

2024 CISO Insight 資安調查解析 (2)

應對企業資安威脅 禦敵於外與制敵於內並重

CISO Insight 是由 CIO Taiwan 的 CISO 資安學院於 2024 年所公布的問卷調查。問卷內容以資安長的角度出發，探查企業資安策略的實施現況及痛點。本刊邀請多位不同產業的資安長針對調查結果做第一手的系列解讀，上一期談資安治理，本期則是聚焦在瞬息萬變的資安威脅。

採訪／施鑫澤、鄭宜芬

在 AI 時代，資安威脅的複雜性日益增長，成為企業攻防戰的關鍵。本篇邀請多位資安長深入盤點威脅現況與應對策略，分享如何提升企業數位韌性。

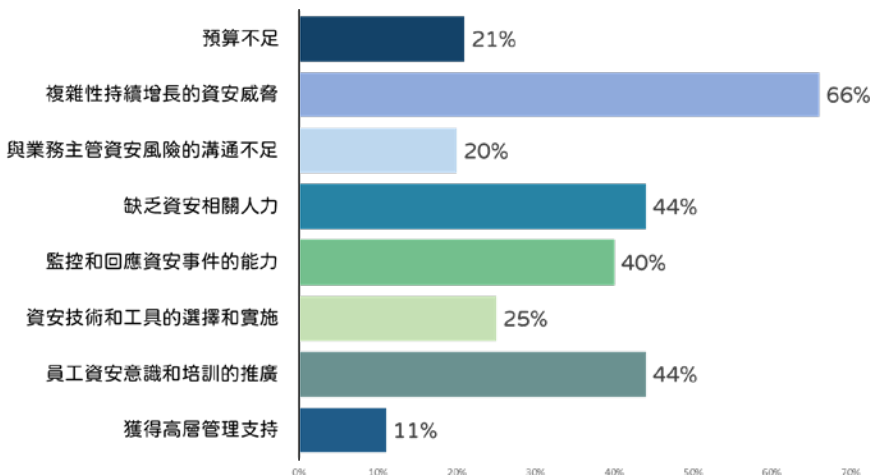
釣魚僅是敲門磚 資料外洩恐無法挽回

隨著全球駭客攻擊手法日新月異，除造成企業重大財損，更對商譽帶來難以彌補的傷害。臺灣是全球駭客攻擊熱區，遭受網路攻擊情況尤為嚴重，位居亞太地區之首。根據本次調查統計，資安長們認為，執行資安策略時，遇到的主要困難是「複雜性持續增長的資安威脅」（66%）（請見圖 1），

這樣的挑戰體現在企業內部時，就反應在另一題關於組織內最缺乏的資安技能和人力，正是與攻擊防禦正相關的「威脅檢測與響應」（32%），這個結果顯示出這些來自四面八方又源源不絕的攻擊行為，讓企業無論在檢測或反應上都顯得倍感壓力。

值得注意的是，從圖 2 及圖 3 可以看到，組織遭受魚叉式網路釣魚攻擊（31%）與惡意程式攻擊（31%）雖然為最大宗，但對於企業的影響僅占約一成（8%+5%）；相較之下，勒索軟體攻擊與資料外洩雖僅各占 8%，但兩者相加對於企業造成的影響卻高達八成（51%+29%）。這些常見或嚴重之不同攻擊方式對企業的影響如下：

圖1 您在執行資安策略時，遇到的主要困難是什麼？



一、魚叉式網路釣魚

可能導致帳號密碼被盜，進而引發更嚴重的攻擊；造成敏感資訊洩露，像是商業機密或客戶資料；特別是如果員工上當受騙，就可能對公司名聲造成損害。

二、惡意程式攻擊

造成系統效能下降，影響日常運作效率；導致資料損壞或遺失；甚至可能為後續更嚴重的攻擊創造條件，例如植入後門程式。

三、勒索軟體攻擊

組織面臨支付高額贖金的壓力；而且即使支付贖金，也不能保證資料能完全恢復；甚至可能造成長期的名聲損害和喪失客戶信任。

四、資料外洩

恐導致敏感客戶資訊或商業機密洩露；面臨嚴重的法律和監管後果，例如高額罰款；造成長期的品牌形象和客戶信任損害；而且需要投入大量資源來調查事件和補救。

合勤投資控股資安長游政卿分析，魚叉式網路釣魚和惡意程式攻擊的高發生率反映了此類攻擊方式常見且容易實施，成本較低，可以大規模進行，所以成為攻擊者的首選手段；相比之下，勒索軟體攻擊和資料外洩雖然發生率較低，但影響卻更嚴重。這種現象的原因主要有以下幾點：

「攻擊複雜度」，勒索軟體和導致大規模資料外洩的攻擊，通常需要較複雜的技術和較久的準備時間，這雖降低了其發生頻率，但也使它們更難防禦；「目標性」，這類攻擊往往更有針對性，攻擊者會精心挑選高價值目標，以獲得最大收益；「影響範圍」，這些攻擊一旦成功，可能導致大規模資料損失、系統中斷，甚至整個業務停

擺，所以影響更深遠；「潛在損失」，勒索軟體可能導致高額贖金支付，而資料外洩可能引發巨額罰款和賠償，這些直接的財務損失往往比其他類型的攻擊更為嚴重。

游政卿強調，考慮到這些影響，資安長的防禦策略需要全面且平衡。既要應對日常的高頻率威脅，又要為那些低頻但高影響的攻擊做好準備。這需要資安長不斷調整和最佳化資安策略，以適應不斷變化的威脅環境。

「駭客索錢最快的方式，就是打企業最痛的地方，綁架企業重要的核心系統。」某位不具名的面板廠資安長指出，從攻擊者的角度來說，用釣魚

圖2 在過去一年中，組織遭受哪種類型的資安威脅最多？

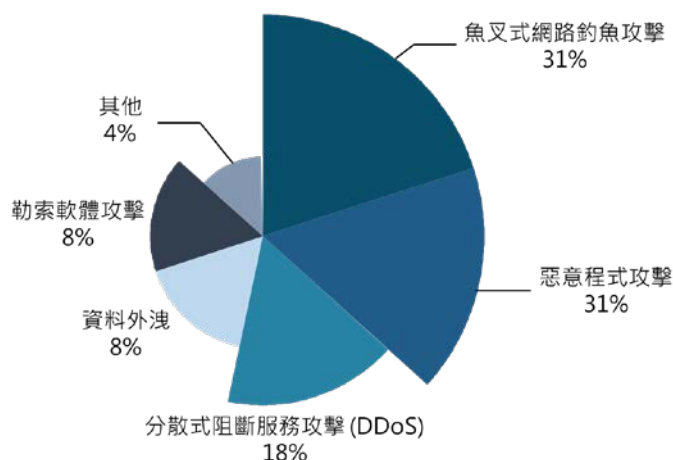
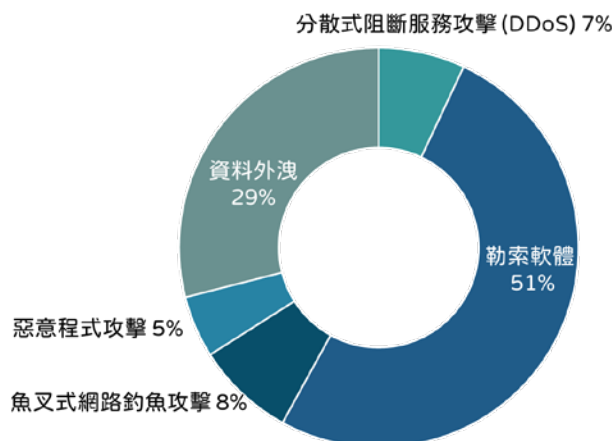


圖3 您認為哪種資安攻擊對企業造成的影響最大？



或惡意程式的方式成本最低，很快就能取得 Initial access（初期存取），進入企業取得憑證，為所欲為。企業的痛點是資料外洩和網路安全，駭客只要攻擊這兩個弱點，贖金便乖乖到手。

佳世達科技資訊長暨資安長黃莉雯補充，魚叉式攻擊近年層出不窮，是鎖定目標的手段，冒用熟人的名義發送郵件，藉由熟悉度降低防備，誘使目標點擊信件或執行其中的指令。這種方式與詐騙類似，假冒親友來博取信任，進而達成攻擊目的。

相較惡意程式攻擊僅是癱瘓網站，駭客的真正目的是金錢，例如通過勒索軟體將系統或資料加密「綁架」，要求受害企業支付贖金以獲得解密密鑰。此外，資料外洩問題日益嚴重，駭客可能將竊取的資料「資料轉售給客戶或商業競爭對手，是企業最大的損失來源。」

遠傳電信資安長朱建國表示，近年勒索病毒盛行，許多企業已加強相關防護措施。然而，儘管業界對勒索病毒的認知逐漸提升，但病毒技術也在持續演進，攻擊手法變得更加多樣化，企業在防禦時需更加謹慎，因為這類攻擊需要投入大量資源來移除。

然而，病毒入侵或惡意程式攻擊的影響雖然嚴重，但透過妥善的應對處理仍能夠復原。一旦資料外洩，即使後續進行補救措施，也無法追回外洩的資料，對企業造成無法挽回的損失。現今的資料竊

取手段常結合多種攻擊工具與管道，包括勒索病毒與資料工程攻擊，防禦不能僅依賴單一方式或工具，需要更全面的策略。全資料加密雖然能有效提高安全性，但並非適用於所有行業。建議企業首先識別資料的敏感性與優先保護的對象，確認資料的集中存儲位置，並根據其特性來制定相應的措施。這種以風險識別為基礎的防護方式，才能合乎企業在資安方面的實際操作性與安全需求。

多層次禦敵於外 多斷點制敵於內

某金控資安長指出，駭客攻擊多以商業目的為主，包括勒索、報復，甚至僅為展示技術實力或「練功」，金融業應依金管會要求，深化各種營運持續計畫（BCP）演練為重，採用策略為「多層次禦敵於外，多斷點制敵於內」，並透過即時偵測與回應，治理加上聯防來確保安全，常用工具如 EDR（端點偵測及回應）、NDR（網路偵測和回應）、XDR（延伸偵測及回應）、Anti-APT（進階持續威脅攻擊防禦）和 SIEM（安全資訊和事件管理）關聯分析，若防護力不足，還可結合網路流量，提升即時偵測能力並予以回應。

尤其要注意的是，「人性的弱點是最大的敵人，會摧毀防禦措施，容易被攻破。」根據 Gartner 2022 年調查顯示，69% 受訪者承認曾為了方便而有意繞過資安控管，更有高達 93% 受訪者坦言其行為可能會增加公司的風險。Gartner 亦於 2024 年將「安全行為與文化計畫」（HBCP）列為重要趨勢。

對於人為因素的資安破口，恰好呼應了此次調查的項目之一：超過半數的資安長認為，組織文化和資安意識是最能影響作為資安長的成功因素（請見圖 4）。

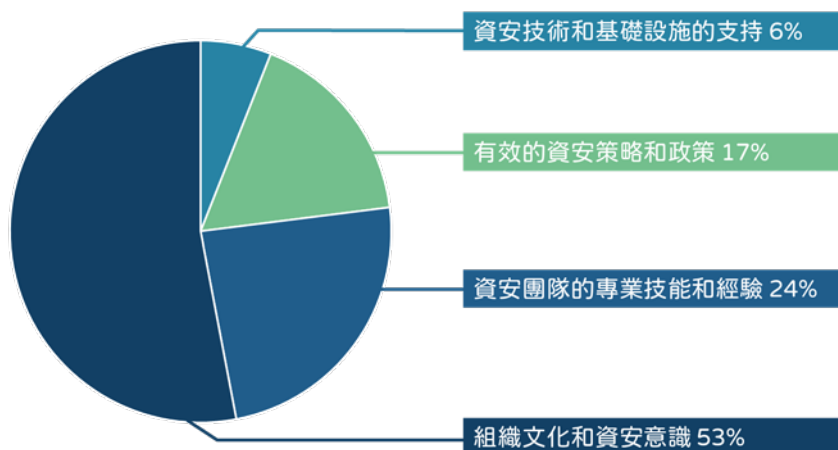
該金控資安長指出，企業即使導入完整的資安防護工具，對任何的網路攻擊仍應保持警戒。尤其現在社交媒體越來越發達，員工的一點小行為就引發重大安全隱患，甚至於將公司內部檔案洩漏出去，因此端點防護相當重要。

針對防範人為因素的資安破口，由於組織文化與紀律是資安防護的基礎，建議主管需積極監管並強化員工意識，還有不斷強化工具與防護措施。然

防範資安攻擊五大策略

- ◆ 加強員工資安意識訓練，特別是針對魚叉式網路釣魚的防範。
- ◆ 實施多層次的安全控制，包括端點保護、網路分段和存取控制等。
- ◆ 建立強大的事件應變和業務持續性計畫，以應對可能的勒索軟體攻擊。
- ◆ 加強資料保護措施，包括加密、存取控制和資料分類等。
- ◆ 定期進行風險評估和滲透測試，以找出和修復潛在漏洞。

圖4 您認為哪項因素最能影響您作為資安長的成功？



而，企業要養成良好的文化與紀律，需要一段時間，需有耐心養成。

而在近年盛行的零信任架構的理念中，即便是內網環境也可能存在駭客威脅，提醒企業應避免盲目追隨流行資安工具，應從有限資源分配，從內至外分輕重應對。

另也提醒，面對生成式 AI 的盛行，善用可以協助處理檔案、應對客戶，但其潛在的詐騙風險亦需謹慎應對。

數位韌性 被攻而不垮

近年臺灣的重大資安事件，包括內政部戶役政資料流入暗網、多家上市櫃公司屢遭網路攻擊，以及時任美國眾議院議長的裴洛西訪臺時，中國駭客入侵臺灣網路，導致超商、臺鐵電視牆、機場官網等機關或場所的網站癱瘓或電子看板內容遭竄改。

「就像人生病才會去看醫生，沒有生病就不會想要吃藥。」彰化基督教醫院資安中心主任粘良祁指出，資安痛點在於大部分的企業預算有限，資安主管多數是由資訊主管兼任，等到事件上新聞才知道自家被打或是服務斷掉，「許多公司怕碰到資安問題，就直接禁止上網，結果面臨很多限制。就像你希望一個人不要溺水，但不知道怎麼辦，於是就禁止游泳。臺灣就變成了『先禁國家』，而非『先進國家』。」

他建議企業應做好根本資安治理來應對攻擊，以彰基為例，資安治理涵蓋範圍廣泛，從採購、人

事及 OT 系統等方面，透過RFP（需求建議書）與評量表把關，並於2019年啟動聯防架構，一旦連線異常便自動斷開使用者設備、及時告警，且與國際資料同步更新，維持資安水準。

粘良祁表示，駭客雖無孔不入，但若攻擊成本過高便會轉向其他目標，數位韌性的關鍵在於「被攻而不垮」，建議企業需持續增強韌性，化被動為主動，才能擺脫墊底挨打的窘境。除了《資通安全事件通報及應變辦法》規定社交工程演練，還有資安教育訓練、加強攻防演練、WAF（應用程式防火牆）、IPS（入侵防護系統）、MDR（受管式偵測與應對）、EDR（端點偵測及回應）等資安工具皆能有效提升防禦能力。

總結資安長們的觀點，在資安威脅日益複雜的現今，企業不僅需要因應高頻率的釣魚和惡意程式攻擊，更必須防範低頻但破壞性甚鉅的勒索軟體與資料外洩。有鑑於此，強化數位韌性是企業資安長期發展的關鍵，包括提升員工的資安意識、採用多層次的技術防護，以及建立強大的應變與恢復能力。面對資安威脅，唯有從策略、技術雙管齊下，並長期培養文化與紀律，才能構築「被攻而不垮」的實力，在快速演變的威脅中立於不敗之地。



掃描 QR CODE
至官網下載完整報告。