# 2025-2026 CISO Insight 調查解析



《2025-2026 CISO Insight 資安調查報告》從 CISO 的視角出發，我們務實地了解企業資安策略的實際執行情況，並藉由最有指標性的統計數據和產業趨勢，協助 CISO 們清楚掌握所屬企業與其他公司的異同，從而更具策略性地制定與優化未來的資安策略。

此次主題涵蓋九大面向：受訪者與人力概況、資安治理與策略、預算、威脅情勢與資安韌性、生成式 AI 的影響、供應鏈、法規遵循與合規挑戰、其他資安重點與展望，以及關於 CISO 自己。

有效份數：157 份
調查對象：2000 大或上市櫃公司資安最高主管
產業比例：高科技製造 36%、金融業 22%、傳統製造 19%、服務業 16%、健康醫療 7%
調查解析顧問團成員：資安院資深顧問（前資安院院長）何全德、合勤投資控股資安長游政卿、漢翔航空工業資訊處處長方一定、遠傳電信資安長朱建國、臺北榮民總醫院資訊室主任郭振宗、中國醫藥大學附設醫院資訊室副主任許凱平等涵蓋各產業與領域之專家。

掃描 QR code
至官網下載完整報告。



資安院
何全德 資深顧問
（前資安院院長）



合勤投資控股
游政卿 資安長



漢翔航空工業
資訊處
方一定 處長



遠傳電信
朱建國 資安長



臺北榮民總醫院
資訊室
郭振宗 主任



中國醫藥大學
附設醫院資訊室
許凱平 副主任

## 01 資安雙面刃 生成式 AI 三大風險與機會

生成式 AI 正改變資安攻防兩端的能力，既能強化威脅偵測與預警，也放大資料外洩與治理複雜度。本篇從 CISO 視角歸納生成式 AI 的三大風險與三大機會，協助企業在創新與控風之間取得平衡，維持資安韌性。

## 02 迎戰 AI 與量子風險 預算是主力配置

AI 武器化掀起治理海嘯，驅使企業重寫網路安全規則。隨著防禦思維轉變，CISO 將資安從成本支出，提升為創造競爭優勢的戰略投資。本文聚焦資源配置重整、零信任架構深化，以及如何以前瞻視野應對 AI 與量子運算的長期挑戰。

## 03 供應鏈動搖企業防線 資安治理問責全面升級

資安風險已從單一技術挑戰，演變為橫跨整個數位生態系的系統性壓力。全球監管機構正同步推動強制問責，將最終治理責任正式推向企業董事會。面對這種高度互聯的供應鏈風險，企業必須重塑防禦邏輯，將供應鏈韌性視為核心治理架構，以穩固企業的生存根基。

## 04 防範威脅三關鍵：零信任、韌性、IT/OT 防線

組織面臨的威脅態勢持續升高，一旦產線停擺或交易受阻，不僅衝擊業務連續性，也可能損及品牌信任。如何透過零信任落地、微分割強化 OT 安全、縮短 MTTD/MTTR，以及提前因應量子時代的加密變革，成為今年 CISO 最關注的核心議題。

## 05 從技術走向治理，CISO 重新定義資安責任邊界

全球監管與法遵壓力正把資安責任推向董事會，迫使 CISO 從技術專家轉為治理與策略角色。面對 AI 風險與治理負擔，如何重塑人力、整合防線，將成為 2026 年企業韌性關鍵。本次解析聚焦資安領導者如何在變局中重構策略，掌握主動權。

# 資安雙面刃　生成式 AI 三大風險與機會

## 2025-2026 CISO Insight資安調查解析-1

**生成式 AI 正改變資安攻防兩端的能力，既能強化威脅偵測與預警，也放大資料外洩與治理複雜度。本篇從 CISO 視角歸納生成式 AI 的三大風險與三大機會，協助企業在創新與控風之間取得平衡，維持資安韌性。**

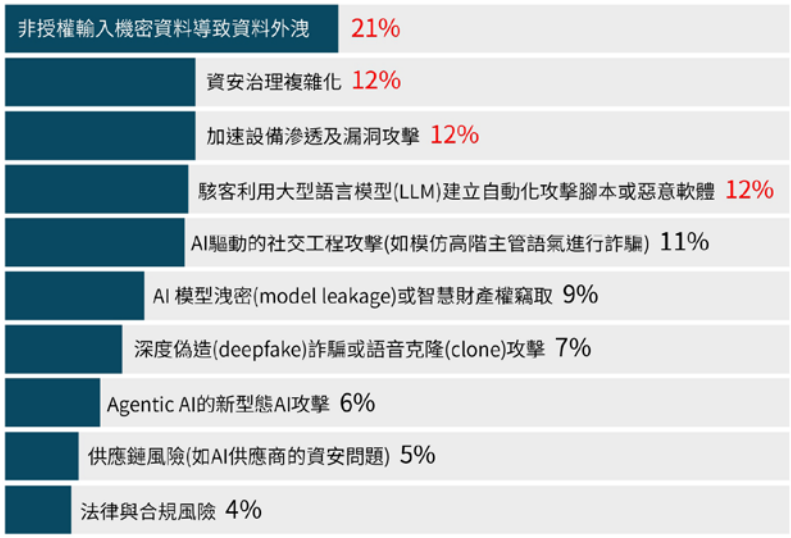
文／鄭宜芬

「生成式 AI 改變了資安的攻防遊戲規則」，前資安院院長何全德引述《微軟 2025 數位防禦報告重點分析》指出，威脅行為者積極將 AI 投入實際作戰，應用方式涵蓋整個攻擊鏈，包括自動化整個攻擊生命週期、規模化社交工程、合成身分詐欺，以及攻擊 AI 模型本身。

AI 正從根本上改變網路戰爭的攻防不對稱性。在過去，防禦比攻擊更困難、成本更高。現在 AI 驅動的攻擊工具降低了技術門檻，讓低技能攻擊者也能發動複雜攻擊，進一步加劇了這種不對稱。

然而，AI 也為防禦方帶來了革命性的變革，包括規模化防禦、壓縮應變時間，以及主動式威脅獵捕。能在企業範圍內運作的 AI 驅動防禦工具，有望扭轉這種不對稱性。未來的網路安全將是 AI 系統之間的戰鬥，缺乏 AI 增強防禦的組織將處於災難性的劣勢。

圖 1 最關注的生成式 AI 資安風險類型



## 三大風險：資料外洩、複雜化、加速滲透

面對生成式 AI 日益普遍，漢翔航空工業資訊處處長方一定表示，CISO 最關注的資安風險類型如下：（見圖 1）

- **非授權輸入機密資料導致資料外洩（21%）**

高科技製造業的核心在於 CUI（受控的非機密資訊），如技術圖紙、藍圖、ITAR（國際武器貿易條例）控制的文件。一旦員工未經授權將這些高價值的智慧財產權輸入公開的生成式 AI 模型，將造成不可逆轉的資料洩露，直接違反合規要求，甚至喪失合約資格。

- **資安治理複雜化（12%）**

此次調查顯示，許多企業在使用生成式 AI 時，尚未建立完整框架的風險評估機制（34%）。（見圖 2）生成式 AI 的導入使傳統資料分類和存取控制框架面臨挑戰，企業難以追蹤資料流向。這對於需要嚴格管控 CUI 邊界和資料流的高科技製造業而言，會直接威脅到其資安成熟度與合規性。

- **加速設備滲透及漏洞攻擊（12%）**

生成式 AI 能被駭客用於建立自動化攻擊腳本或惡意軟體。由於營運中斷對公司影響最大（58%），駭客利用 AI 加速發現 OT／工控系統、研發系統的漏洞並進行滲透，將極大提升製造業面臨的即時威脅水平，使得防禦難度與反應速度要求大幅提高，營運中斷風險急遽升高。

## 三大機會：強化分析、自動化營運、提升威脅預警

與此同時，AI 也為防禦方帶來了革命性的改變，圖 3 顯示，CISO 認為生成式 AI 帶來三大主要機會：提升威脅識別與預警能力（30%）、提升資安分析效率（22%）、自動化資安營運任務（15%）。

方一定表示，現有知名的資安大公司所提供的資安防護，都是以某一功能性為主，在公司必須靠收容所有資安設備 Log後，由 SOC 資安監控中心進行關聯分析，才提早發現 APT 類型的駭客行蹤，而且仍有許多工作必須靠資深有經驗的資安專家來解析。只要是人就有時間限制及疏失，因此怎樣運用 AI 來達到 7X24hr 監控及即時無誤的阻斷作為至關重要，必須靠上述這三項能力。

合勤投資控股資安長游政卿表示，過往高科技製造業每天面對幾萬條 log、幾百個事件，SOC 團隊八成的時間都耗在排除誤報。現在透過 AI，能在幾分鐘內完成關聯分析，把一萬條 log 收斂成三個真

圖 2 是否有生成式 AI 的資安風險評估機制？

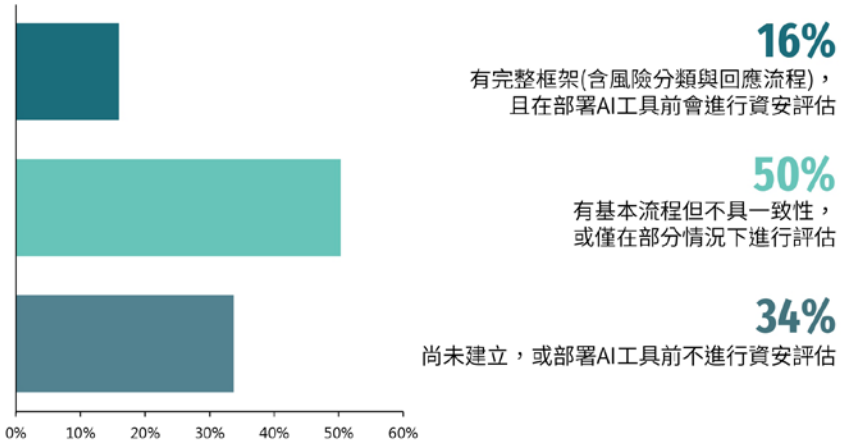
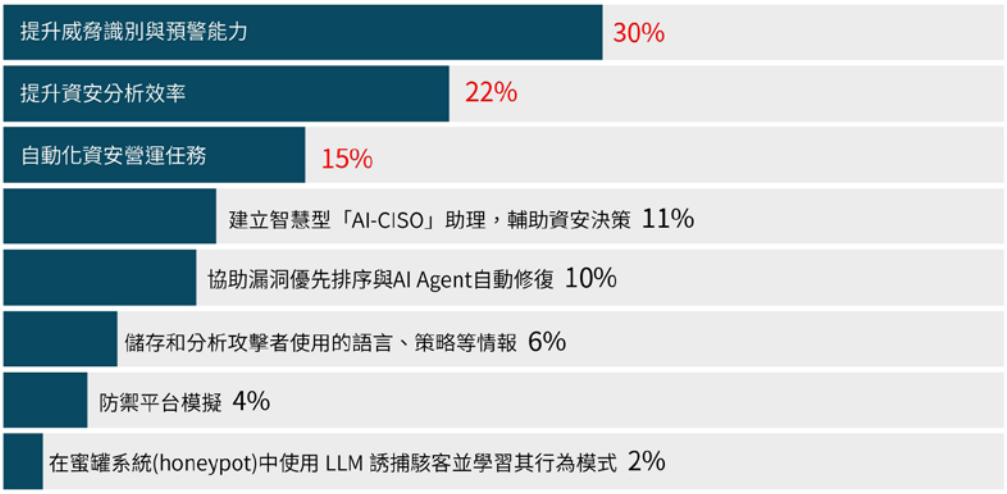


圖 3 生成式 AI 能為企業資安防禦帶來的機會




正需要處理的事件，分析師不再被警報疲勞拖垮，可以專心於高價值的威脅狩獵上，也就是提升分析效率（22%）與自動化營運（15%）。

同時，AI 能協助人發現那些人眼看不出的異常軌跡，例如潛伏數週、跨網段移動的 APT 攻擊，當分析師從「追著警報跑」變成「主動找問題」，整個防禦思維就不一樣,就是提升威脅識別與預警能力（30%）的長期價值。

工研院產科國際所資料亦指出，台積電的專屬機密資訊保護政策（PIP）控管導入 AI，透過大數據監控內部是否有不正常的連線，以及遠端連線回公司時是否有不正常的動作；聯電導入 AI 即時分析駭客威脅資訊，讓防毒系統更完備。

## 分階段、分環境導入 AI 強化漏洞管理

此次調查亦顯示，有一成（10%）的組織已利用 AI 協助漏洞優先排序與 AI Agent 自動修復。

游政卿提醒，AI 的判斷再精準，也不代表每個環境都適合讓它全自動執行，合勤的策略是分階段、分環境導入。

**・ AI 漏洞優先排序**

過去 CVSS（通用漏洞評分系統）分數常會誤導判斷，現在合勤已導入 AI 漏洞優先排序，整合外部威脅情資、內部資產清單（SBOM），再結合攻擊可被實際利用的程度（EPSS，漏洞利用預測評分系統），算出真正的風險排序。優先修補「駭客已在利用、而且組織環境確實存在」的漏洞，再用 LEV（攻擊可能性分級值）作為參考，讓修補程式部署的流程更精準，也更有依據。

**・ AI 自動修復**

在 IT 環境裡，AI 可自動執行低風險、可回復的動作，例如隔離中毒筆電或封鎖可疑 IP。但在 OT 或 R&D 環境，絕不讓 AI 自行下判斷，這些環境的系統高度敏感，誤判就可能造成停線。目前合勤審採取的方式是「AI 輔助決策、人工確認執行」，AI 可以提出建議與生成修補程式，但最後的「執行」仍由維運人員按下。

## 高權限 AI Agent 與資料串接成新風險

金融業面對高監管壓力，嚴謹控管生成式 AI。某金控資安長表示，行內策略包括：一、在隔離環境中使用；二、禁止將個資輸入模型；三、禁止使用公開免費的語言模型；四、透過 DLP（資料外洩防護）等傳統機制進行控管；五、發布全行適用的 AI 安全

指引；六、由總經理主持「AI 治理委員會」，並依據金管會「金融業運用人工智慧（AI）指引」，擬定風險分級方法，考量使用對象、對客戶權益的影響、是否有人機協作等，決定對應的控制強度、核准層級與安全檢核深度。

他提醒，未來須注意 AI 應用的兩大風險：AI Agent 相當於一個擁有權限的內部員工，若被攻擊者控制恐造成災難（新型態 Agentic AI 攻擊 6%）；以及 AI 應用間的資料串接，若權限或 Token 管理疏失，可能造成大型資料破口，不可不慎。（資安治理複雜化 12%）

## 對外導入資安檢測 對內統一平台管控

此次調查顯示，86% 組織採用生成式 AI 工具（60% 有條件允許使用＋26% 完全開放）（見圖 4），但 34% 缺乏風險評估機制，僅 16% 有完整框架，並在部署 AI 工具前進行資安評估(見圖 2)。且 36% 沒有明確定義或宣告同仁使用 AI 工具的管理機制（圖 5）。

某面板廠資安長透露自家策略，對外與對內設置兩大不同的策略：

**・ 外部應用：產品導入 AI 的資安檢測**

將 AI 整合至產品時，要求高於一般產品，需進行 AI 資安檢測，確保符合法規、模型安全、具備 Prompt Injection 防護，並以測試工具驗證產品上市時不含機敏資料或已進行遮蔽。

**・ 內部使用：統一平台管控**

為避免同仁直接連接外部 AI 服務，採用統一平台以控管資料外洩風險（包括營業秘密、個資等）。平台可過濾與監控資料，並推動 AI 安全開發生命週期（SSTLC），以因應 Prompt Injection 在內的各類漏洞。

遠傳電信資安長朱建國則表示，為解決根本問題，公司主動提供可讓員工安心使用、滿足業務需求的 AI 環境與平台，並訂定規範與教育訓練，以降低影子 AI／影子 IT風險。針對既有 AI 服務，亦導入檢測工具。

## 不同層級決策者如何推動 AI 韌性

何全德引述《駕馭複合危機：2025年全球網路安全格局與韌性要務戰略報告》指出，面對人工智慧軍備競賽，不同層級的決策者應參考不同的策略，明確其在建立組織韌性中的角色與職責。

**・ 董事會／執行長（CEO）**

制定全組織範圍的 AI 治理政策，明確風險容忍度與安全部署原則。將 AI 安全視為戰略性投資，而非

圖 4 企業是否允許員工使用生成式 AI 工具？

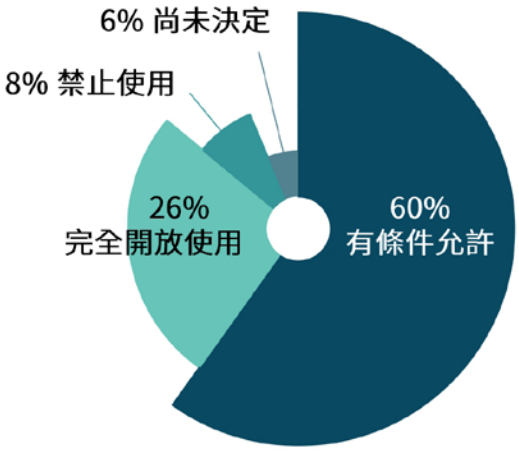
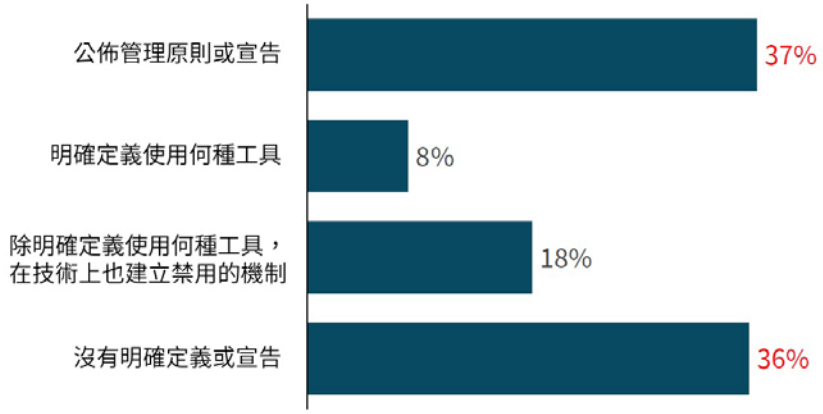


圖 5 是否有明確的生成式 AI 管理機制




僅是 IT 支出。

- **資安長（CISO）與安全領導團隊**

應建立 AI 安全評估流程（AI Security Assessment），強制所有 AI 工具在部署前通過審查。利用 AI 驅動的防禦工具（如 AI 原生 SOC）提升威脅偵測與回應速度。

- **IT／營運團隊**

實施 AI 模型與數據的安全監控，防範模型中毒與數據洩露。對開發人員進行安全 AI 編碼實踐的培訓。

## 模型開發與應用 確保隱私、建立審查流程

在開發與應用 AI 模型時，必須同時確保資料隱私與系統安全，才能避免非授權輸入機密資料導致資料外洩（21%）。

臺北榮民總醫院資訊室主任郭振宗表示，北榮擔任衛福部推動的負責任 AI 執行中心，在前期設計與開發階段，醫院與開發者需符合三大要求：資安與隱私保護、透明可解釋性、生命週期管理。

在驗證與取證階段，臨床 AI 取證驗證中心整合不同層級醫院的資料庫、導入 FHIR 以蒐集驗證用資料。審查時亦重視資料規模、族群代表性、模型於真實臨床環境的效能與安全性；上線後，亦需持續監控效能、偏差、資料漂移、資安事件等。

為避免臨床決策誤用，院內明確定位所有生成式 AI 工具僅能作為輔助用途，臨床決策仍須由醫師判斷。導入前由院內 AI 審查委員會（含臨床、資安、法遵）審核模型用途與風險。另制定 AI 輔助報告審閱 SOP，提供臨床使用指引。並建立 AI 使用後的追蹤與回饋機制，蒐集誤用案例，同時定期評估模型表現與臨床一致性。

總結 CISO 們的觀察，生成式 AI 對企業資安的影響已超越技術層面，成為治理與文化的議題。生成式 AI 改變了防禦的速度與思維，讓分析師有更多時間思考真正的風險。然而，生成式 AI 對機密資料洩露的潛在影響是不能容忍的，對 CISO 來說，AI 既是挑戰，也是重整資安流程、提升韌性的契機，必須將 AI 的妥善使用納入資安治理的重點，才能確保創新與風險可控。

# 迎戰 AI 與量子風險 預算是主力配置

## 2025-2026 CISO Insight 資安調查解析-2

**AI 武器化掀起治理海嘯，驅使企業重寫網路安全規則。隨著防禦思維轉變，CISO 將資安從成本支出，提升為創造競爭優勢的戰略投資。本文聚焦資源配置重整、零信任架構深化，以及如何以前瞻視野應對 AI 與量子運算的長期挑戰。**

文／明雲青

據統計，資安預算投入三大方向為終端設備（24%）、地端設備（23%）與雲端防護（12%）。資本支出與營運支出約各半（41%）。（圖 1、2）

網路威脅的演變，已讓資安最終責任從機房轉移至董事會。前國家資通安全研究院院長何全德強調，資安早已不是 IT 人員的工作，而是企業高層的責任，與財務、法務並列為治理核心。這種根本性的觀念轉變，標誌著資安已成為公司財報與股價的關鍵影響因素。

遠傳電信資安長朱建國指出，資安預算主要由客戶期待驅動，這將推動整體投資持續上升。對資安體系相對成熟的企業而言，當前預算編列重點已不在總量擴張，而在於分配結構的優化與治理效能的提升。

當企業能夠自信地向客戶保證「您的資料在我們這裡受到最嚴謹的保護」，所傳遞的是一份可轉化為訂單的信任價值。

### 情資驅動的預算重塑，從邊界防禦走向早期預警

資安預算的增加趨勢與不斷進化的威脅情勢緊密相關。漢翔航空工業資訊處處長方一定指出，生

圖 1 資安預算主要投資項目

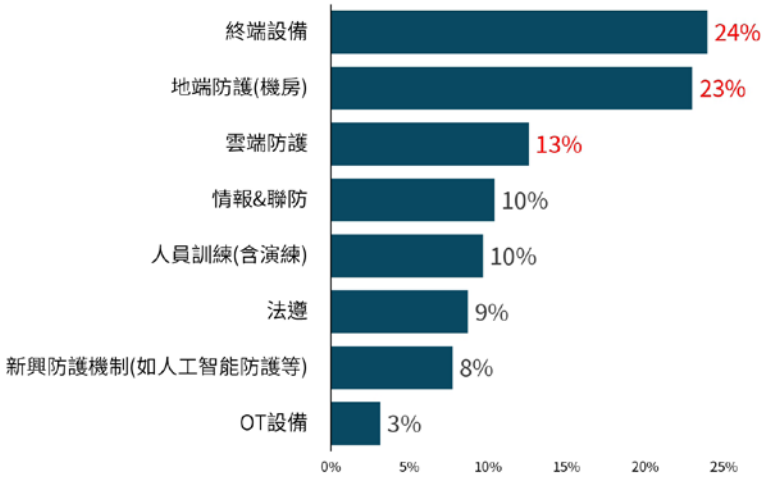
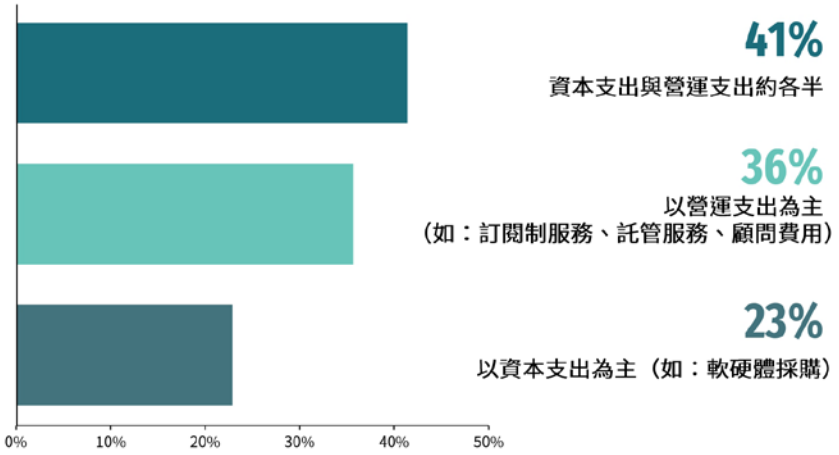


圖 2 企業資安預算的支出類型佔比




數與頻率大幅增加，2026 年的預算將增加雲端防護與相關投資。

為了更早發現異常行為，臺北榮民總醫院資訊室主任郭振宗說明，以往該院的預算著重於 A 級公務機關應辦事項的投資，以建立基礎防護與合規能量為主，目前院方正評估導入 AI 資安產品，用於對 EDR log 進行分析及偵測，將防禦重心從被動防護轉向主動預警。

一位不具名的金融業資安長表示，資安控制強度應依據風險的程度來決定，將寶貴預算資源投注在高風險情境的防護上。

成式 AI 被普遍視為驅動 2026 年資安預算增長的最主要原因（25%）（見圖 3）。

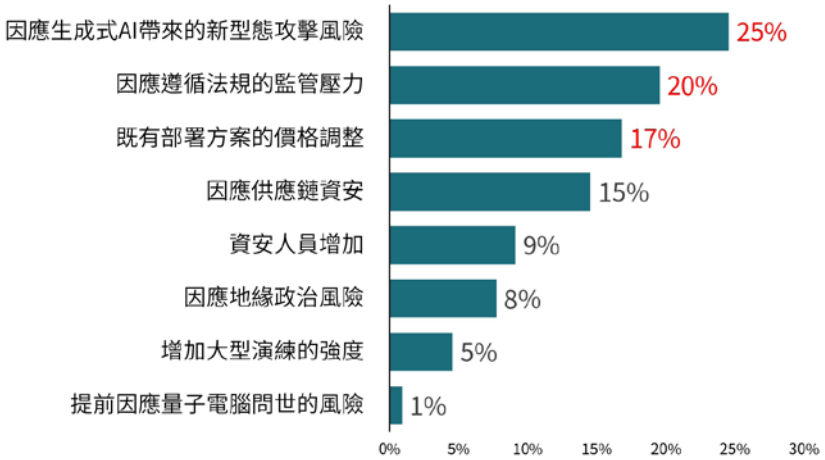
朱建國觀察到，結構性調整後的投入重點是威脅情資，這代表企業從過去被動的事後應變，轉向透過強化情資作業，期望在事件潛伏階段就取得告警線索，連帶使得「資安可視性」成為企業競相追逐的熱門投資。他同時提到，預算浮動增加的原因還包括既有部署方案的價格調整、以及業務持續擴展，需擴充現行防護機制來覆蓋新的服務象限。

某面板廠資安長表示，由於雲端被攻擊的次

## 駕馭 AI 雙重挑戰，以零信任深化治理框架

面對攻擊從「駭入」轉向「登入」的趨勢，零信任架構成為實現網路韌性的技術藍圖。方一定指

圖 3 資安預算增加的主要原因



出，零信任架構必須先確認保護範圍，涵蓋公司內關鍵數據、資產、應用程式和服務的加密保護，確保萬一檔案遭竊時無法被解密讀取。

合勤投資控股資安長游政卿補充，談及 AI 治理，CISO 應扮演稱職的「翻譯官」角色，負責幫 AI 這個業務加速器「裝上煞車、加上行車紀錄器」，以協助企業解除對 AI 的最大隱憂：非授權輸入資料、導致機密外洩。

某面板廠資安長表示，公司採用統一平台的方式，避免同仁直接連到外部的 AI 服務，以便針對機密資料外洩進行過濾或監控。

游政卿建議將 AI 視為「數位員工」，遵守最小權限與完整日誌的原則。他強調，尤其在 OT 或 R&D 等敏感環境中，資料外洩的衝擊遠超過一般業務系統。因此，企業應採取「AI 輔助決策、人工確認執行」模式，因為即使 AI 是優秀的副駕駛，但方向盤必須永遠掌握在公司同仁手上。

## 量子威脅逼近，投資重心轉向治理與技能韌性

真正的韌性，不僅要求應對當前威脅，還需要為未來的典範轉移做準備。據統計，目前仍有 51% 尚未評估或導入 PQC 相關技術（見圖 4）。

前國家資通安全研究院院長何全德強調，企業必須為量子運算時代的到來做好準備。這意味著必須應對敵對方正在今天攔截並儲存加密數據的「先獲取，後解密」（HNDL）威脅。

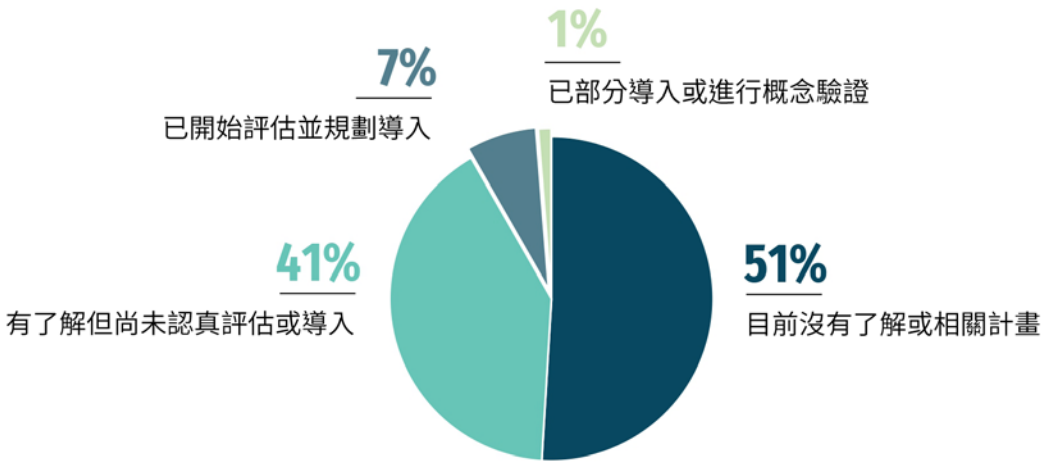
朱建國以電信業為例指出，企業在導入類似於 PQC 等前沿技術時，應依循國際標準的成熟度來決定導入時機與節奏，前期宜以少量概念驗證與趨勢掌握為主。

此外，資安的重點仍在於人、系統與資料等三大核心面向，所以當今投資策略重點應著重於持續訓練、高擬真演練與優化通報機制，以強化整體組織對突發事件的應變能力。

方一定認為，生成式 AI 帶來的最大機會是提升威脅識別與預警能力，這有助於讓有限的資深專家能專注於高價值的調查工作，以應對資安人才短缺的挑戰。

總結來說，面對 AI 與量子的長期威脅，CISO 的角色已從成本的控管者，轉變為資源的戰略配置者。透過情資驅動預算結構，深化零信任治理框架，企業得以掌握主動權，將資安提升為獲取客戶信任與商業價值的核心驅動力。

圖 4 是否已開始評估或導入量子防禦密碼學（PQC）相關技術？



# 供應鏈動搖企業防線 資安治理問責全面升級

## 2025-2026 CISO Insight 資安調查解析-3

**資安風險已從單一技術挑戰，演變為橫跨整個數位生態系的系統性壓力。全球監管機構正同步推動強制問責，將最終治理責任正式推向企業董事會。面對這種高度互聯的供應鏈風險，企業必須重塑防禦邏輯，將供應鏈韌性視為核心治理架構，以穩固企業的生存根基。**

文／明雲青

網路安全戰場已明確從企業防火牆邊界，轉向高度分散的供應鏈節點。前資通安全研究院院長何全德指出，駭客偏好攻擊資安防護最薄弱的中小企業，因其投報率高、滲透成本低。使得大型企業最致命的破口，往往來自一個防禦鬆懈的小型外部供應商。

合勤投資控股資安長游政卿指出，因供應商資安成熟度落差極大（33%），實務上難以用單一標準管理上千家合作廠商（15%）。另外，20% 組織難以確認供應商是否有確實遵守要求（見圖 1）。

這些挑戰使供應鏈成為最大障礙，全球54%的大型組織亦持此看法（出自 WEF《Global Cybersecurity Outlook 2025》報告）。

何全德強調，駭客可輕易入侵防禦鬆懈的小型供應商，使之成為大型企業防線致命破口，因為一旦協力夥伴被攻陷，再堅固的內部防線也形同虛設。

### 重構防線思維，供應鏈成資安韌性支柱

為降低供應鏈資安風險，22% 組織定期稽核及演練、17% 遵守產業標準並共同遵守、12% 提升第三方依存關係的可視性（見圖 2）。

遠傳電信副總經理暨資安長朱建國指出，供應鏈資安策略須因應不同產業情境與供應商特性進行調整。在產品供應商眾多的成熟市場中，甲方若未明確定義資安規格，將無法有效落實風險控管。

漢翔航空工業資訊處處長方一定表示，對於航太高科技製造業而言，第三方認證已是進入市場的基本門檻。漢翔透過開發供應鏈資安評級系統（SISAS）輔導下游廠商，將合規工作轉化為產業服務，以提升整體生態系的資安治理能力。

某面板廠資安長指出，公司對供應鏈的管理策略，先從自評問卷與第三方稽核起步，並未直接套用合約條款，因合約必須依據供應商能力彈性制定。

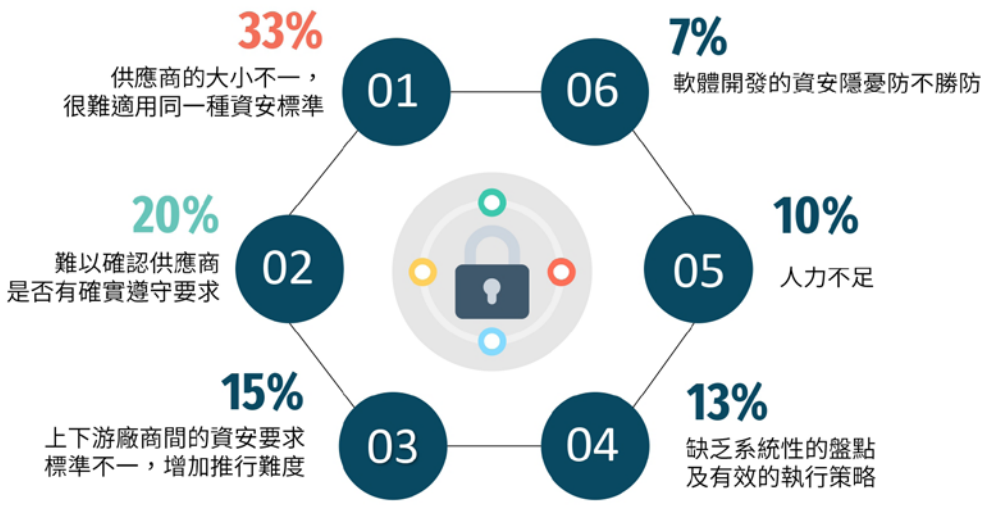
臺北榮民總醫院資訊室主任郭振宗補充，在實際供應鏈審查中，除合約條款與自評問卷外，院方也會在履約過程抽查曾發生資安事件的供應商，確保防護完整性。

何全德強調，CISO 必須在合約中明訂對委外廠商的資安稽核權，因現行法規已將 CISO 列為供應鏈資安事故的連帶責任人。這屬於責任延伸，而非單純風險轉移。多位資安長一致認為，集體防禦已不再是可選的選項，而是保障自身核心生存的重要措施。

### 法規問責升溫，資安治理直指董事會

全球監管機構正同步推動資安治理的透明化與公開化。游政卿形容，對全球佈局的跨國企業而言，法規遵循已成一場「多重合規的馬拉松」。

圖 1 供應鏈資安難以落實的關鍵原因

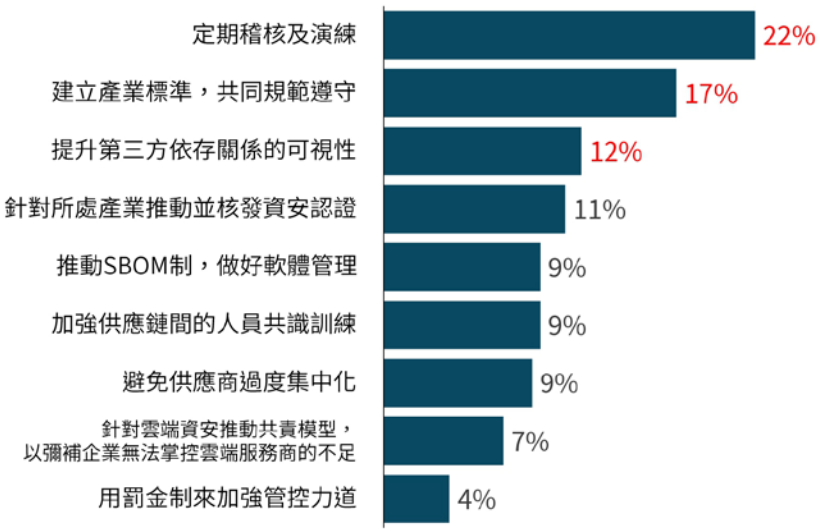



美國證券交易委員會（SEC）的新規定要求上市公司在重大資安事件發生後，須在4個工作天內，透過 8-K 文件揭露事件的性質、規模及對公司的影響。顯見資安治理績效的量化，正快速成為評估一家企業價值的標準配備。

最終，企業資安治理的好壞將成為強制揭露、須經過會計師查核的項目，將直接影響企業的股價與商譽。

一位不具名的金融業資安長指出，法規與規範通常只是最低底線，真正關鍵仍在於企業自身的風險控制力度。他認為多數金融機構會依據風險程度調整資安控管強度，風險越高，所需施加的控管力道必須遠高於法規門檻。

圖 2 可以有效降低供應鏈資安風險的方法




## 法遵為槓桿，打造資安驅動的營運優勢

郭振宗說明，醫療院所必須嚴格遵守個資法（42%）、醫療法與資安法（37%）（見圖 3），但在兼顧資料共享與合規性時，其核心思維是執行資料分級。他指出，如基因這類極高度敏感的資料，原則上不得釋出到外部環境，必須在像是健保署加值中心這類封閉環境執行 AI 訓練。

某面板廠資安長則提到，由於其在歐盟境內設有子公司，需嚴格遵循 GDPR 規範（10%），因而將資料跨境使

## 圖 3 目前須遵守之主要資訊安全/隱私法規




37% 資訊安全管理法(台灣)
3% CIRCIA / HIPAA (美國)
1% DORA / NIS2(歐盟)
10% GDPR(歐盟)
3% 無明確跨國法規壓力
1% 新加坡網安法
1% 日本 APPI

用列為當前最嚴峻的挑戰。

資安長們普遍面臨的挑戰，與此次問卷結果高度契合，主要包含：人力與工具不足以應對合規要求佔 21%，以及執行各項規定增加營運複雜度佔 19%（見圖 4）。

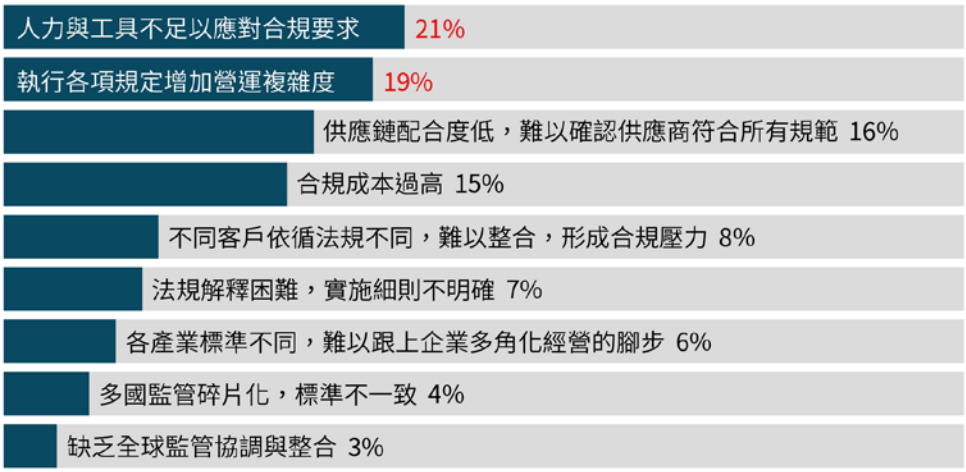
游政卿強調，CISO 在向董事會溝通資安事項時，不能只談法規要求或技術詞彙，而是要將不合規的風險轉化為可量化的營運風險，從而讓資安和法遵投資成為有效的避險工具。並且對供應鏈採取分級制度：要求高風險供應商（核心廠）須有第三方稽核或認證；對於中風險供應商，透過合約條款約束，並要求填寫資安自評問卷；至於低風險供應商：在合約中納入基本資安條款即可。同時，團隊在系統開發與採購初期就導入「Secure by Design」的概念，把法規要求內建進流程。這樣不僅降低後期修正成本，也讓資安與法遵成為營運日常的一部分。

何全德指出，臺灣「個人資料保護法」是一堂必修課，只要公司有收集客戶資料，就有法律義務善加保護。值得留意的是，法律懲罰重心已從「是否外洩」轉向「是否盡責」。

最後，朱建國建議，即使非資安法適用對象，也可參考其法規內容，因它提供完整且落地的技術性規格，可作為企業制定安全設計準則的明確指引。

面對資安與合規風暴交織的未來，企業唯有將資安從成本中心轉化為信任與競爭力的引擎，才能在風險中創造韌性，在壓力中贏得市場。資安不再只是防線，而是體現商業價值的護城河。

## 圖 4 合規工作主要挑戰



# 防範威脅三關鍵：零信任、韌性、IT/OT 防線

## 2025-2026 CISO Insight資安調查解析-4

**組織面臨的威脅態勢持續升高，一旦產線停擺或交易受阻，不僅衝擊業務連續性，也可能損及品牌信任。如何透過零信任落地、微分割強化 OT 安全、縮短 MTTD/MTTR，以及提前因應量子時代的加密變革，成為今年 CISO 最關注的核心議題。**

文／鄭宜芬

網路詐騙（33%）、DDoS 攻擊（17%）及勒索軟體攻擊（10%）仍是 2025 年最常見的攻擊類型（見圖 1）。對組織影響最大的資安攻擊則是營運中斷（58%）與資料外洩／個資洩漏（19%）（圖 2）。尤其製造業與金融業一旦遭遇勒索或系統癱瘓事件，就可能造成產線停擺、交易延遲與品牌信任受損。

### 零信任＋微分割 強化 R&D／OT 韌性

對高科技製造業來說，產線停擺造成的損失以分鐘計。合勤投資控股資安長游政卿表示，合勤在提升韌性的實務上，分成兩大面向對策：R&D（研發）和 OT（產線）。

- **R&D 防止智慧資產外洩：**

落實零信任原則與行為分析，一旦行為偏離常態，系統就會即時標記並通報（45%，見圖 3）。

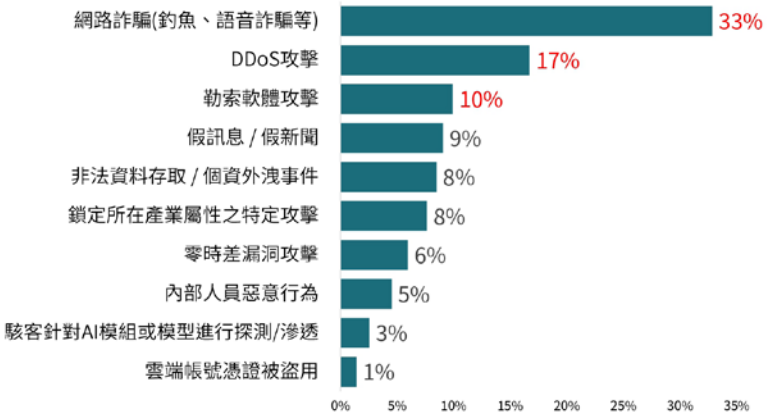
- **OT 防止營運中斷：**

針對產線設備採取「圍堵」，透過微分割，把產線劃分為許多獨立小區塊，就算 A 區被滲透，也不會蔓延到 B 區。風險就能從「全廠停擺」縮小成「單點事件」。

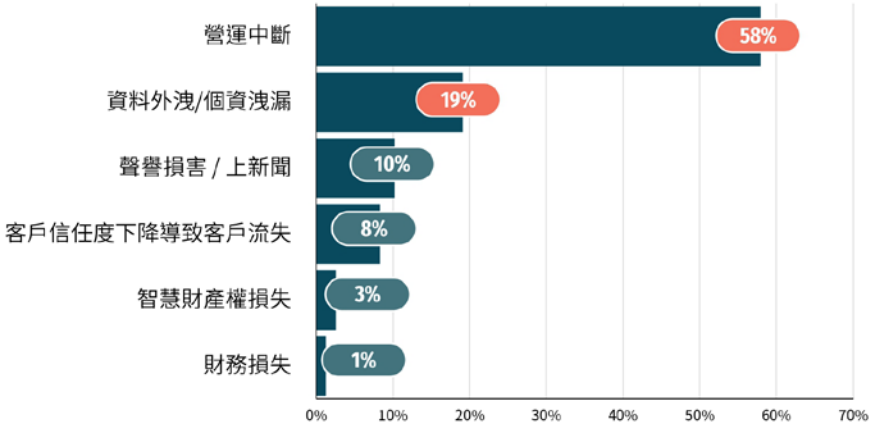
漢翔航空工業資訊處處長方一定表示，漢翔以三大策略確保資安韌性：

一、建立回應與復原機制，如關鍵資訊系統異地備援，盤點資產風險、制定復原時間目標（RTO）、復原點目標（RPO），並透過演練來確保在

圖 1 在過去一年中最常遭受的資安威脅



## 圖 2 哪種資安攻擊對企業造成的影響最大？




可容忍的時間恢復並驗證有效性。另外，建置足夠的縱深防護，將受影響範圍縮小，以及營業秘密及機敏檔案一律加密保護。

二、研發機敏資料除加密外，部分研發部門採實體隔離。

三、OT 網路採取東西向隔離互不通、南北向（連線至 IT 資料擷取僅限讀取、必要時加裝防火牆、封包偵測、分析與監控網段內容）、最小權限、限定 IP 等措施。

### 零信任落地兩大挑戰：系統整合與使用者慣性

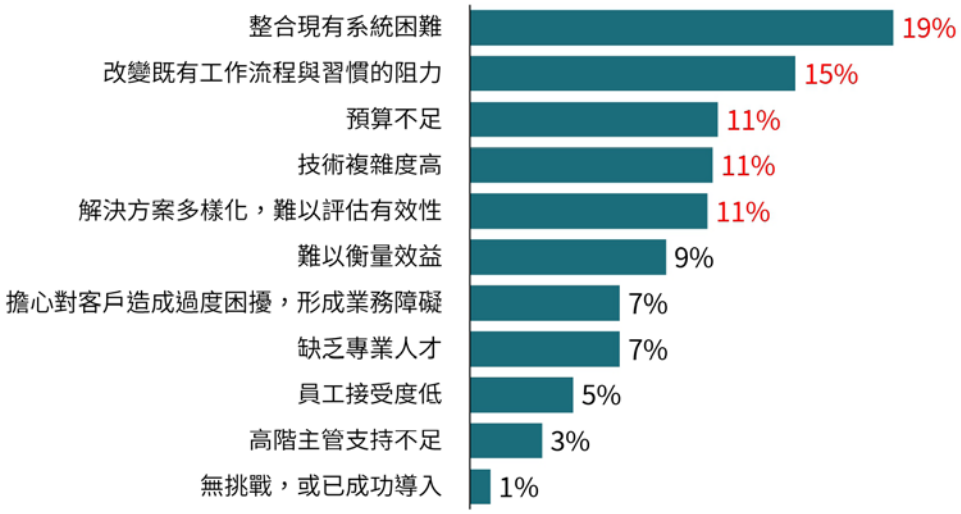
此次調查亦顯示，組織在導入零信任（Zero Trust）架構時，面臨整合現有系統困難（19%）和改變既有工作流程與習慣的阻力（15%）這兩大主要挑戰（見圖 4）。

游政卿表示，針對系統整合困難，合勤的做法是「包裹」，在舊系統前面加一層「零信任閘道」，原系統不動，但任何進出的人（或系統）都得先驗證身份，這樣既可控管又不影響既有穩定性。

## 圖 3 在面對資安事件或疑慮時，內部是否有通報及支援機制？



## 圖 4 導入零信任架構時遇到的主要挑戰




至於慣性阻力，員工抗拒的其實不是安全政策，而是「麻煩」。建議策略是讓安全變得「更方便」，例如導入 SSO（單一登入），員工只要登入一次，後端自動完成多數驗證，阻力自然就消失了。

方一定表示，導入零信任必須先確認保護範圍，由公司最關鍵且最具價值的數據、資產、應用程式和服務（DAAS）組成。並建立三大保護機制：多重驗證、限時最小授權並預設已經遭到入侵，持續監控、偵測、記錄、分析，同時具備災難復原能力。

有效的零信任策略不只是單一技術，應結合多種技術及方法，包括：身分與存取管理、多因子認證、網路監控與網路微分割、端點安全與裝置狀態檢查、持續監控與 SIEM（安全資訊和事件管理）整合、事件模擬與演練。

漢翔先在關鍵環節逐步導入零信任元素，並透過風險評估與優先排序，漸進式推動，結合公司內

## 圖 5 當前資安韌性的最大挑戰

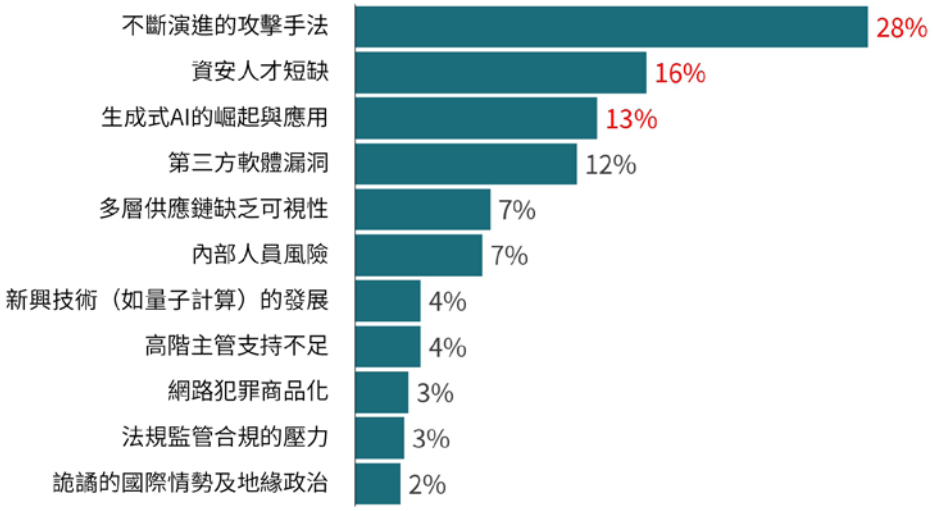
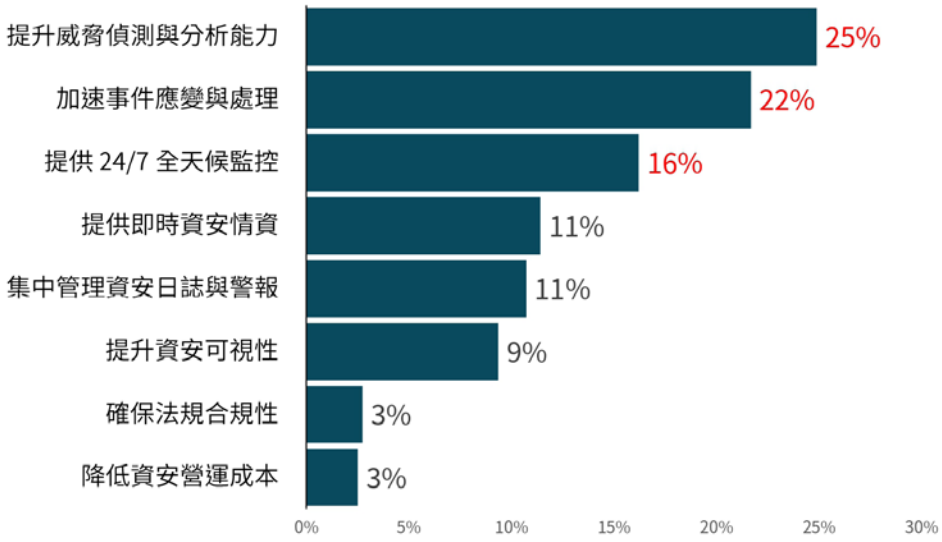


圖 6 資安營運中心（SOC）在資安防禦上貢獻度較高的功能




既有的 CDM（網路防禦矩陣）與零信任實作方向，橫軸為 NIST CSF 的 I（辨識）、P（保護）、D（偵測）、R（回應）、R（復原）；縱軸為使用者、裝置、應用程式、網路、盤點，逐一實現來克服挑戰。

## 多層次防禦＋教育訓練 縮短 MTTD 與 MTTR

面對攻擊手法不斷演進（28%，見圖 5），資料外洩風險持續升高。CISO 們認為，資安營運中心（SOC）的主要貢獻，包括提升威脅偵測與分析能力（25%）、加速事件應變與處理（22%）、提供 24／7 全天候監控（16%）（圖 6）。

遠傳電信資安長朱建國表示，公司定期進行社交工程、勒索病毒等演練，以及技術型測試與 Paper Drill（書面演練），持續改良通報機制與制度，並成立資安事件調查應變小組，確保遇到事件能快速反應。

為避免災害擴大，遠傳以多層次防禦縮短偵測時間（MTTD）與事件快速回應（MTTR）。第一層是提升員工資安意識訓練，降低點擊成功率；中間關鍵層是縮短偵測時間，透過 EDR（端點偵測回應）與異常行為監控等，在事件擴大前即時處置；最後一層是事件發生後的快速反應體系。另外，結合情資分析，辨識企業受到哪些威脅，例如資料外洩販售、假網站蒐集帳密等，即時處置與下架。

中國醫藥大學附設醫院資訊室副主任許凱平表示，為應對大量的釣魚郵件，院內持續透過社交工程等演練，重要單位亦須設立高標準，讓員工面對各種攻擊時能降低誤點擊率。為避免營運中斷影響病患安全，以單機備援方案確保維持基本醫療作業。至於 ERP 系統與數位訊息被攻擊也有對策，將 ERP 系統與外網隔離。

## 迎戰量子威脅 從十大基本功啟動 PQC 轉型

面對量子計算等新興技術的威脅（4%），前資安院院長何全德最後引述《駕馭複合危機：2025 年全球網路安全格局與韌性要務戰略報告》，提醒組織須審慎應對「先獲取，後解密」（HNDL）的手法，及早啟動後量子密碼學（PQC）轉型，並且保護 IT／OT 融合環境。中小企業亦可參考台積電「十項最低要求」，先求有再求好，完成基本功，便能在控制預算的前提下降低風險。

# 從技術走向治理，CISO 重新定義資安責任邊界

## 2025-2026 CISO Insight資安調查解析-5

**全球監管與法遵壓力正把資安責任推向董事會，迫使 CISO 從技術專家轉為治理與策略角色。面對 AI 風險與治理負擔，如何重塑人力、整合防線，將成為 2026 年企業韌性關鍵。本次解析聚焦資安領導者如何在變局中重構策略，掌握主動權。**

文／明雲青

面對地緣政治升溫、AI 武器化與供應鏈風險交織，傳統「完全預防」邏輯已不敷使用。前資安院院長何全德引述多個報告指出，資安已是企業主責任，與財務、法務並列為策略核心。追求百分之百預防並不現實，新目標是打造營運韌性，使企業在攻擊前後皆能維持營運。法遵與金融壓力正推動此思維轉向，資安也被納入 ESG 架構，成為治理要項。

### 角色上移與責任滲透，以組織重塑應對人力缺口

調查顯示，資安長（CISO）由資訊長（CIO）兼任比例達 38%，專任僅 28%；但在高度監管的金融業，專任比例已升至 45%（見圖 1）。某金融業資安長指出，CIO 著重效率與成本，而 CISO 聚焦資產保護，兩者關注焦點截然不同，這也反映組織對資安戰略地位的定義差異。

在人力結構方面，漢翔航空工業資訊處處長方一定指出，資安韌性面臨的最大挑戰為人才短缺，缺口集中於威脅偵測、SOC 分析與事件調查（18%）（見圖 2）。

圖 1 依產業別來看資安長的專任及兼任

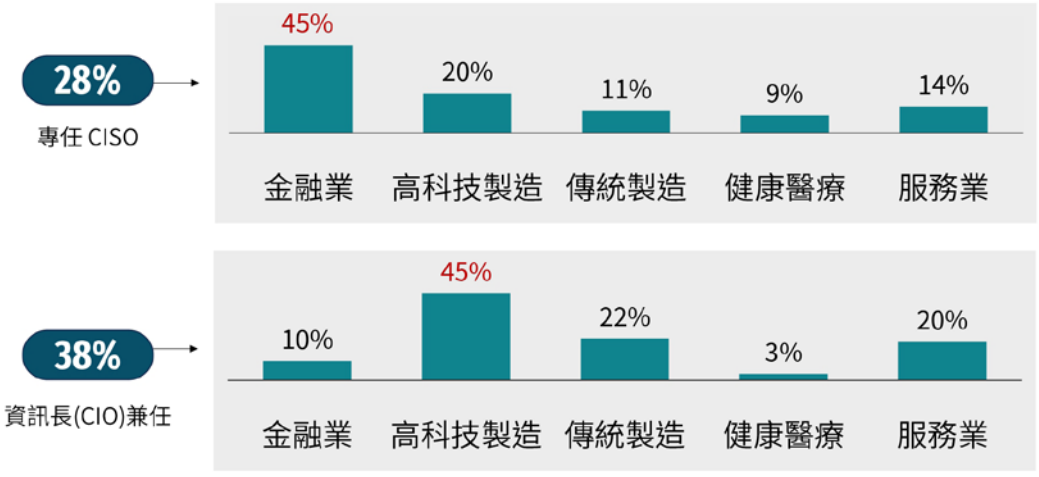
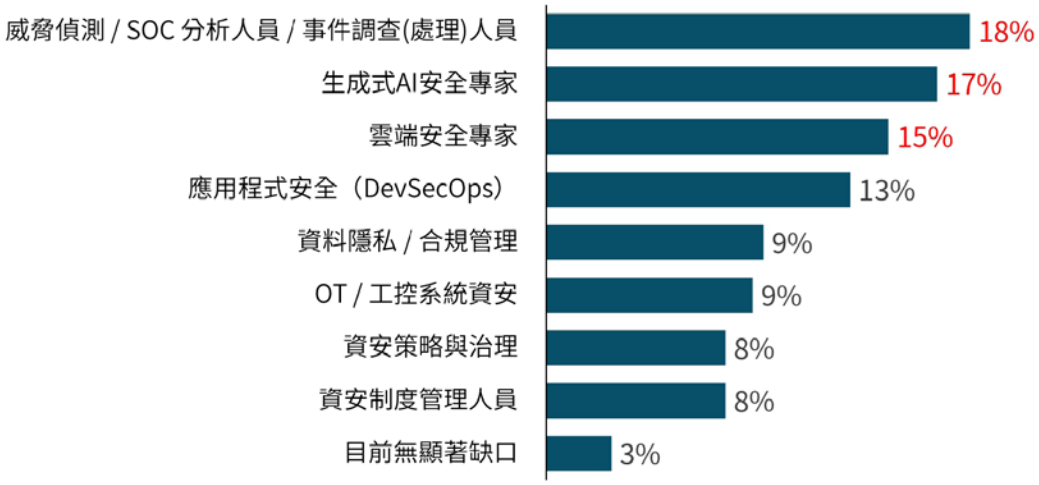


圖 2 企業資安人才類別缺口




遠傳電信資安長朱建國認為，隨著數位化深化，單靠擴編專職人力已難應付挑戰，資安責任必須擴大，推動成為全民運動，並致力將資安要求滲透至技術與業務部門，內嵌於日常流程，使非資安專業人員也能承擔把關責任。

某面板廠資安長表示，透過將資安納入供應商評核機制，可提升整體生態系防護能力。

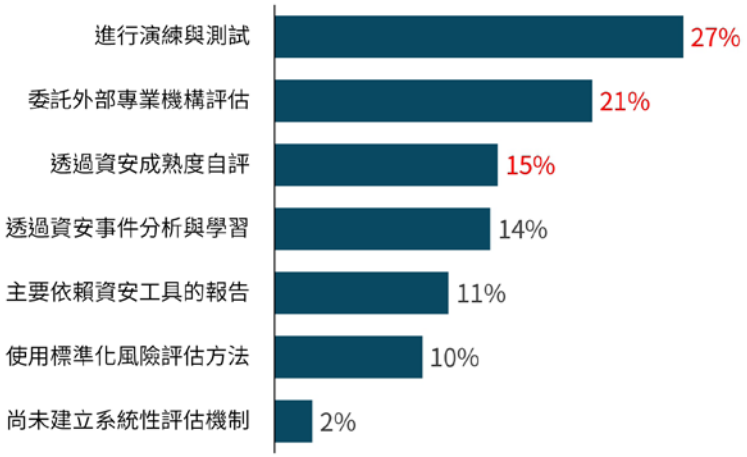
臺北榮民總醫院資訊室主任郭振宗提到，將合作院所比照供應商進行資安審查，亦屬責任滲透模式之一。

調查亦顯示，組織在風險管理上的日常運作，以演練測試（27%）、委外評估（21%）與成熟度自評（15%）為主要常態性資安風險評估方式，已逐步將資安從專案式投入轉向例行化治理。（圖 3）。

## 零信任與可視性前移，以架構升級償還資安債

合勤投資控股資安長游政卿指出，OT 與 IT 整合挑戰，實則源自數位轉型累積的「資安債」，需加速償還。他將治理任務歸納為三點：提升可視性（17%）、整頓基礎架構（12%）、應對新興科技風險（15%）（見圖 4）。

圖 3 您如何進行常態性的整體資安風險評估？



朱建國補充，資安治理的核心主軸在於「風險—可視性—監控告警」的連動，須先釐清新興科技對營運的風險，再設計對應的可視性與防護機制。

在技術藍圖上，零信任架構已成為鞏固資安韌性的主軸，其精神在於「永不信任、始終驗證」。方一定指出，導入零信任時面臨兩大挑戰：一是整合既有系統的困難，二是改變工作流程與習慣的阻力。因此，漢翔採取漸進式推動策略，依循「明確驗證、最小授權、預設已遭入侵」三大原則建立機制。

游政卿補充，合勤採「包裹而非替換」策略，透過在舊系統前端加裝零信任閘道，在不影響穩定性的前提下實現控管。

觀察 2025 年整體趨勢，CISO 推動的資安重點普遍左移。游政卿表示，圖 5 呈現出明確趨勢，企業同時在前端防禦與後端偵測上加碼投資，但若兩端沒有被制度化串聯，資源再多也只是各自為政。他建議企業應善用 ISO 27001 的 PDCA 循環，將後端偵測結果回饋至前端防護策略，實現防禦閉環。

圖 4 另有正在推動或整頓的特別重點項目

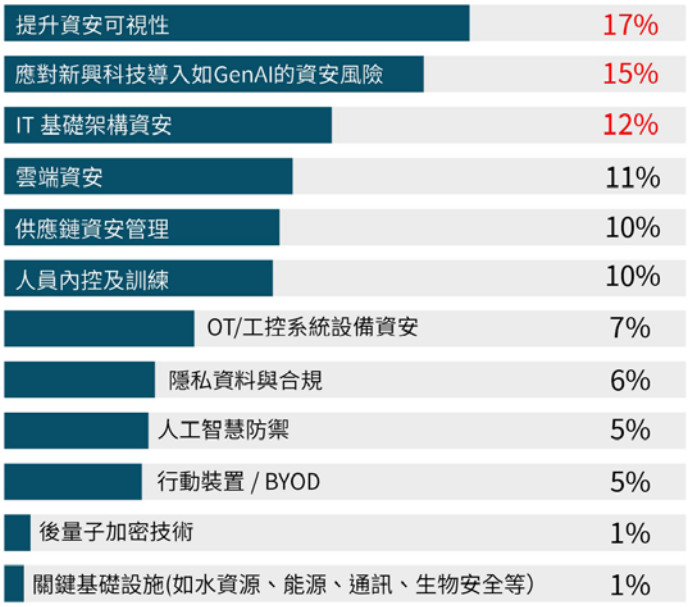



圖 5 2025 年最關注推動的資安治理重點？

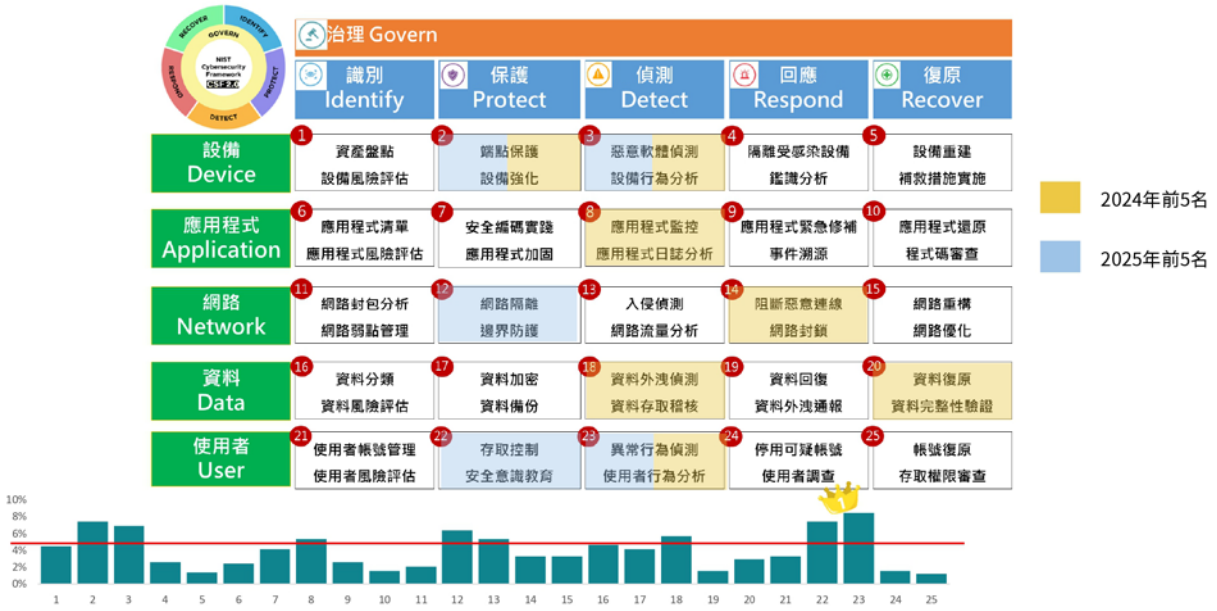


圖 6 影響資安長成功與否的關鍵因素

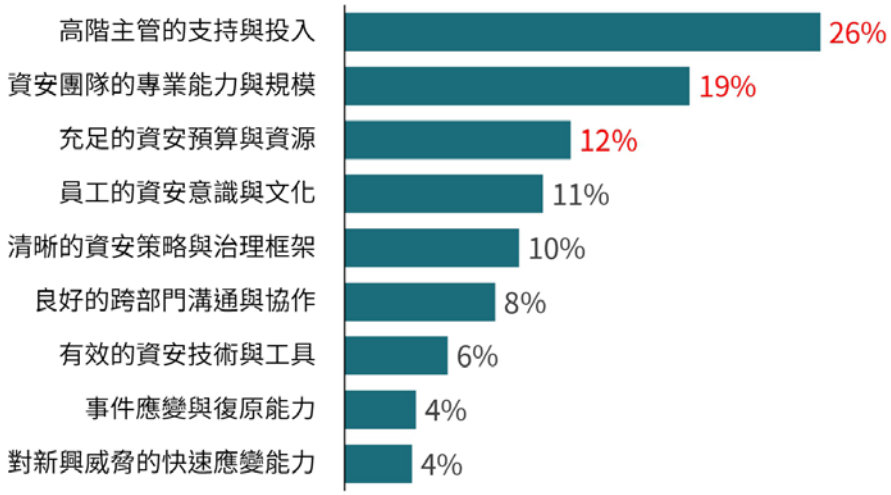
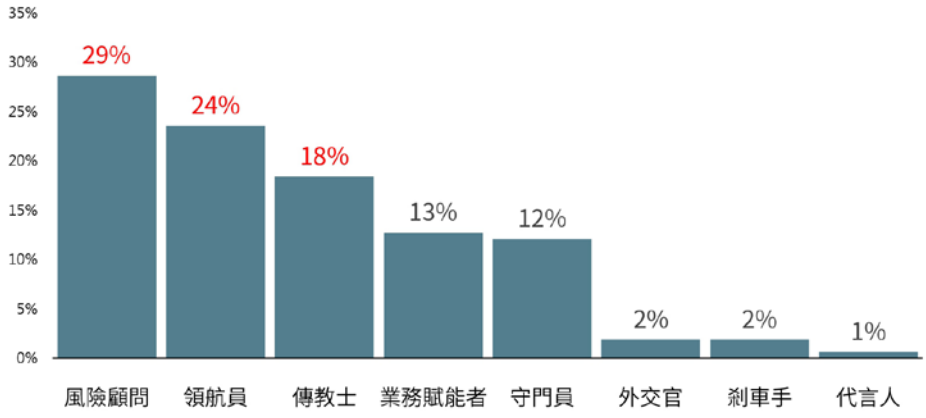



圖 7 您會如何形容資安長的工作？




## 從法遵到風險經理人，以商業視角驅動資安策略布局

隨著全球監管趨勢轉變，資安責任已上升至公司最高層。何全德指出，監管機構的焦點已從「為何被駭」轉向「被駭後如何處理」。他強調，美國 SEC 新規要求上市公司在重大事件發生後，必須於 4 天內揭露；歐盟 NIS2 指令更將資安責任「個人化」，管理層可能面臨法律訴訟。

某金融業資安長補充，金融監管法規通常只是最低門檻，沒有妥協空間；但執行強度應依風險程度調整，尤其在高風險場景下，防護力必須超越法規底線。

游政卿強調，CISO 必須是翻譯官兼風險經理人，能將法規要求轉化為商業語言，例如說明違反 GDPR 可能失去歐洲市場，此時法遵投資不再是成本，而是風險控管手段。

某面板廠資安長則透過將 ESG 評價與供應商 QBR 分數連結，藉由業務機制驅動供應商提升資安。

朱建國指出，在導入後量子加密（PQC）等前沿技術時，應依循 3GPP 等國際標準，初期僅進行少量概念驗證，以避免因認證與環境尚未成熟而產生風險。

而在角色定位上，CISO 最常自喻為風險顧問（29%）與領航員（24%），並一致認為成功關鍵在於高階主管的支持與投入（26%）（見圖 6、7）。

何全德提醒，領導者應在董事會聚焦三大議題：誰應負最終網路風險責任、如何在 4 天揭露期限內做出決策，以及企業是否曾演練過最極端的營運中斷情境。

隨著資安責任上移治理核心，CISO 正同步調整角色定位與技術策略，從風險顧問到組織領航員，從防線整合到治理滲透。下一階段挑戰，將落在如何在有限資源下優先排序、強化跨部門協作，並以預算配置回應風險現實與治理期待。