊補牢，從《2025 CIO Insight 調查報告》可以得知，企業未來一年的IT重點專案類型正是以「網路安全軟體與服務」占最大宗，但專家卻一針見血的指出，台灣資安跟不上腳步是因為存在著「資安意識提升，但行動力不足」、「缺乏整體策略，看到了才補救」、「新威脅難掌握，建置緩不濟急」三大軟肋，前者包含預算、人力、角色、評估上的困境；中者點出企業難以獨立完善資安防護，只能見招拆招；後者則是對於新威脅缺乏掌握，因而難有因應之道。

對此，有不少業界人士建議，與其固守實體機房、形同孤島無援，不如把架構、資料放上雲端，利用其託管服務的安全機制來為企業或政府的資安把關，其好處是「一來可以藉機落實數位轉型，淘汰老舊又難以防護的設備；二來省去成本與人力，把資安交由CSP雲端服務商（Cloud Service Provider）一肩扛起。」專家說。

令人憂心的是，總有很高的比例企業認為「能獲得完善的資安保障，正是它們願意遷徙雲端的主要動機」，同時卻也陷入最大的誤區，就是「行動跟不上心動」。對此，業界專家表示，台灣企業與政府時常會「說服」自己不用變革，理由有以下三種：

- 對於地端設備的眷戀，捨不得早期投入的成本
- 認為現行仍然能運作，下一個出事的並非自己
- 架構與資料搬遷麻煩，深怕日常營運受到影響

然而，長時間拖著無疑是將自己與用戶暴露在高度風險的攻擊危機之下，加上各式新興威脅與日俱增，全球每一年所面對的資安挑戰，恐只會越來越棘手。



AWS/提供

雲端真的比較安全？ 看看AWS做了什麼？

「比起單打獨鬥的實體機房，答案絕對是肯定的！」現代資訊架構下，相信多數專業人士會給出這樣的答案。

以 AWS 來說，他們會運用旗下的 Amazon GuardDuty、Amazon Macie 即時監測異常行為，同時自動化保護機敏資料，也會利用 AWS Key Management Service（KMS）與 CloudHSM 為高度機敏資料再加密上下足功夫。另一方面，則是符合當地法規與認證，企業可以「一卡皮箱」的搬遷，不需要擔心法令問題，而「災害備援、災中維運」同樣也是雲端服務的強項。

在業界，每一家CSP都會有自己的看家本領！一般來說無論是那一朵公有雲都握有一群資訊科技業的頂尖人才，也長期致力於資訊安全。以目前市佔率最高的AWS為例，首先，光是擁有動輒數千人的專業資安團隊，從事24小時全天候的監控與威脅應對，就已經是一般企業難以達成的優勢；第二，雲端平台有自動化安全更新，能快速修補漏洞，避免後續的風險；第三，所宣成的資安防護，均需經過第三方安全認證，認證標準相當嚴苛，還要符合國際規範，除了ISO外，還有GDPR、HIPPA、NIST 等，並非一般企業都有資源能完整具備；第四，所有在雲端上的資料，都會經過加密處理，無論是儲存或傳輸中。

「不僅擁有多層的防護網，還擁有資安事件的應策中心、情報中心！ 對企業來說十分划算。」這是許多加入 AWS 公有雲行列企業的共同心聲。不僅如此，美國國防部、中情局、日本內務省等，被視為必須窮極資安之能事的世界各國政府單位，也早在多年前上了雲端，目的就是為了資訊安全、簡化管理，同時為AI與缺工時代做好準備。

上雲成自然？ AI、資安、缺人才帶動二次雲端浪潮？

前一次的企業上雲浪潮約莫始於2013~2014年，為的是迎接行動網路帶來的數位生活型態。十年後的今天，「AI導入、永續規範、人才缺乏」很可能就是背後主因。

首先，AI算力與應用，已非企業可以自建維運，雲端平台「即用、節省、快速，可因應新變化」的優勢，幾乎成為導入AI的唯一途徑；其次，ESG永續浪潮下，公司治理也被賦予落實監督資訊安全的重責大任，資安需求只會變得越來越剛性；最後，資訊人才日漸缺乏下，企業也開始找尋新出路，取代傳統耗人費時的維運方式。

此一跡象也能從《2025 CIO Insight 調查報告》看得出來。報告指出，台灣五大產業（服務、金融、健康醫療、高科技製造、傳統製造）未來一年的前三大IT專案類型分別為：1. 網路安全軟體與服務、2. IT基礎架構現代化／雲端基礎架構、3. 人工智慧與機器學習平台工具，如此的資訊支出配置，幾乎也佐證了台灣迎接第二次雲端浪潮的說法。

最後，根據《iThome 2024資安大調查》顯示，台灣面臨多達12種的資安風險，企業卻因著「人手不足、員工意識不足、預算不足、高層缺乏意識」等阻礙裹足不前。倘若台灣各界仍對於資安投入抱持「沒發生事情，就先不編列預算」或「錢都花了，卻沒發生事情，很浪費」的心態，恐怕將永遠跟不上駭客、詐團、有心人士的積極手段。

個人資料保護法

蝦皮購物疑有中資「掌握個資恐危及資安」 監察院要查了

蝦皮購物平台有中資疑慮，監委主動申請調查。資料照片，廖瑞祥攝

陳康宜/太報報導
2025年4月17日 週四 上午11:06
監察院今（4/17）發新聞稿表示，蝦皮購物平台疑有中資背景，恐影響我國資安及經濟主權，監察委員賴振昌、賴鼎銘申請主動調查。

監委賴振昌、賴鼎銘表示，國人慣用的蝦皮購物平台，其母公司冬海集團（Sea Limited）的大股東為香港騰訊，且現任董事與中共政商背景人士具高度關聯，該平台疑具中資背景，且其掌握國人個人資料與金流資訊，恐影響我國資訊安全及經濟主權。

監委賴振昌、賴鼎銘認為，蝦皮平台在我國境內投資及從事之各項業務，主管機關是否確實依法審查及監管？該平台資訊安全機制是否健全？其掌握之個資及資金有無違法使用之情事？都有深入瞭解的必要。

蝦皮購物2022年曾澄清，最大投資來源為新加坡和美國，無任何國安疑慮。

每月一常識

新版個人資料保護法與過去有很大的不同，新法進一步擴大了個人資料的保護範圍，並且讓所有產業一體適用；新法甚至首度增加團體訴訟，而且違法的罰則也加重了，企業老闆要負更大的責任。接下來，我們以60個Q&A，快速帶你認識新版個人資料保護法

Q13 什麼情況下可蒐集特種資料？

A 符合以下事項，則可合法蒐集與使用特種資料：
1.法律明文規定。
2.公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施。
3.當事人自行公開或其他已合法公開之個人資料。
4.公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料。

文/iThome

出國玩拍護照封面會洩個資？外交部回應了！拍到1資訊直接上不了飛機

（示意圖／李艾庭攝）

風生活綜合報導/2025-04-23 12:38

近日有網友在社群平台Threads發文提醒，出國時別拍攝護照封面上傳社群，否則可能會讓個資外洩，甚至有人指出護照封面上的晶片標誌藏有個人資訊。這類說法引發網友熱議，貼文獲上千次分享與按讚。不過，政府相關單位已出面澄清，這些都是錯誤訊息，護照封面不含個資，晶片資料也無法遠端讀取。

出國玩拍護照封面會洩個資？外交部回應了

根據事實查核中心報導，對於網路盛傳的說法，負責核發護照的外交部領務局與負責製作的中央印製廠皆表示，護照封面本身並不包含任何個人資訊。晶片雖內嵌於護照，但並非設置在封面，護照上的「金色晶片標誌」僅為標示這是一本晶片護照，無讀取功能。

外交部領務局副局長陳尚友進一步指出，晶片資訊必須使用專屬設備，並幾乎與護照貼合，才能成功感應與判讀。即使距離只差幾公分，機器也無法讀取內容。

中央印製廠副總經理楊振億也補充，晶片實際嵌在護照封底的夾層中，外觀上的標誌純屬識別用途，不具任何儲存或讀取功能。

依據外交部資料，台灣晶片護照使用的是「非接觸式晶片模組」，其讀取距離極短，需打開護照並將資料頁貼近機器判讀區，才能透過無線射頻方式讀取。護照若處於閉合狀態，即無法進行任何資料掃描，有效避免資訊外洩風險。

拍到1資訊直接上不了飛機

要小心的不是護照封面，而是訂位的詳細內容。一名網美先前在限時動態曬出飛往南京的來回機票，畫面中清楚顯示訂位代碼與電子機票編碼等個資。沒想到隔天她驚慌發文，表示機票被人退票，自己根本沒操作，還因此得多花近7000元重訂，讓粉絲紛紛指出是因為公開了敏感資訊。

旅遊達人蓋瑞哥提醒，機票上的訂位代碼、機票號碼與乘客姓名都是關鍵資訊，只要掌握其中兩項，任何人都能更改甚至取消機票。此外，登機證上的 QR code 也藏有這些資料，建議出國炫耀時務必遮蔽個資，以免被人動手腳。

責任編輯／梁溶珈