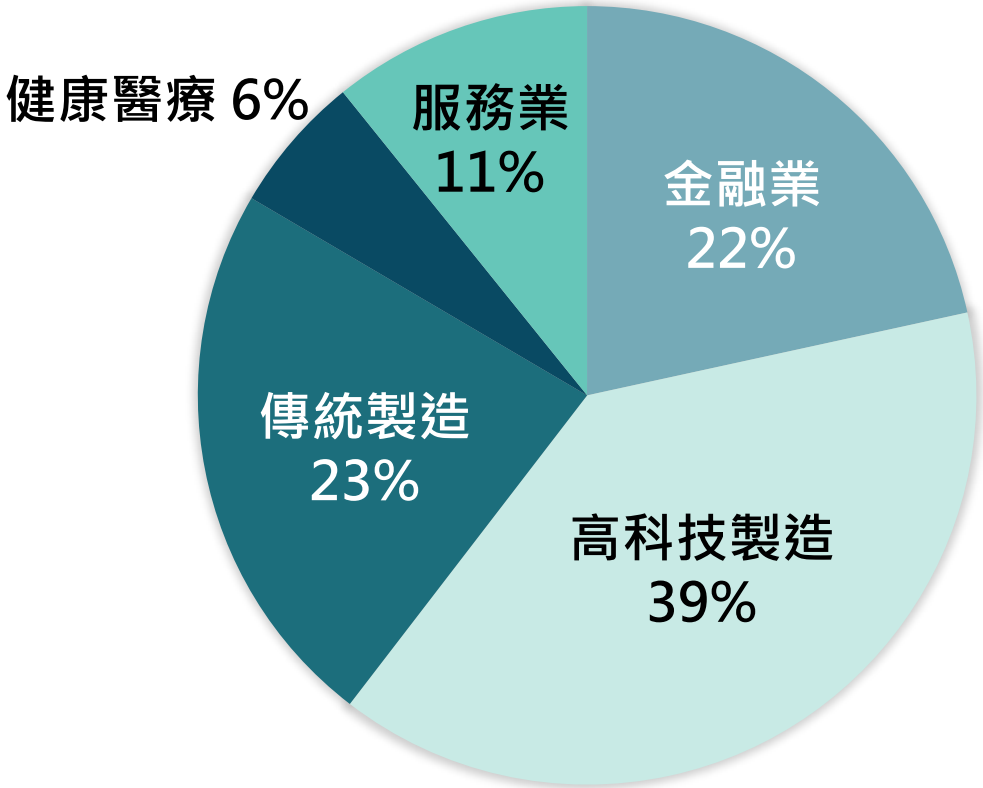


CIO Taiwan　CISO 資安學院

背景資料 關於CISO Insight 資安問卷調查

- 調查期間：115年8月25日～9月16日
- 調查對象：上市櫃及台灣2000大企業資安最高主管
- 有效份數：159
- 產業比例：如右圖



目錄



1 企業基本資料與組織

2 資安防禦與韌性

3 AI治理與AI資安

4 供應鏈安全與第三方風險管理

5 資安預算與採購

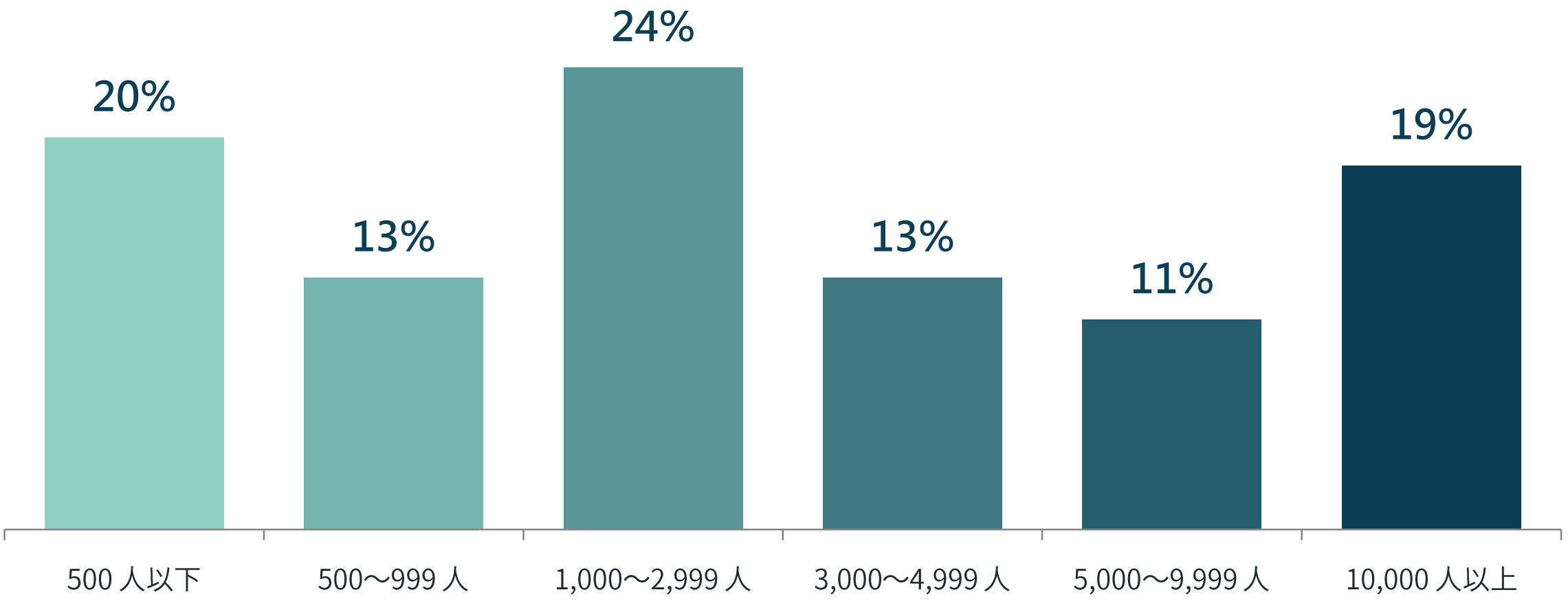
6 資安治理與資安長角色



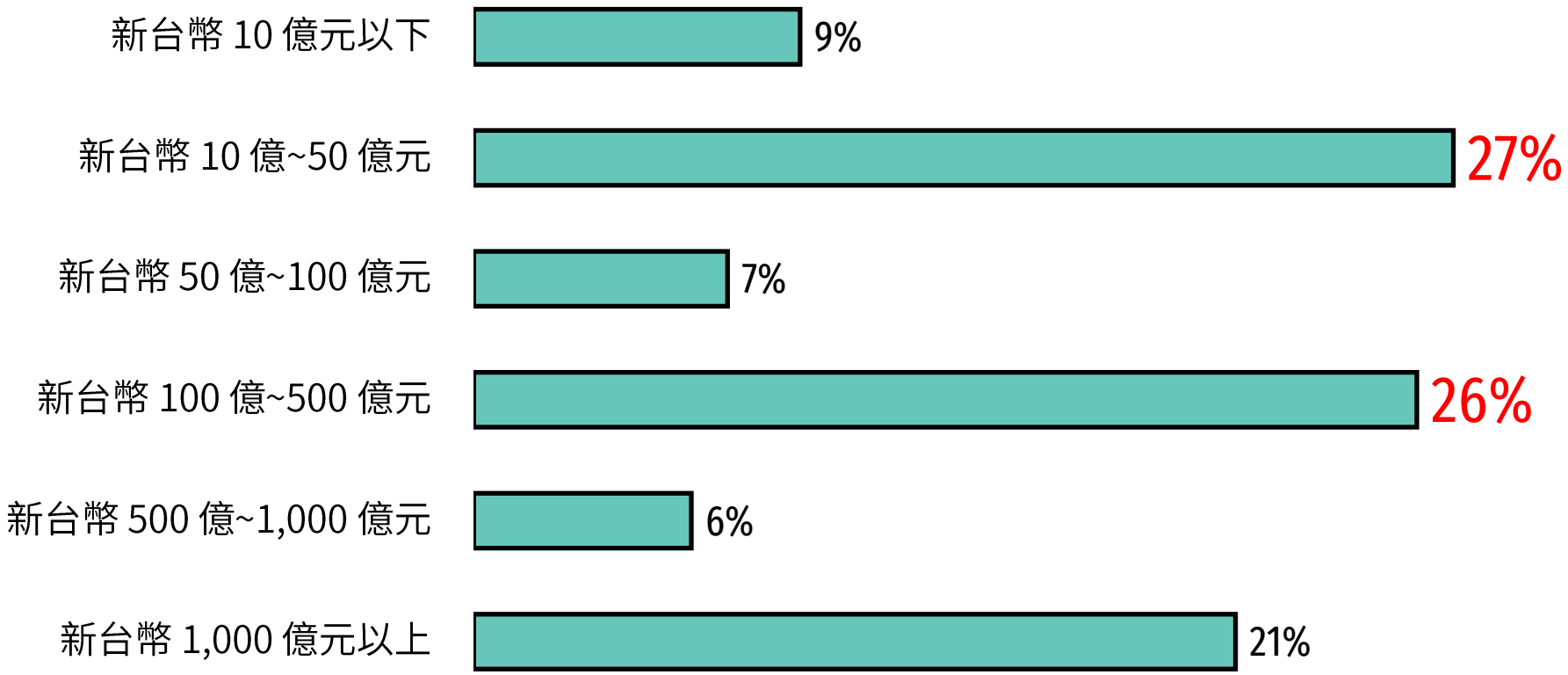
一、企業基本資料與組織

CIO Taiwan CISO 資安學院

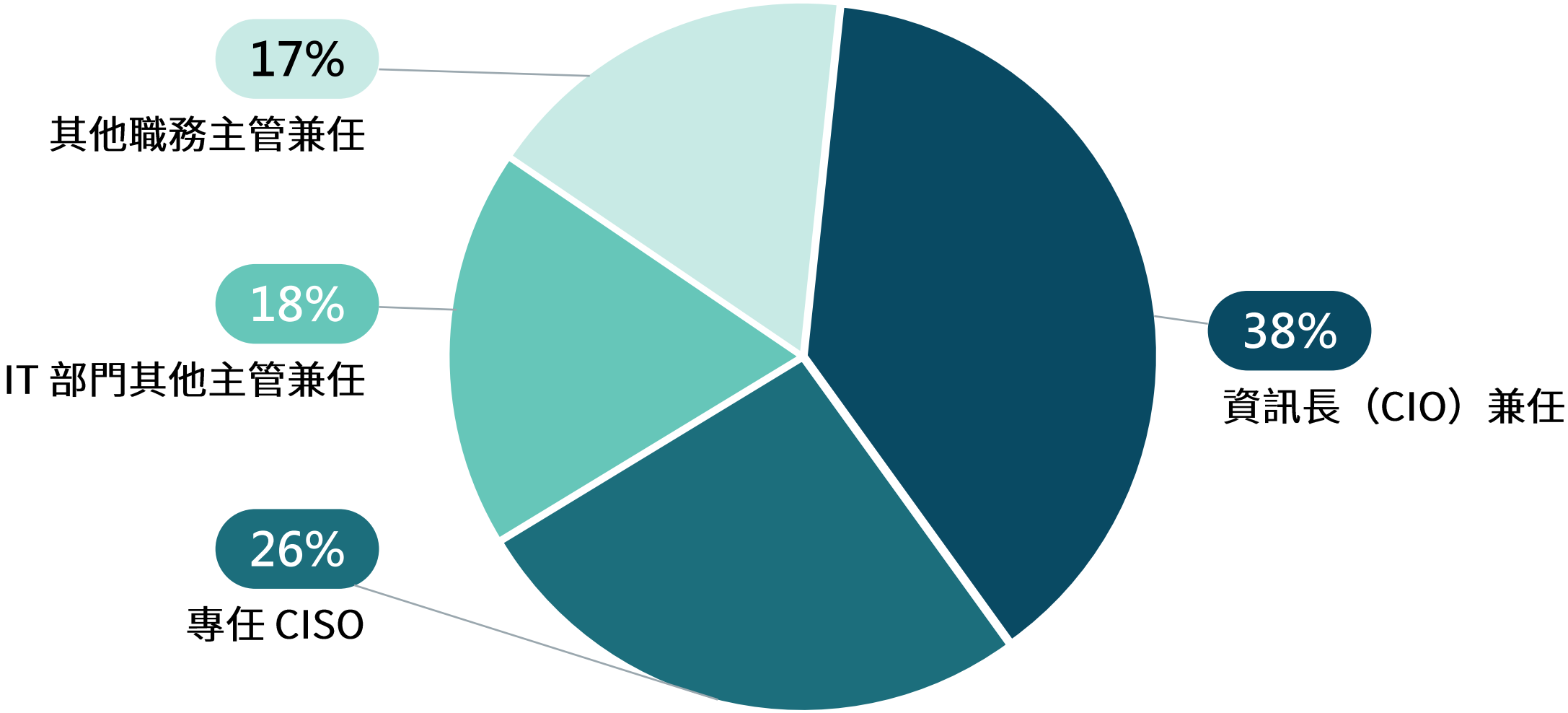
公司全球員工總人數（含海外分支機構與廠區）



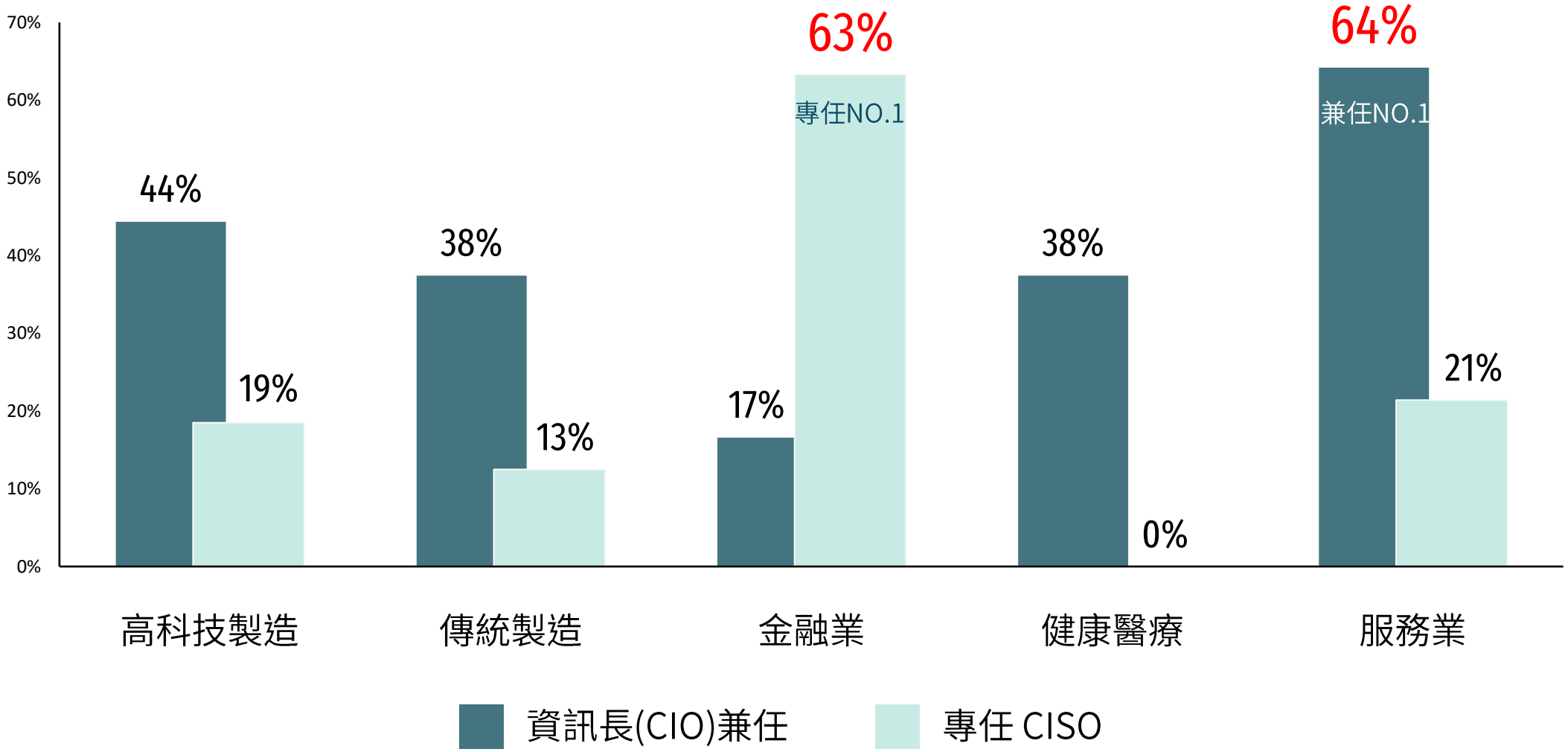
公司去年度全球合併營收



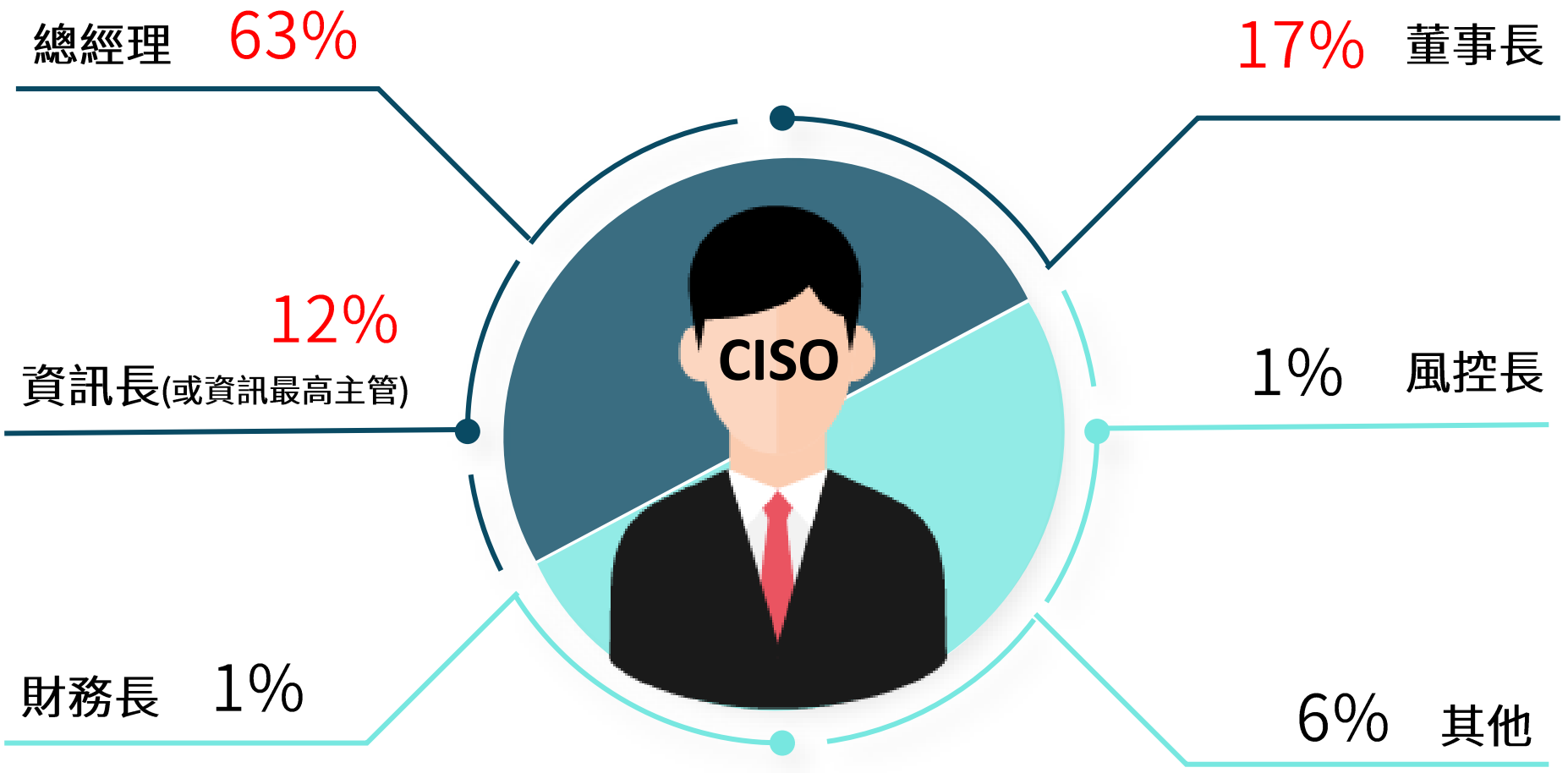
公司資安最高主管(資安長 / CISO)專/兼任比例



公司資安最高主管(資安長 / CISO)專/兼任比例



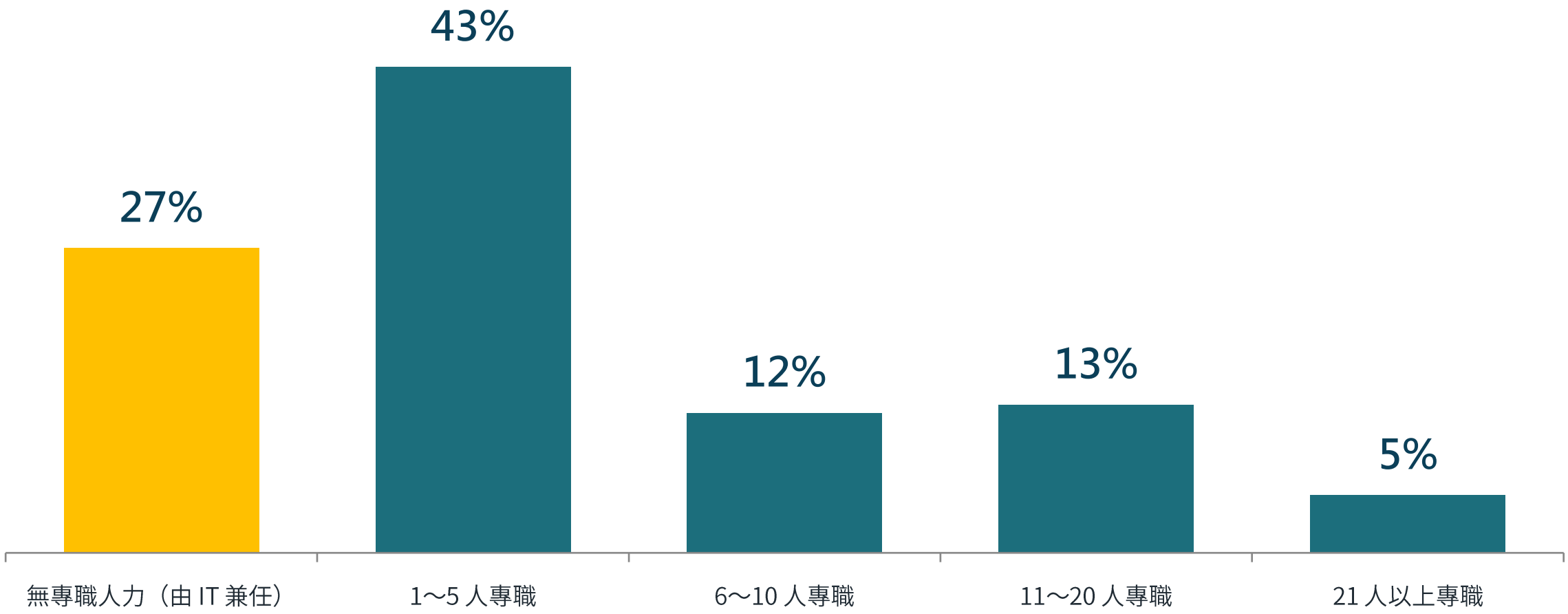
資安長（或資訊資安長）向誰報告?



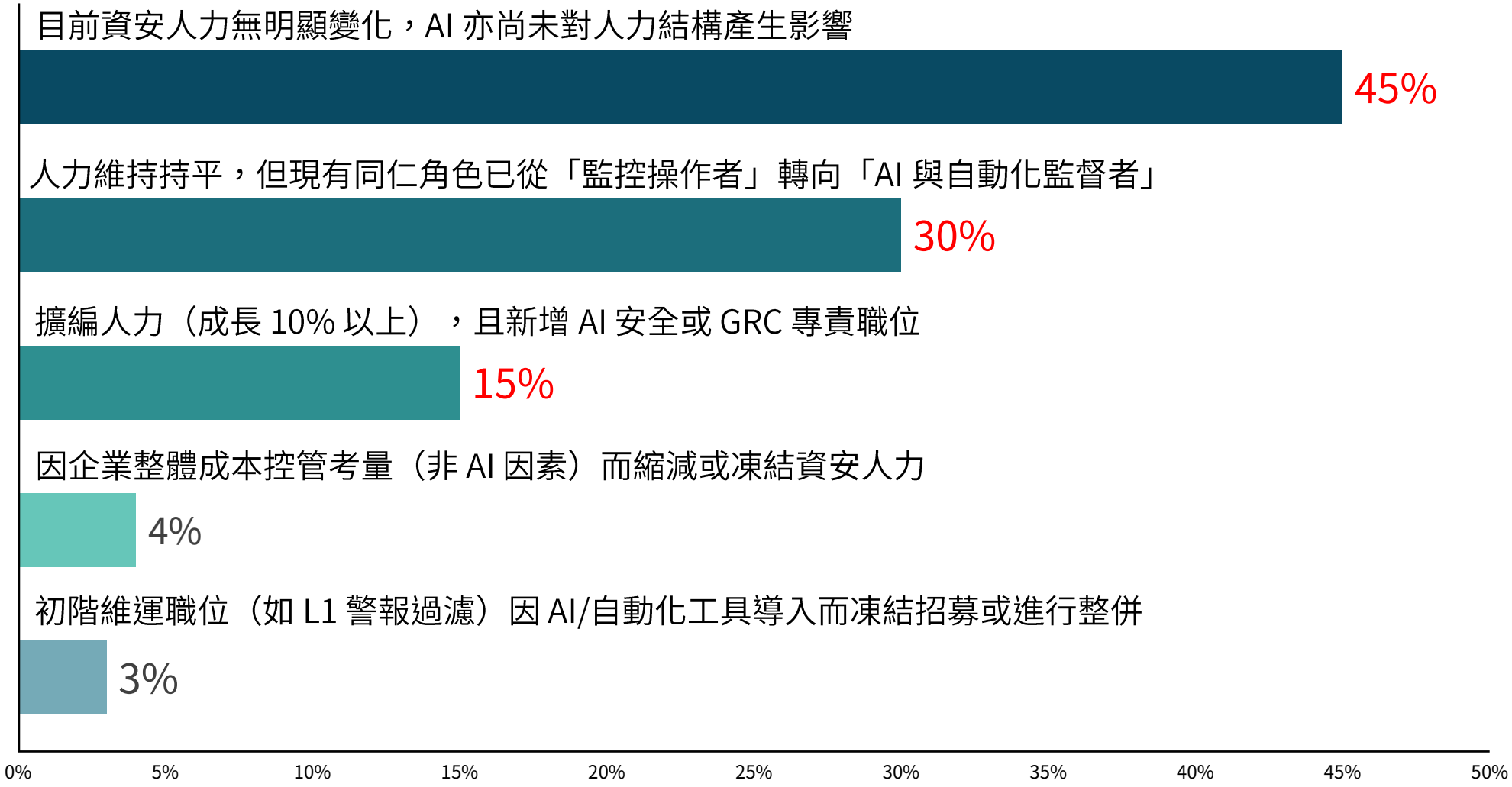
「資安專責部門」的獨立營運狀況



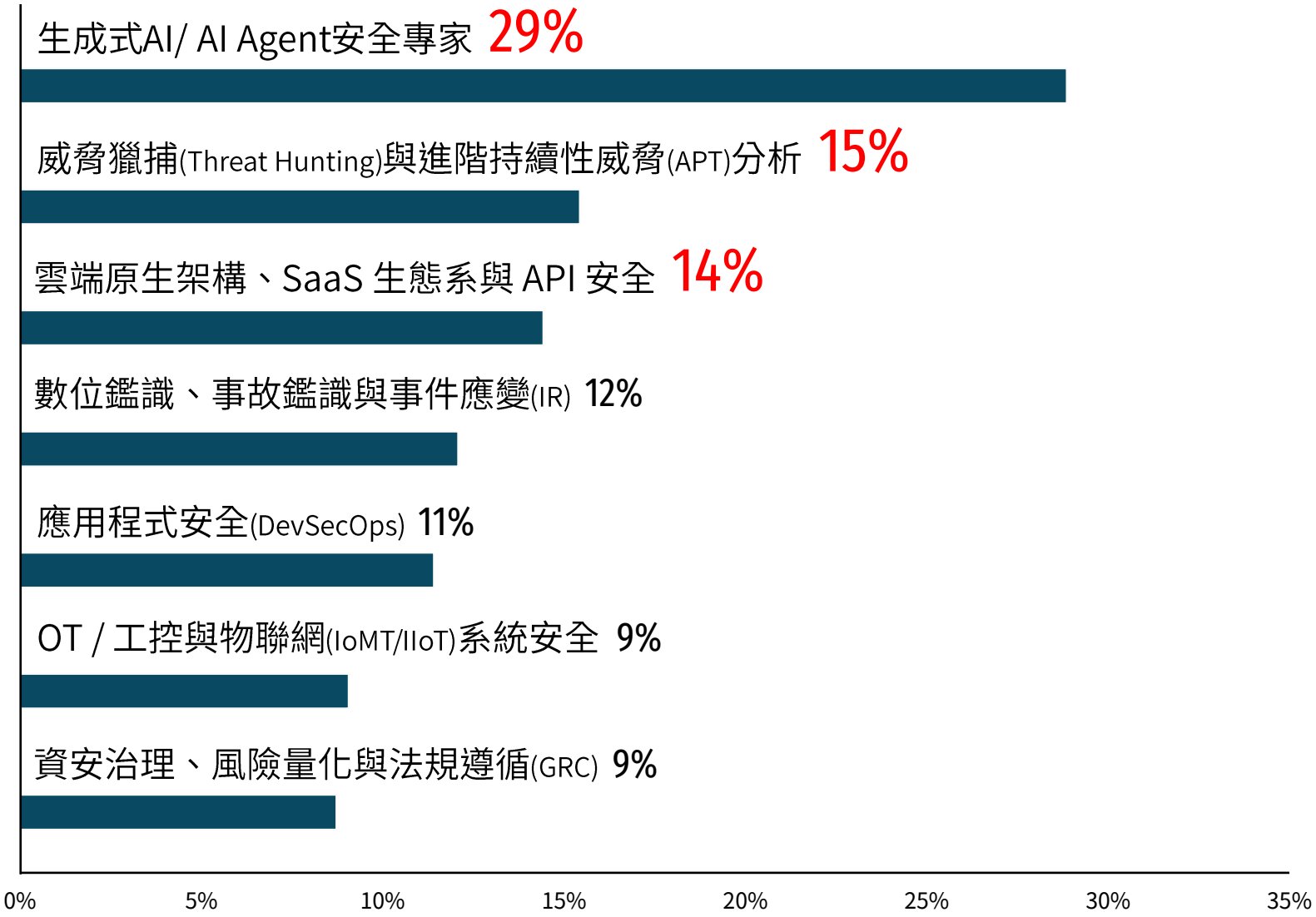
專責資安團隊的人數



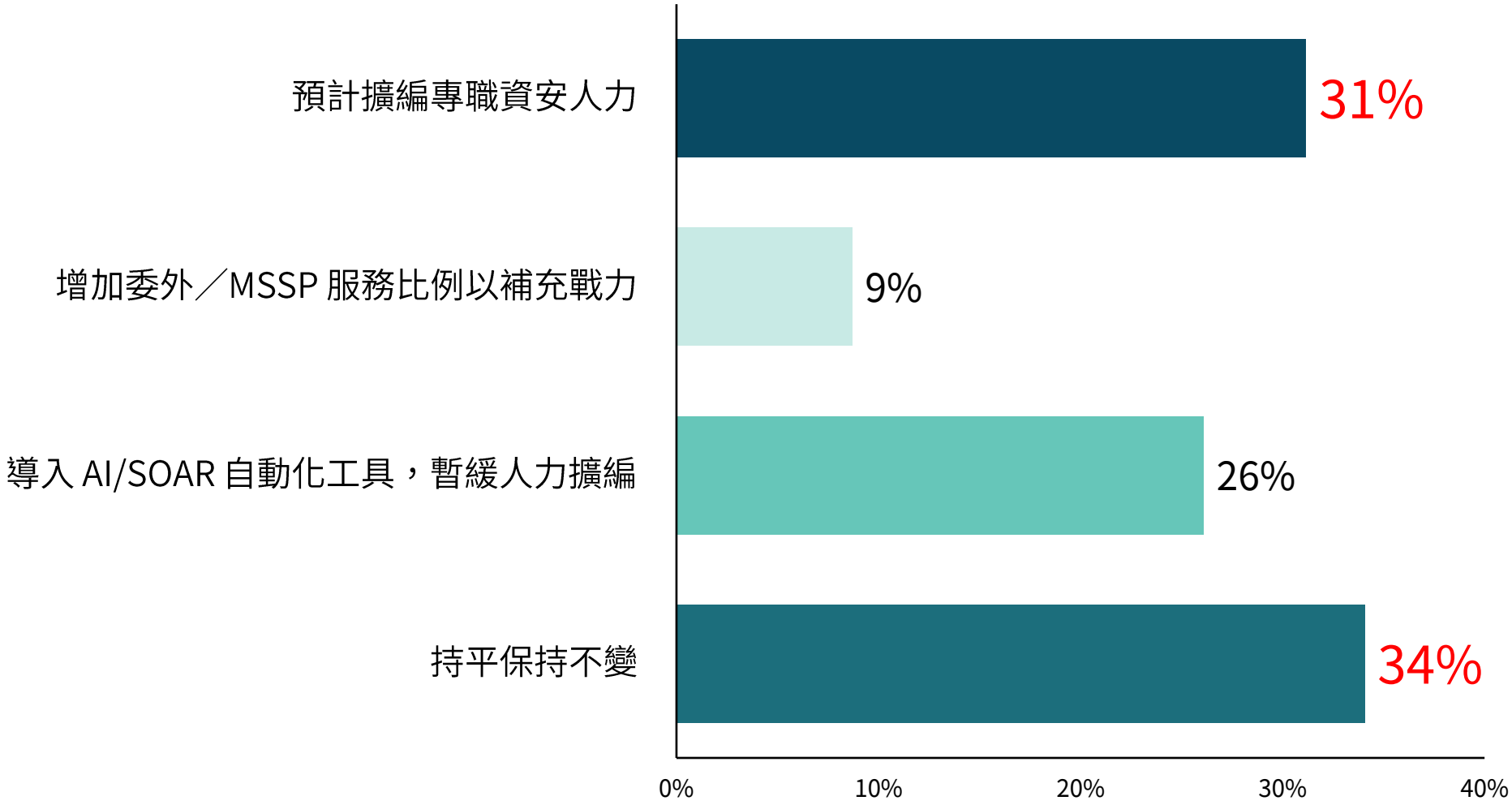
資安人力配置變化及 AI/自動化導入對人力的實質影響



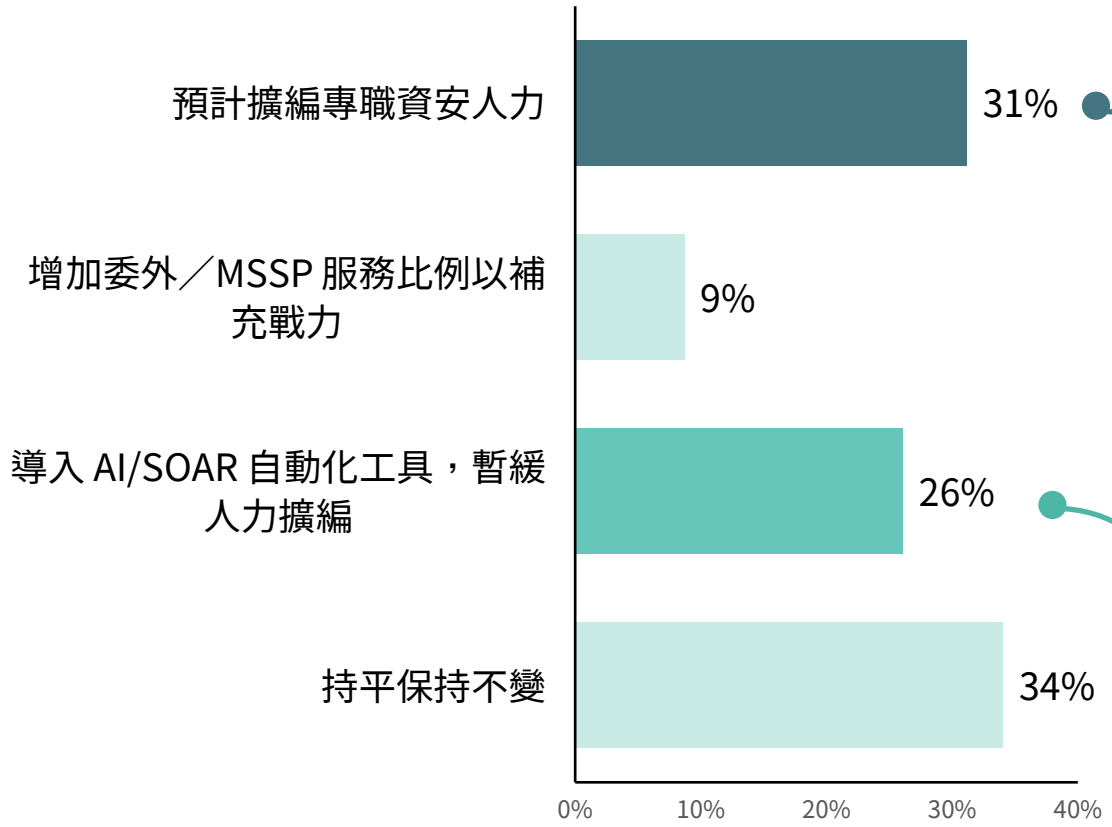
資安團隊目前最欠缺之核心技能

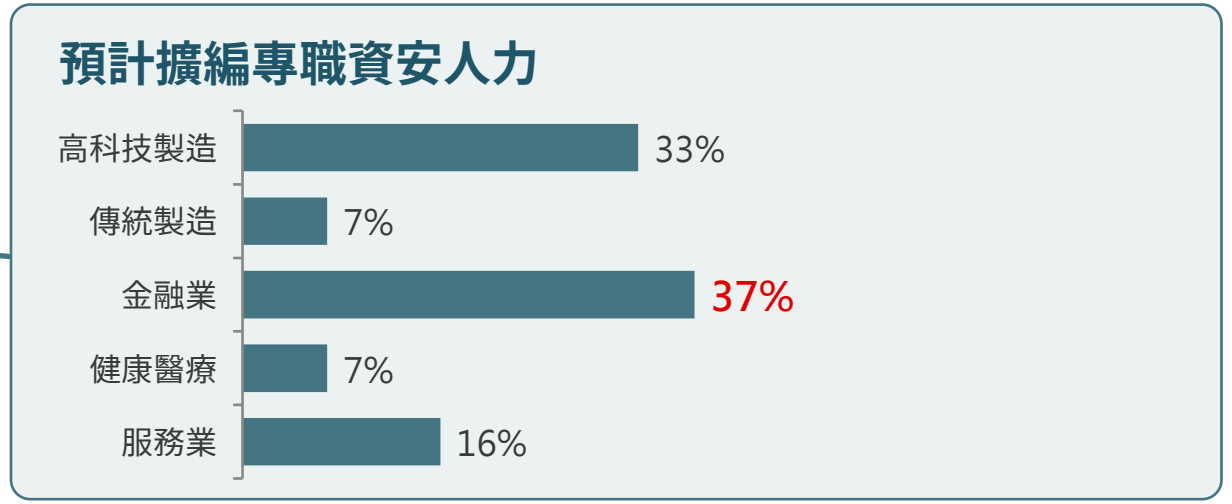


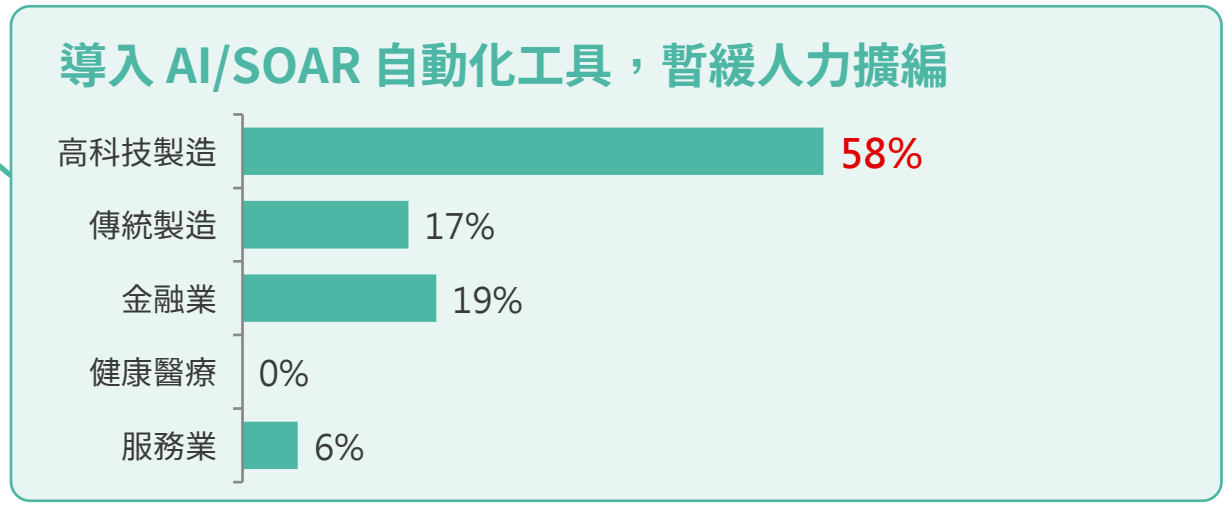
未來一年在資安人力規劃重點



未來一年的資安人力規劃重點









二、資安防禦與韌性

CIO Taiwan CISO 資安學院

過去 12 個月內，貴公司是否曾遭遇下列資安事件?

1

60%

並未發生選項
所列事件

2

13%

社交工程釣魚郵件得
逞(含 Deepfake 語音/
視訊詐騙)

3

8%

內部人員蓄意(員工/
離職員工)或
非蓄意資料外洩

4

5%

勒索軟體攻擊

5

5%

針對OT/工控/物聯網
系統之網路攻擊

6

4%

供應鏈、第三方外包
商或 SaaS 漏洞導致
之跨網入侵

7

2%

未授權將企業機密
個資上傳至外部AI工具
或AI Agent異常行為

8

1%

OAuth權杖(Token)劫
持、API金鑰或非人類
身分(NHI)遭竊濫用

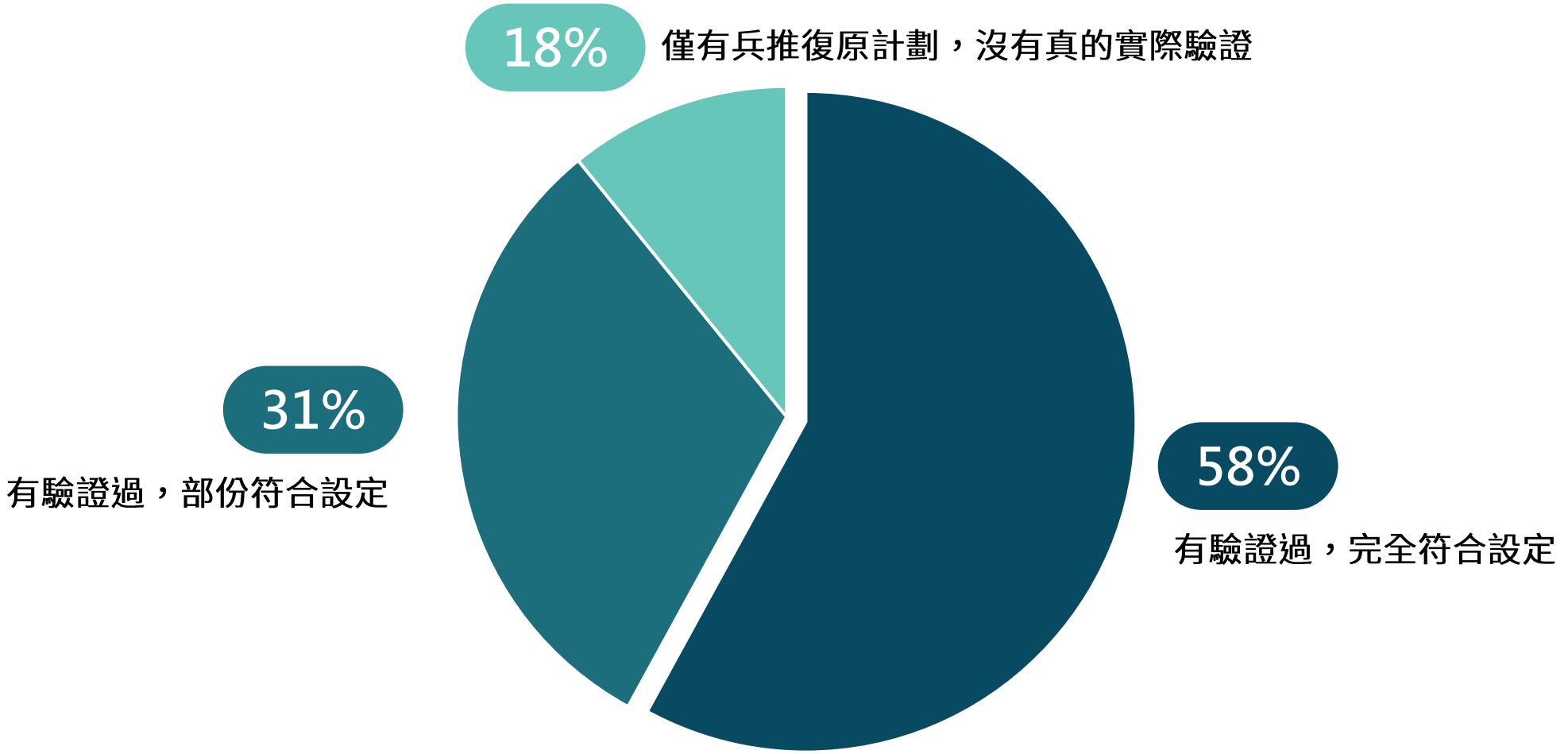
從偵測到事件發生至完成初步圍堵的平均時間（MTTR），是否有能力因應「分鐘級甚至秒級」的 AI 驅動攻擊?

- **圍堵時間 1～8 小時**：部分系統具自動化防護，但關鍵決策仍需人工介入，速度存在落差 — 56%
- **圍堵時間 8～24 小時**：高度仰賴人工介入與外包廠商響應，難以應對 AI 速度 — 24%
- **圍堵時間於 1 小時內**：已具備 SOAR 自動化即時圍堵能力，有信心因應秒級攻擊 — 12%
- **圍堵時間超過 1 天或無法有效量測**：缺乏即時可視性，目前無能力因應極速攻擊 — 8%

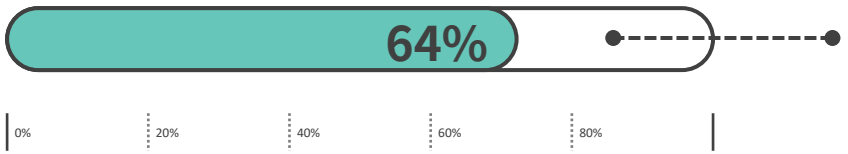
展望 2026 下半年至 2027 年，最擔憂之資安威脅類型?

1. 雙重勒索軟體與機密資料外洩勒索
2. AI 驅動之高度個人化社交工程與 Deepfake 詐騙
3. 內部人員威脅與影子 AI/IT 資料外洩
4. AI 代理(AI Agent)遭挾持、越權或惡意濫用(Agent Hijacking)
5. 雲端 / 多雲環境組態失誤與特權帳號外洩

過去一年是否真的驗證過關鍵系統復原，而且符合原來設定的 RTO/RPO?



當前勒索軟體多採「加密系統＋外洩機密」雙重勒索。
若不幸中招，高層對「堅持不支付贖金」的決心與應變方針?



決心堅定

已建立「零贖金」政策，技術上確信備份能在無失真狀態下快速復原



態度動搖

雖有備份，但若涉及核心商業機密或客戶資料公開，高層仍可能考慮談判支付



信心不足

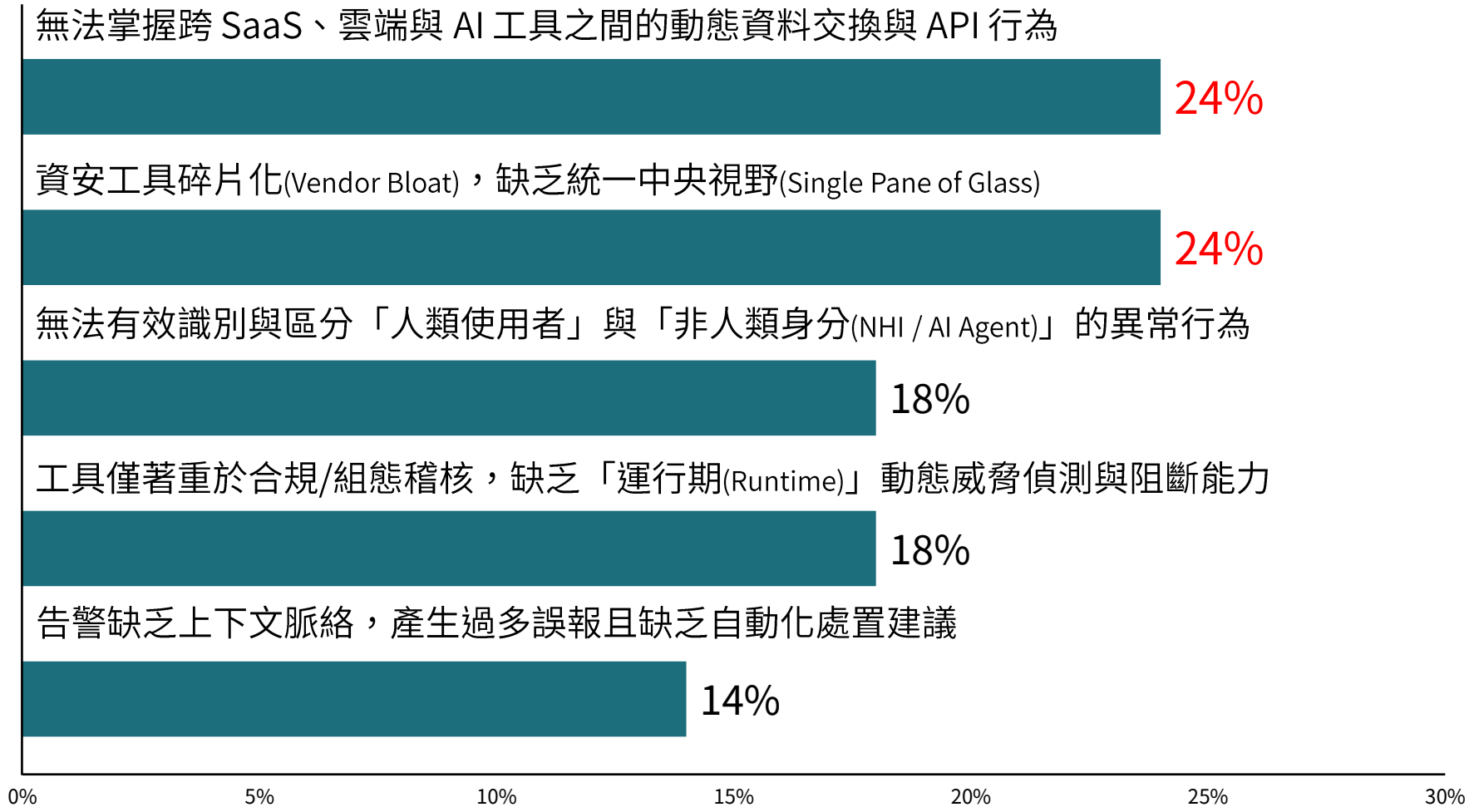
復原時效難掌握，面臨龐大營運中斷壓力，實務上可能被迫談判



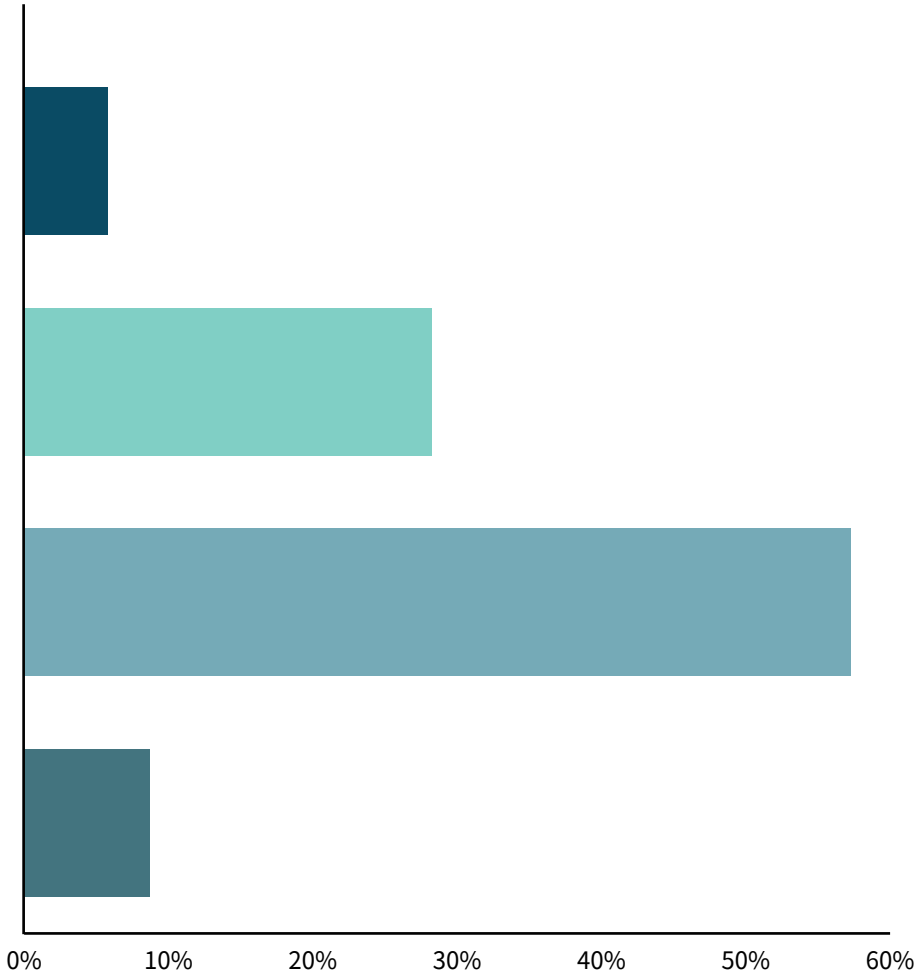
無明確方針

內部尚未建立針對勒索贖金談判與應變的決策共識

在對抗新興威脅時的技術瓶頸



對後量子密碼學(PQC)與密碼敏捷性(Crypto-Agility)的準備



6% 已完成加密資產盤點(Cryptographic Inventory)，並開始規劃/執行 PQC 遷移路徑圖

28% 已意識到時程提前，目前正評估具備「密碼敏捷性」之系統架構或要求供應商提供 PQC 條款

57% 知道此議題，但認為技術與標準尚未成熟，目前處於觀望階段

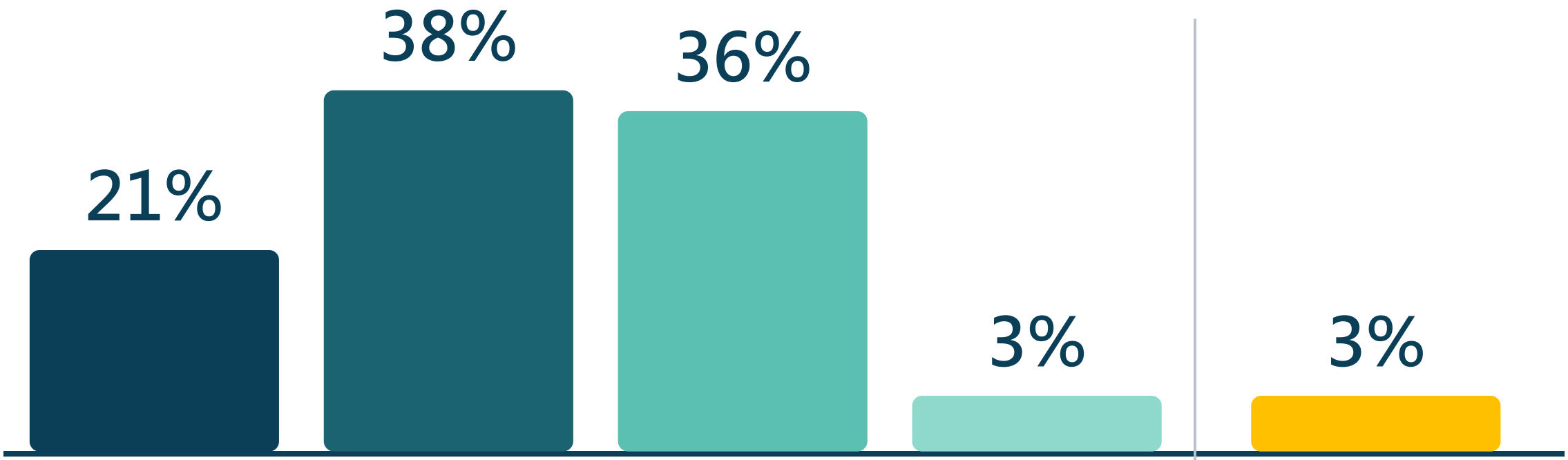
9% 完全不了解此議題，亦無任何準備規劃



三、 AI治理與AI資安

CIO Taiwan CISO 資安學院

目前導入生成式 AI / AI Agent之程度



Shadow AI	政策宣告	特定試行	正式規模化	全面禁止
第 1 級	第 2 級	第 3 級	第 4-5 級	—
員工私下使用，無政策亦無技術管控	已頒布使用規範，缺乏技術攔截與稽核	特定部門試行，具白名單、DLP 與資產盤點	深度整合核心業務，治理與風險量化成熟	公司明文禁止使用外部生成式 AI

AI 對貴公司資安治理之「淨影響」？
資安團隊是否已將 AI 自動化代理應用於資安維運?

雙重衝擊並存

41%

正在評估引進 AI 防禦工具，同時面臨龐大的 AI 安全治理壓力

30%

尚未應用 AI 於資安維運

目前尚未將 AI 技術應用於資安維運

12%

助力大於威脅

已將 AI 用於程式碼弱點掃描、修補建議與高階報告生成

11%

助力大於威脅

已將 AI 用於 SOC 告警降噪、威脅獵捕與 SOAR 自動處置

7%

威脅大於助力

攻擊面擴大（提示詞注入、資料外洩），且防禦工具維運成本過高

因應生成式 AI 與 AI Agent 之導入，貴公司對「既有資安政策體系」做了哪些關鍵調整?

新增專屬《企業 AI 可接受使用政策(AI AUP)》 31%

修訂《資料分類與外洩防護政策》，納入向量資料庫(Vector DB)與 RAG 機構知識庫之保護 9%

修訂《第三方與供應鏈風險管理政策》，要求外包商揭露開發流程中 AI 工具之調用情形 9%

修訂《身分與存取管理(IAM)政策》，納入非人類身分(NHI)與 AI Agent 之權限邊界 8%

擴充《資安事件應變計畫(IR Playbook)》，納入 AI 模型毒化與 Agent 越權處置流程 6%

尚未針對 AI 進行任何資安政策條文之修訂 34%

是否已成立「AI 安全審查機制」或「跨部門 AI 治理委員會」

28% 已成立跨部門治理委員會

含資安、法務、研發、業務、人資，評估 AI 工具與使用邊界

42% 資安／IT 兼管，逐案審查

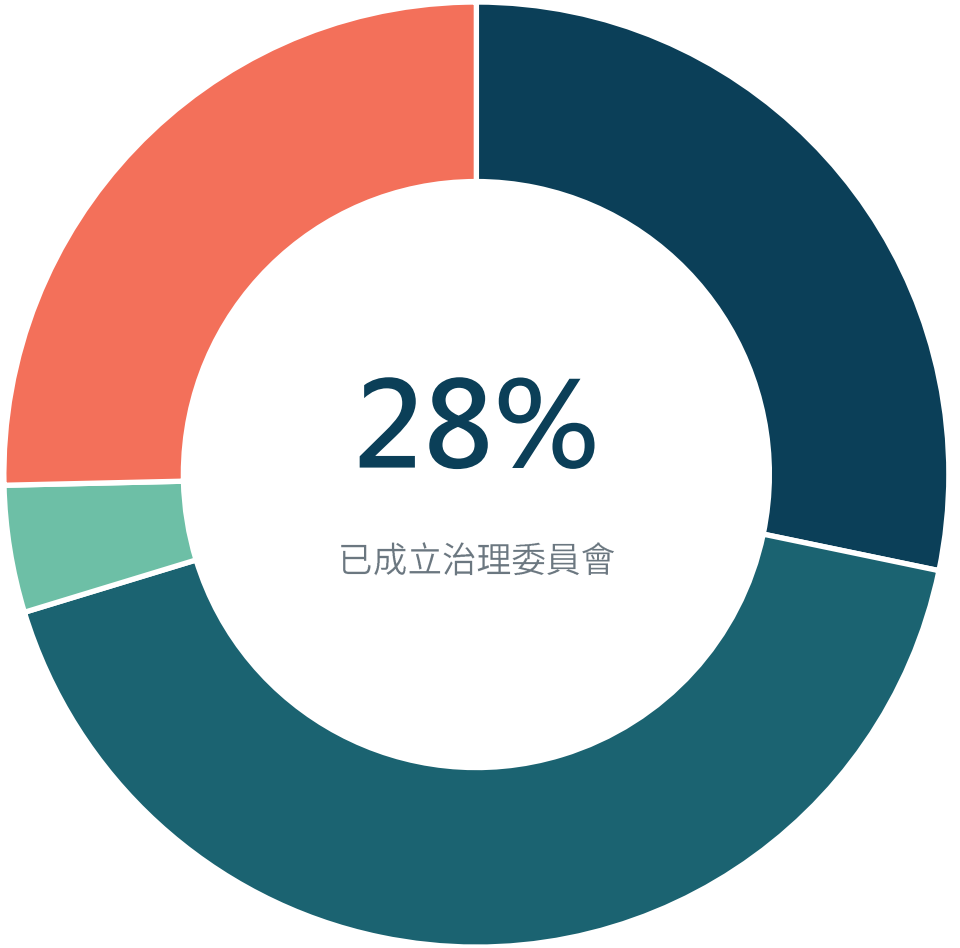
採逐案審查方式進行安全性與合規評估

4% 業務自行評估，資安被動

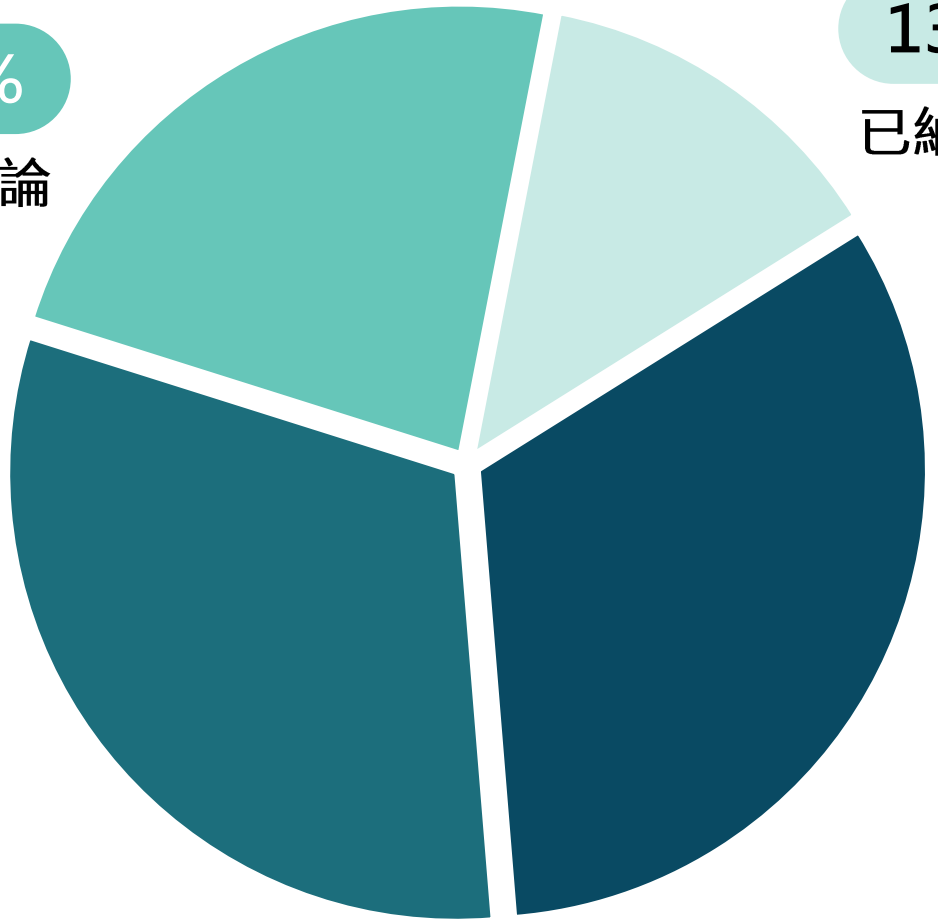
業務單位自行評估引入，資安僅於出事時介入

25% 尚無任何審查機制

內部尚無任何 AI 安全或治理審查機制



董事會或IT管理委員會是否定期檢視 AI 相關風險?



13%
已納入董事會固定議程

23%
僅管理階層討論

31%
尚未正式納入治理機制

33%
不定期報告

評估內部 AI 系統的「國際 AI 安全基準與合規框架」



生成式 AI 與 AI Agent 的資安治理成熟度

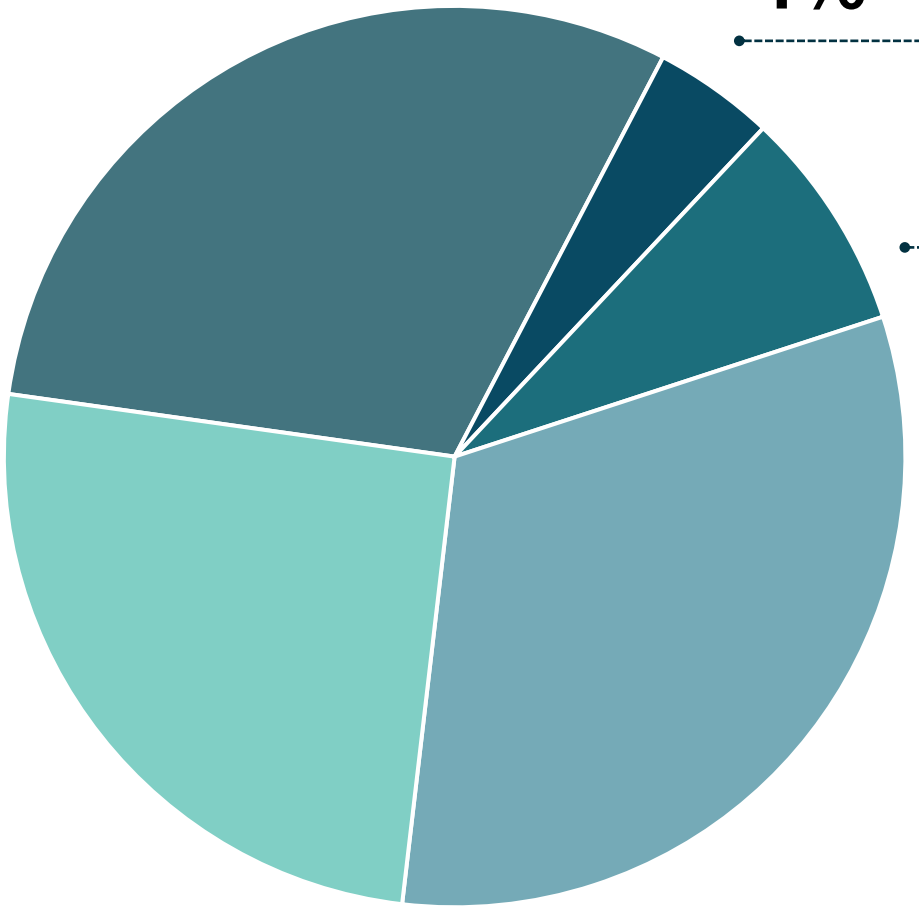
4%
已建立完整 AI / Agent 治理框架，
並整合 ERM、資安、法遵及 董事會監督

8%
已建立跨部門 AI 治理
及持續監控機制

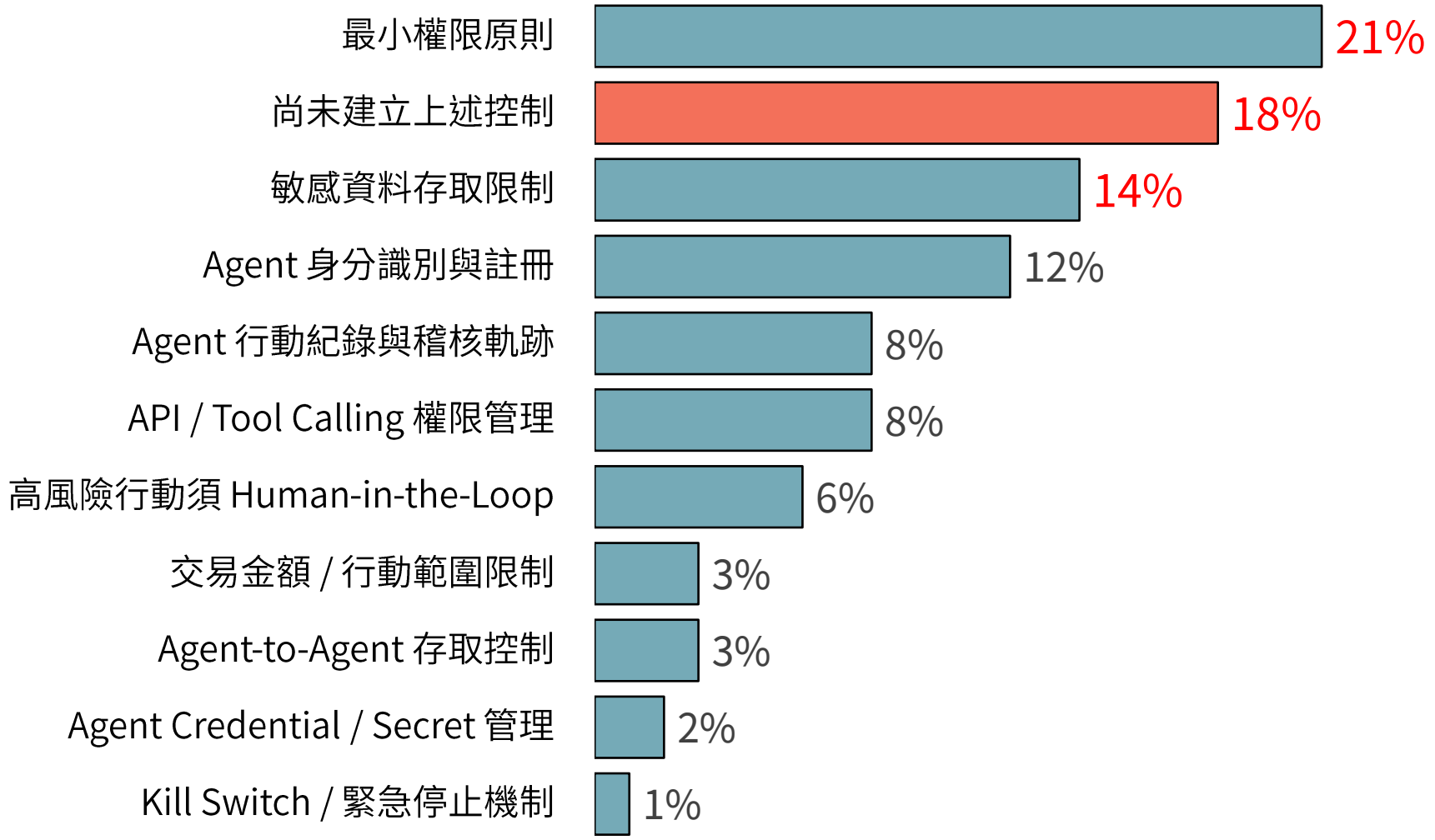
32%
已開始盤點 AI 使用情況及風險

25%
尚未建立相關治理機制

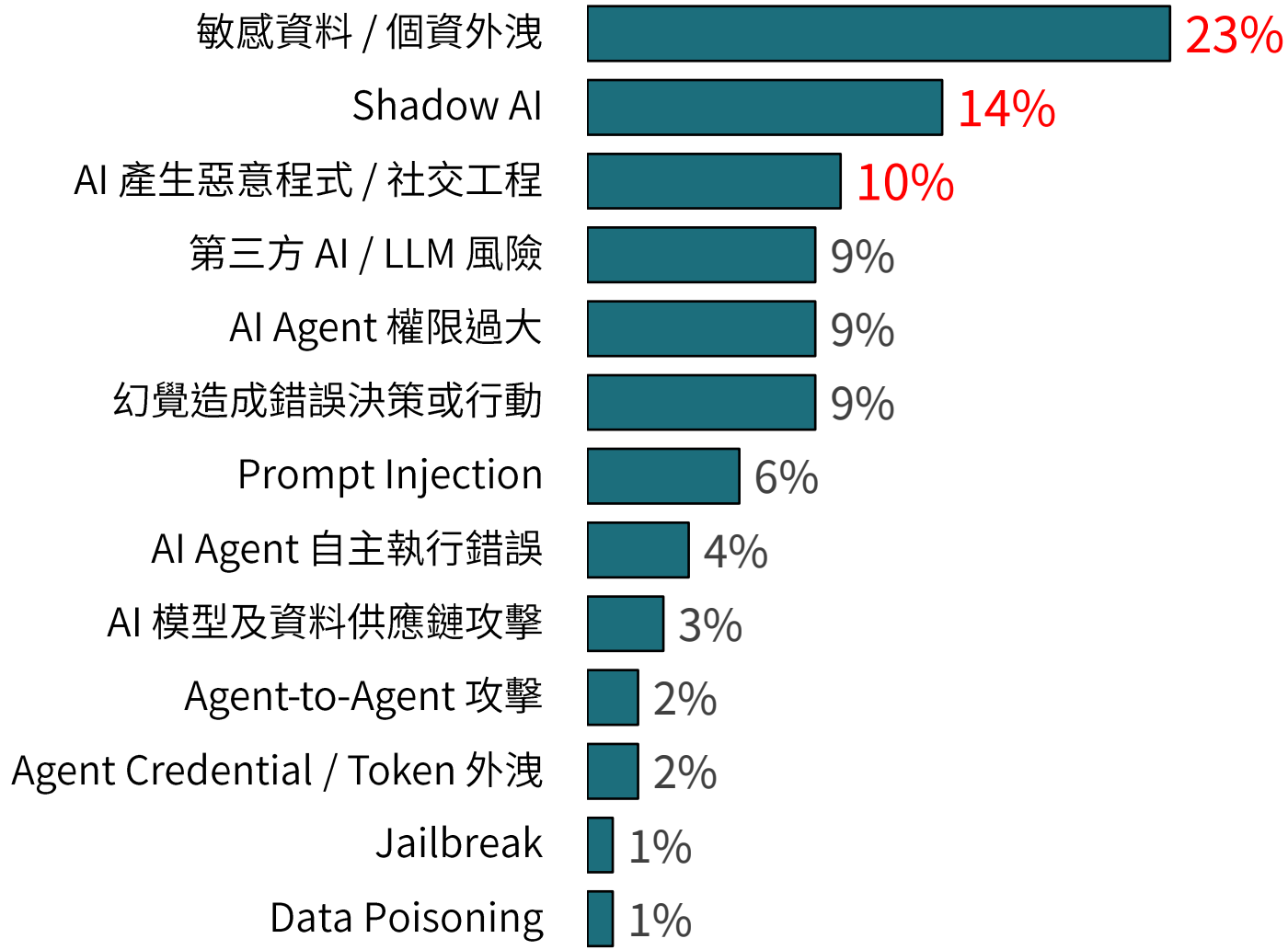
30%
已建立 AI 資安政策、權責與基本控制



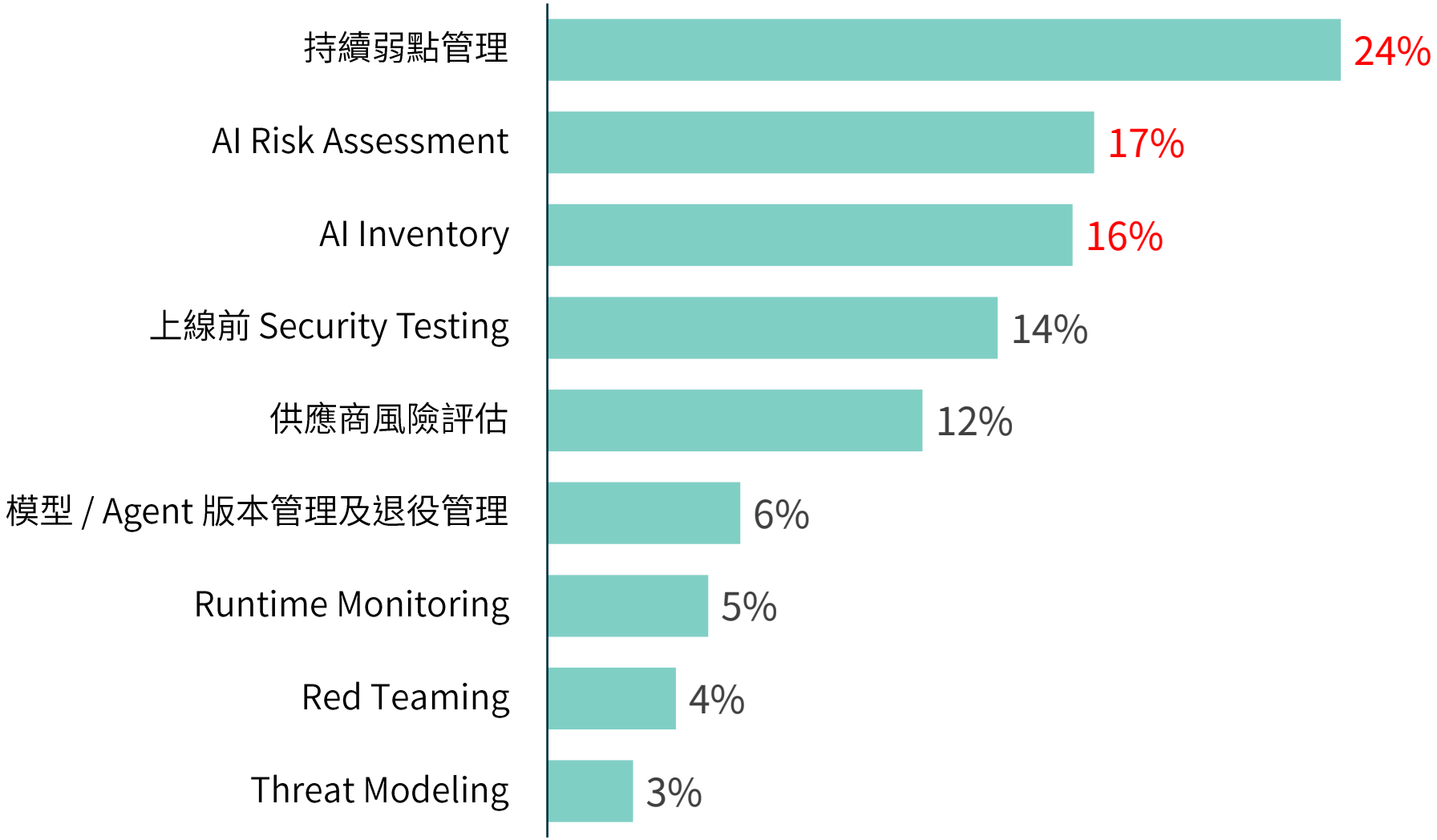
是否已針對 AI Agent 建立下列安全控制?



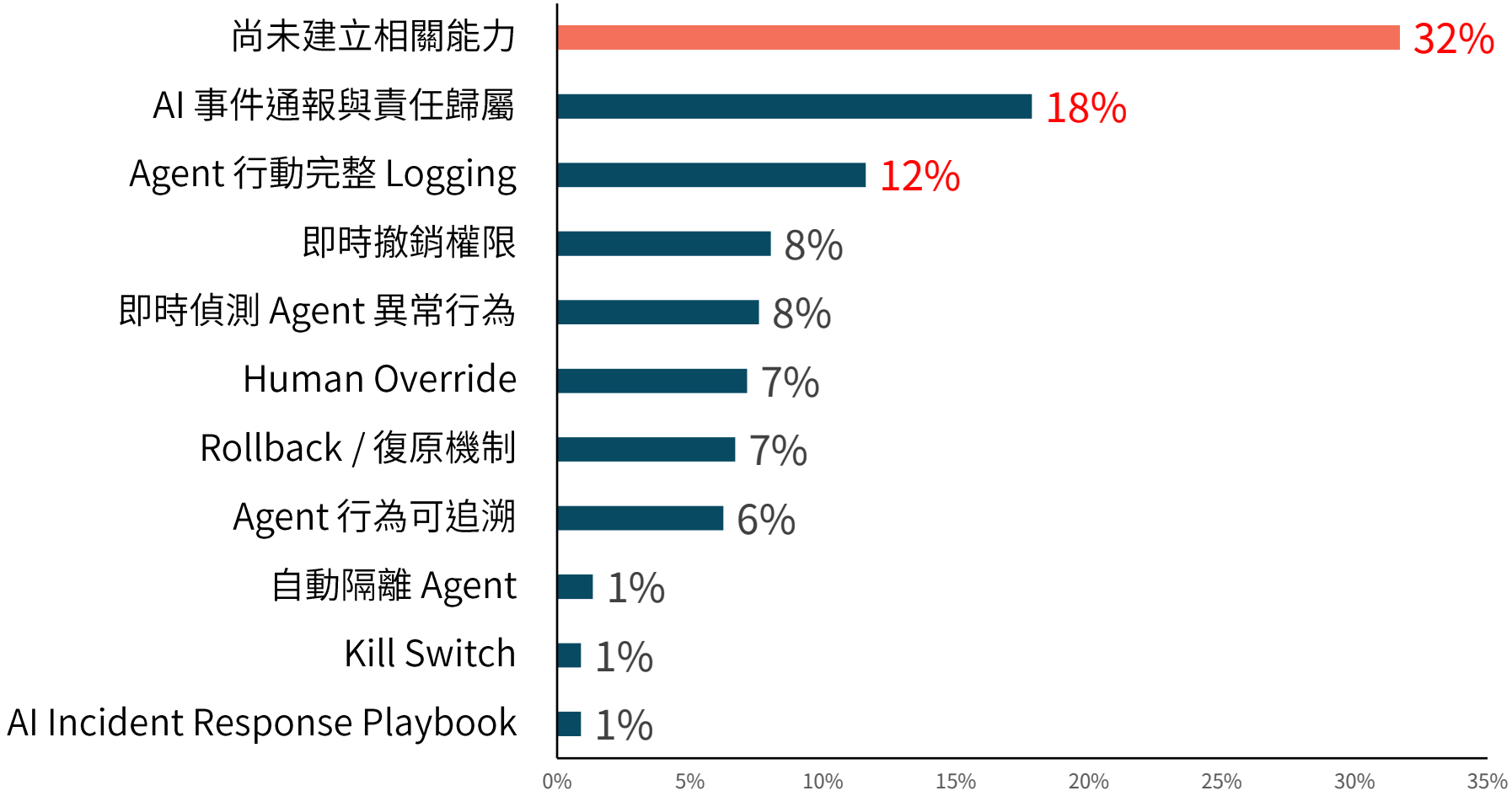
最難管理的三項AI / AI Agent 資安風險



目前在哪些 AI / AI Agent 生命週期建立正式資安控制?



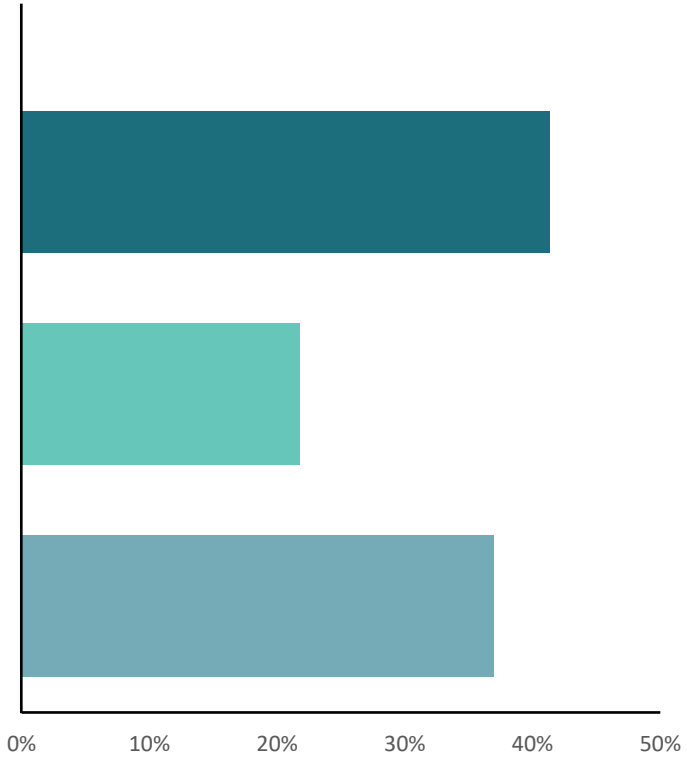
若 AI Agent 發生異常、遭受攻擊或執行錯誤行動，公司具備哪些反應能力?



於 AI / LLM 應用落地時所採取的實質「資料保護技術」

- 目前完全仰賴員工政策宣導，技術層面尚無專屬資料保護手段 — 44%
- 私有化隔離部署：採用地端私有化模型或 VPC 隔離環境，並簽署零資料留存(Zero Data Retention)協定 — 21%
- Prompt 即時去識別化：於 AI Gateway 即時遮蔽或去識別化機敏個資與商業機密 — 17%
- RAG 動態權限隔離：於向量資料庫落實與企業 AD/IdP 綁定的列級動態權限(RBAC / ABAC)控制 — 17%

全體員工之「AI 安全識讀」教育訓練現況



41% 已將「AI 安全識讀與負責任 AI 使用」納入全體員工年度必修資安教育訓練

22% 僅針對特定部門(如 IT、研發或財務)提供專門之 AI 資安防禦與合規訓練

37% 目前尚未針對 AI 安全安排實質全員訓練



四、供應鏈安全與第三方風險管理

CIO Taiwan CISO 資安學院

供應鏈資安的常態管理機制



1. 已建立動態且持續性的供應商資安稽核機制（定期檢附 ISO 27001、SOC 2 或現場抽稽）



25%

2. 僅針對核心一級（Tier 1）關鍵供應商管理，二三線外包商存在嚴重盲點



12%

3. 僅於合約簽署階段進行一次性紙本資安宣告或問卷，缺乏後續技術追蹤



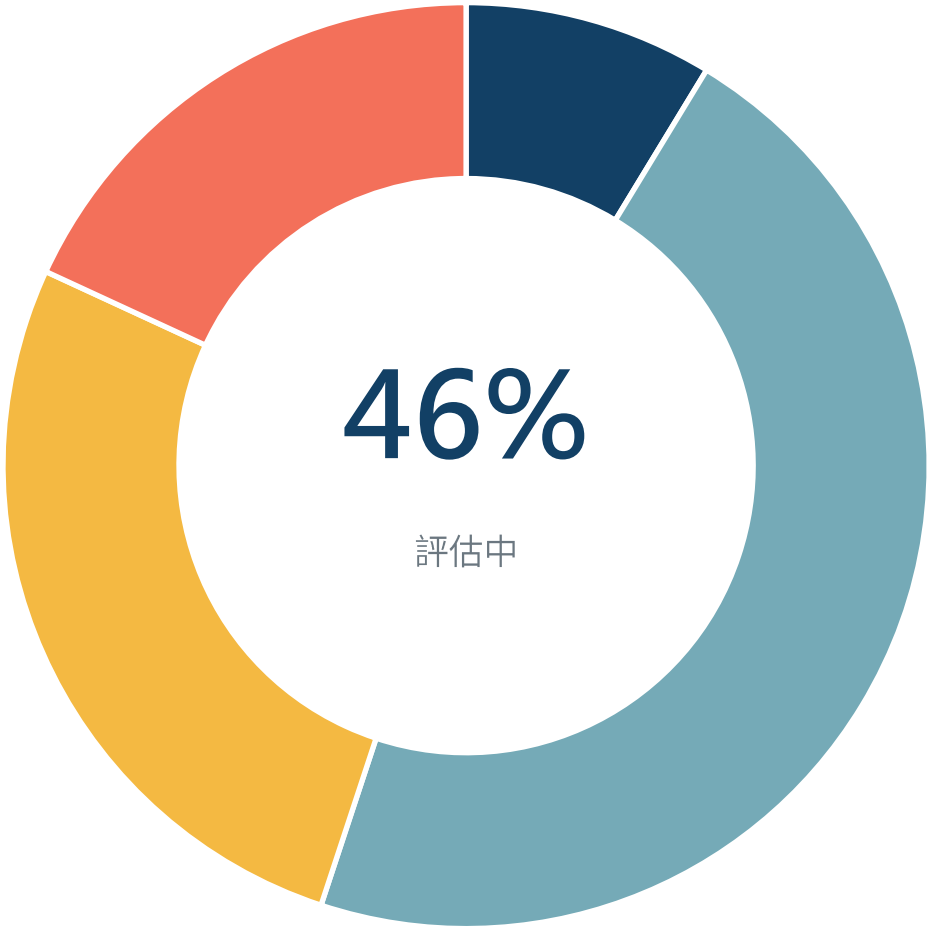
36%

4. 尚未將供應鏈風險納入常態合規與治理範疇



27%

在委外開發與開源組件管理上，是否要求軟體供應商提供「軟體物料清單（SBOM）」？



9% 已全面導入 SBOM

已全面要求廠商檢附 SBOM，並對接自動化漏洞情資

46% 評估中

正嘗試在核心系統委外合約加入 SBOM 條款，尚未普及

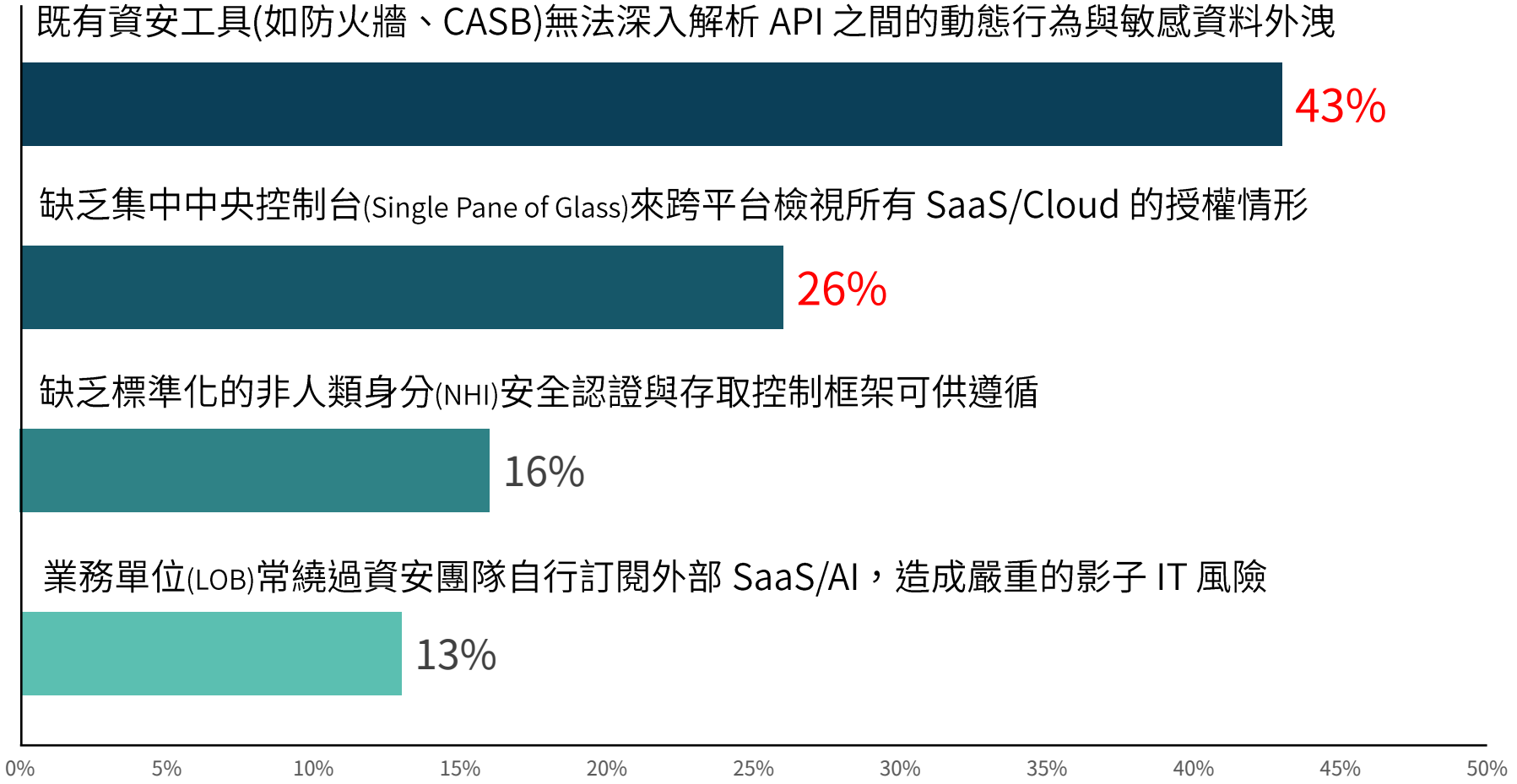
27% 暫不考慮

受限於國內軟體開發結構或供應商配合度，難以強制推行

18% 不了解 SBOM

對 SBOM 的實務概念與應用價值尚不了解

阻礙企業有效治理跨系統連線與 API 信任破口（引擎室生態系破口）的核心技術瓶頸



在採購與引進第三方 AI SaaS 或 API 服務時，要求供應商必須提供哪些「專屬安全承諾」？

31%

零資料留存與免訓練承諾：明文保證客戶資料絕不被用於通用模型訓練，且具備 Zero Data Retention 機制

25%

獨立第三方安全認證：出具 SOC 2 Type II、ISO/IEC 42001 或 ISO 27001 等認證報告

尚未針對 AI 供應商訂定專屬安全要求 23%

智慧財產權擔保(IP Indemnity)：提供因 AI 生成內容衍生侵權訴訟之法律賠償與擔保承諾 11%

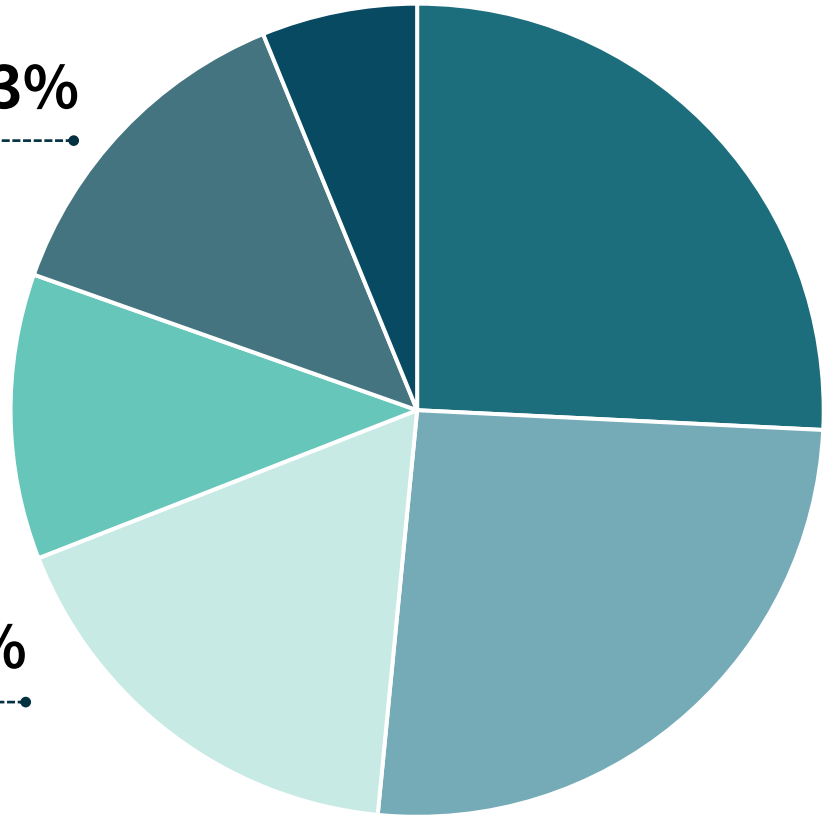
資料主權與在地化：承諾資料處理與推理終端(Inference Endpoint)必須位於指定境內機房 8%



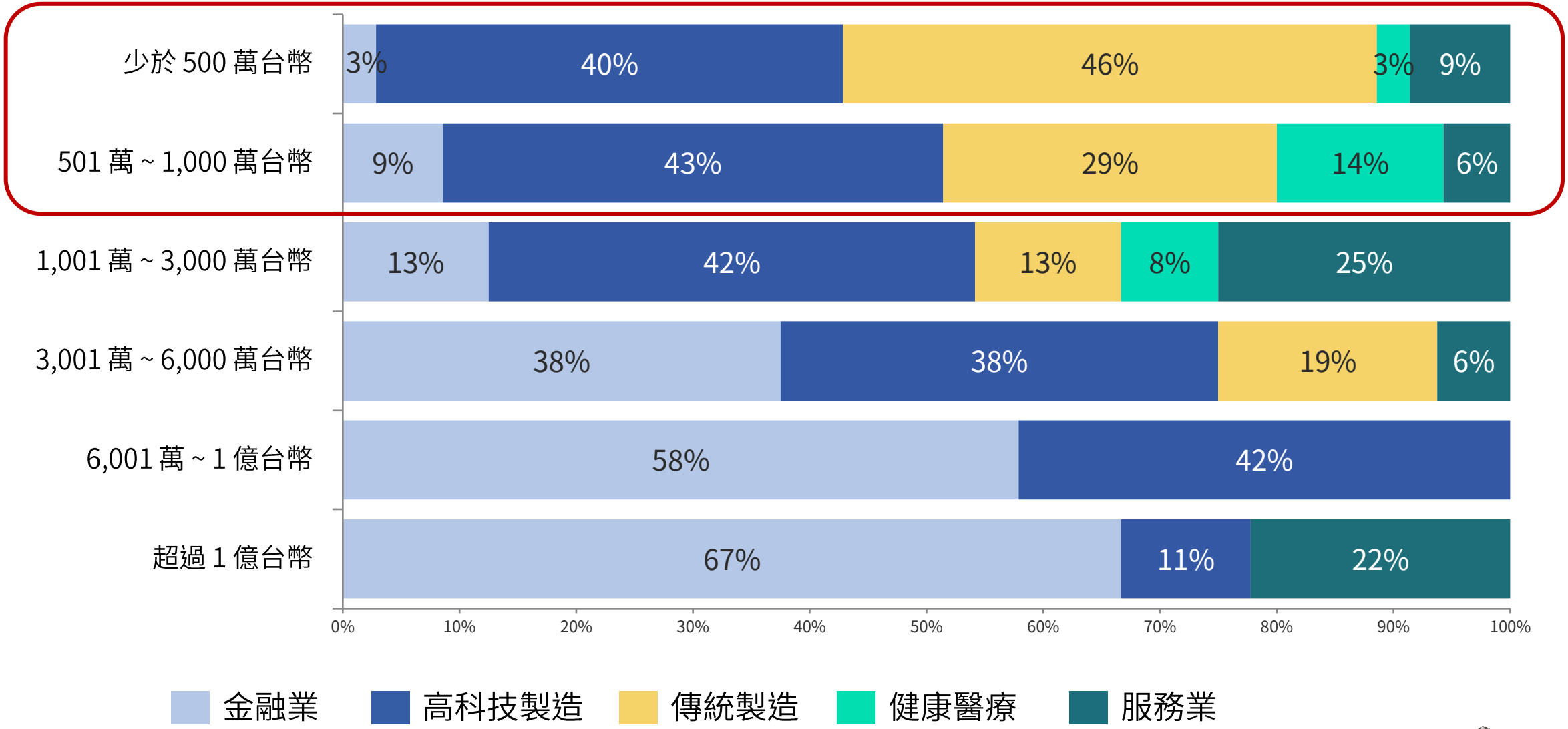
五、資安預算與採購

CIO Taiwan CISO 資安學院

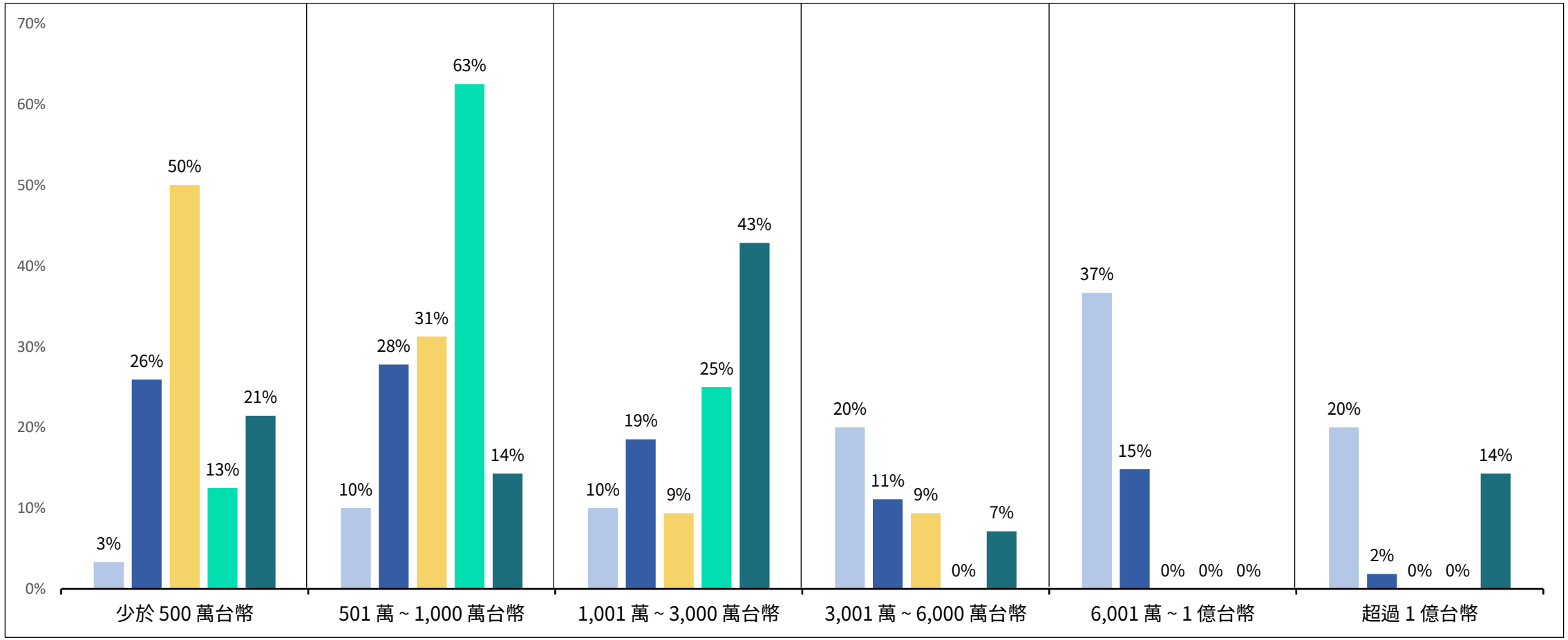
2027 年全產業資安總預算



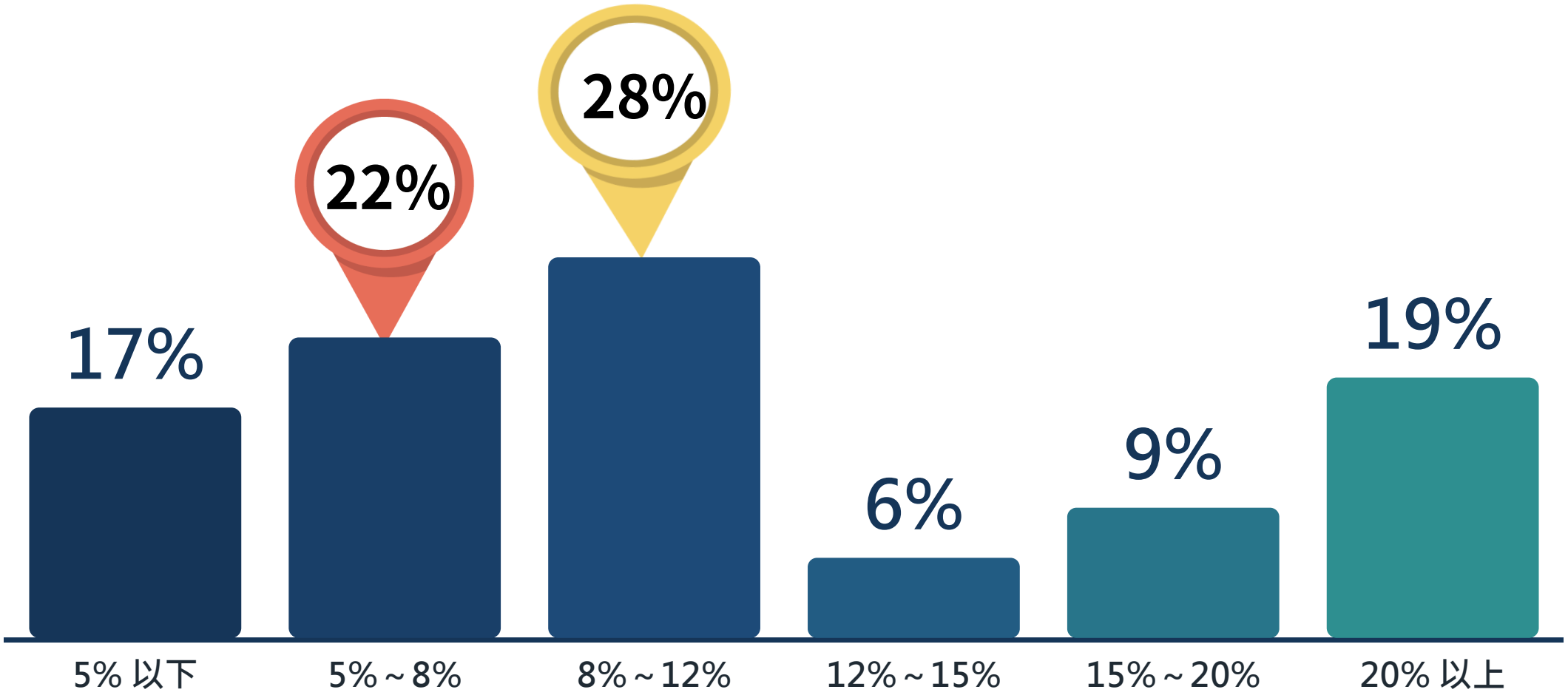
2027 年各產業資安總預算分佈



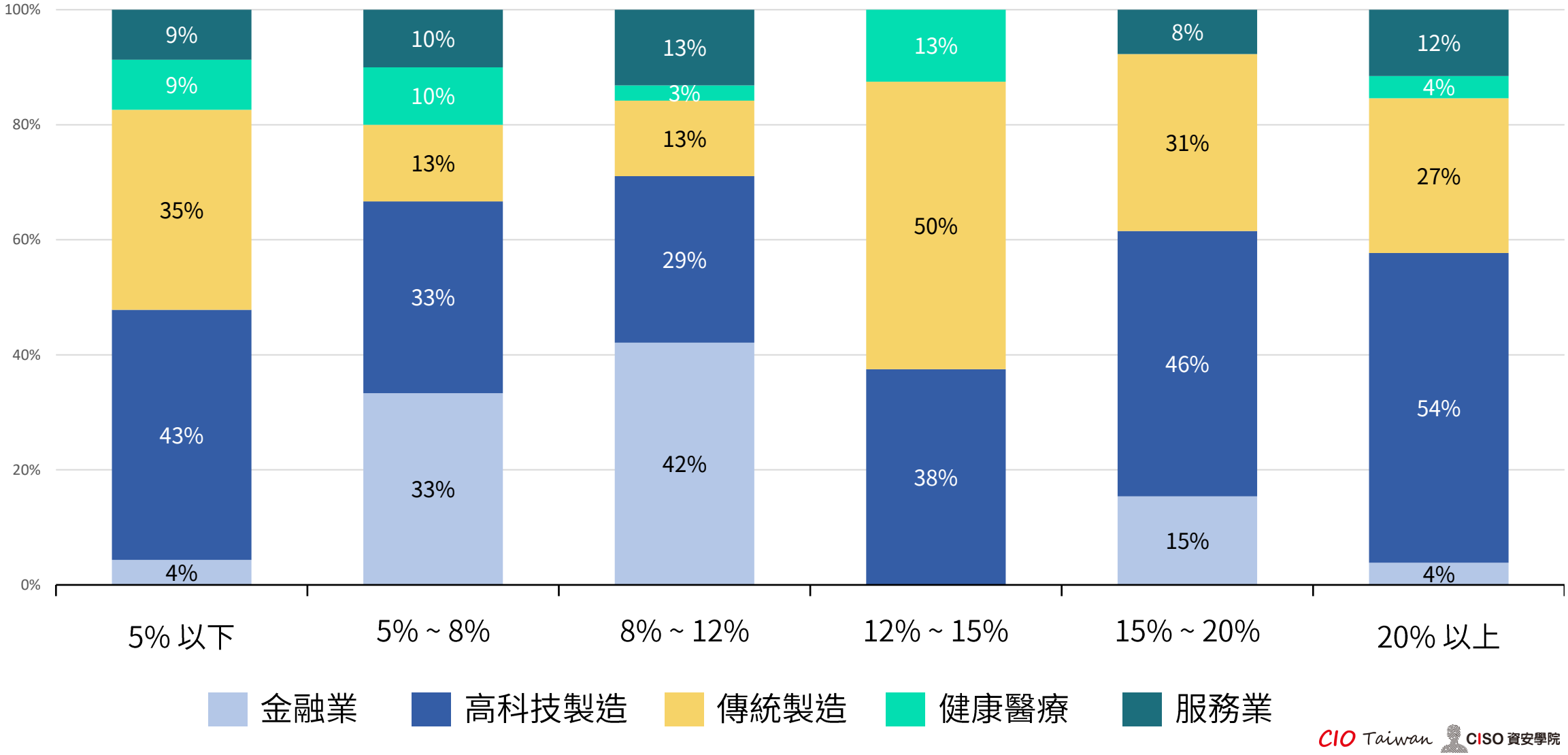
2027 年資安總預算各區間的產業別佔比



2027 年全產業資安總預算占 IT 總預算之比例

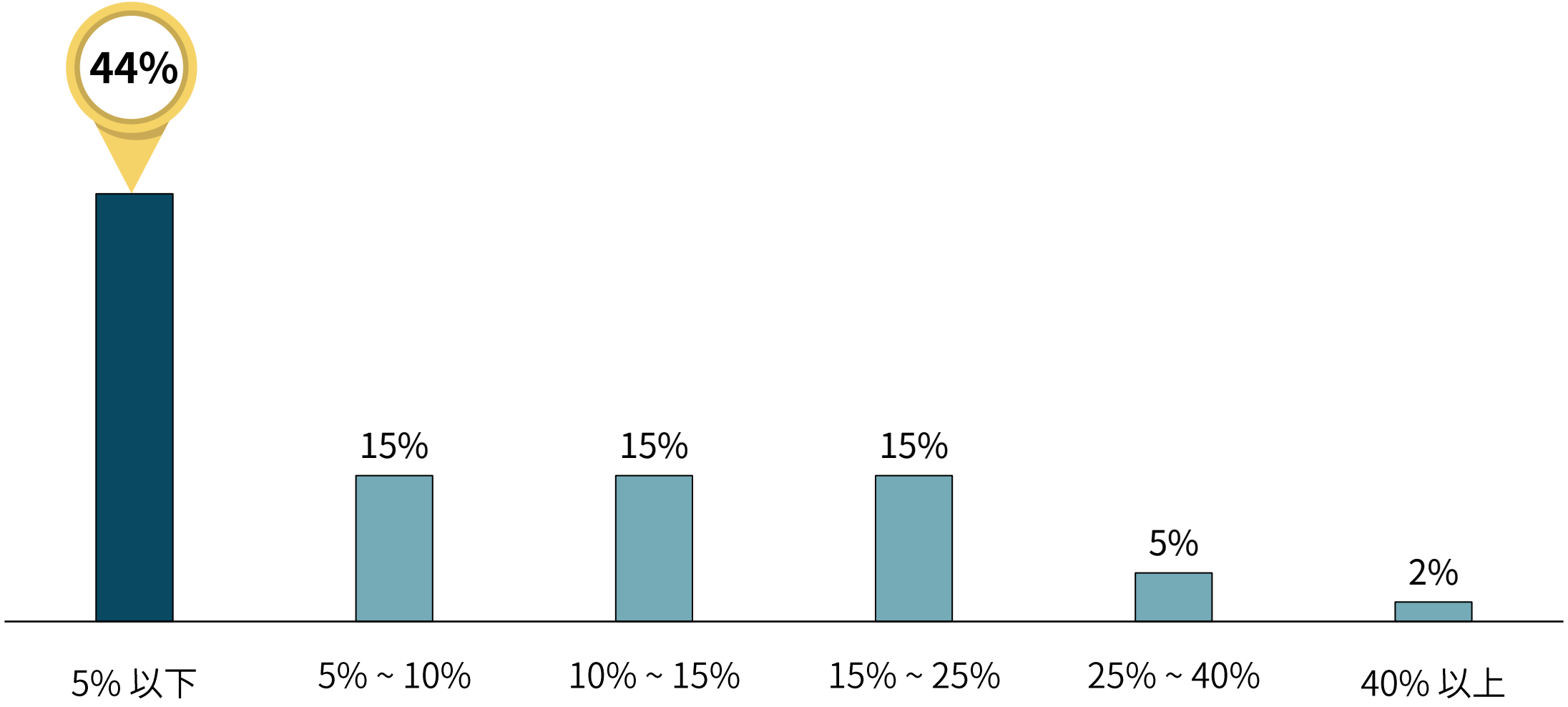


2027 年各產業資安總預算占 IT 總預算之比例

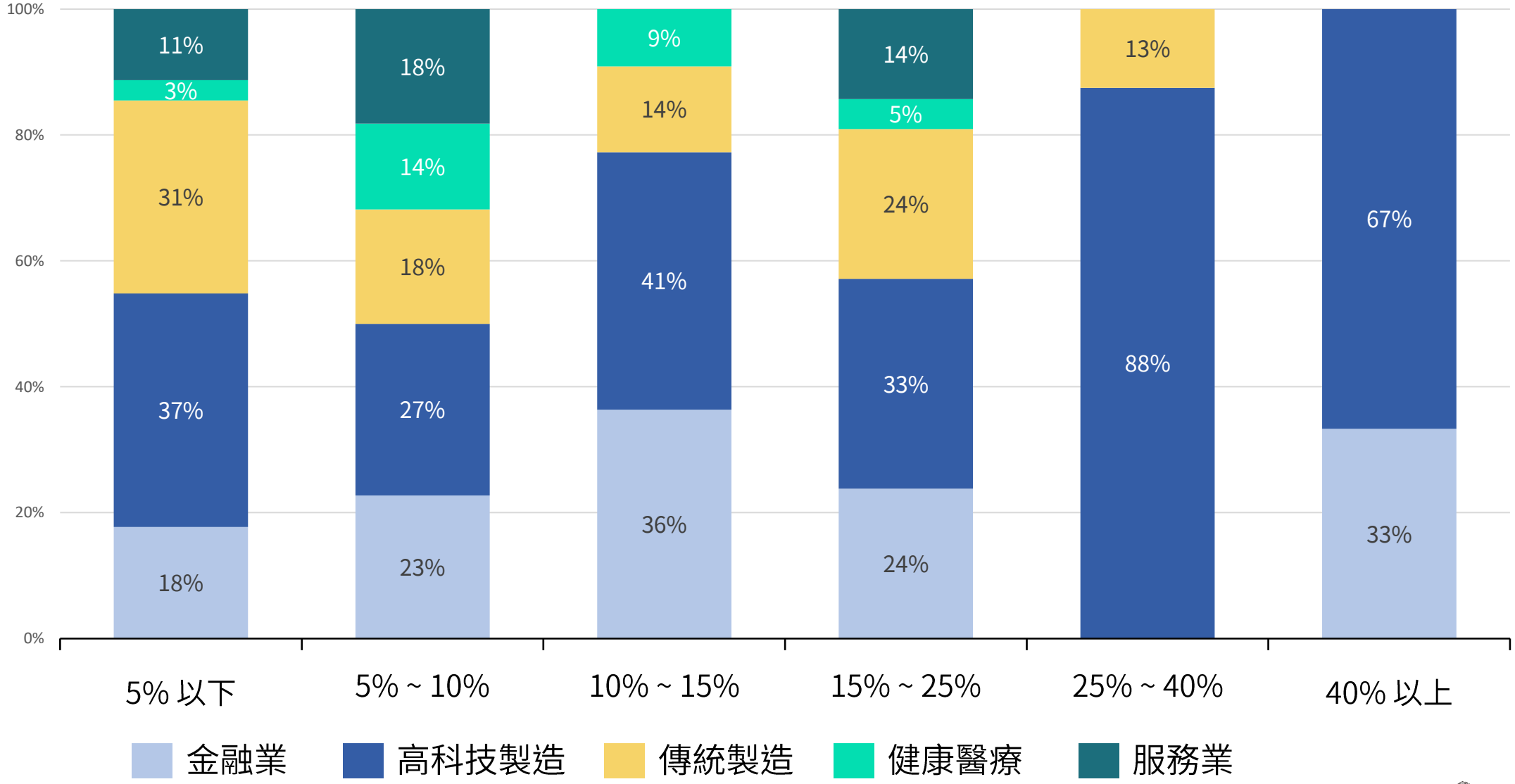


CIO Taiwan CISO 資安學院

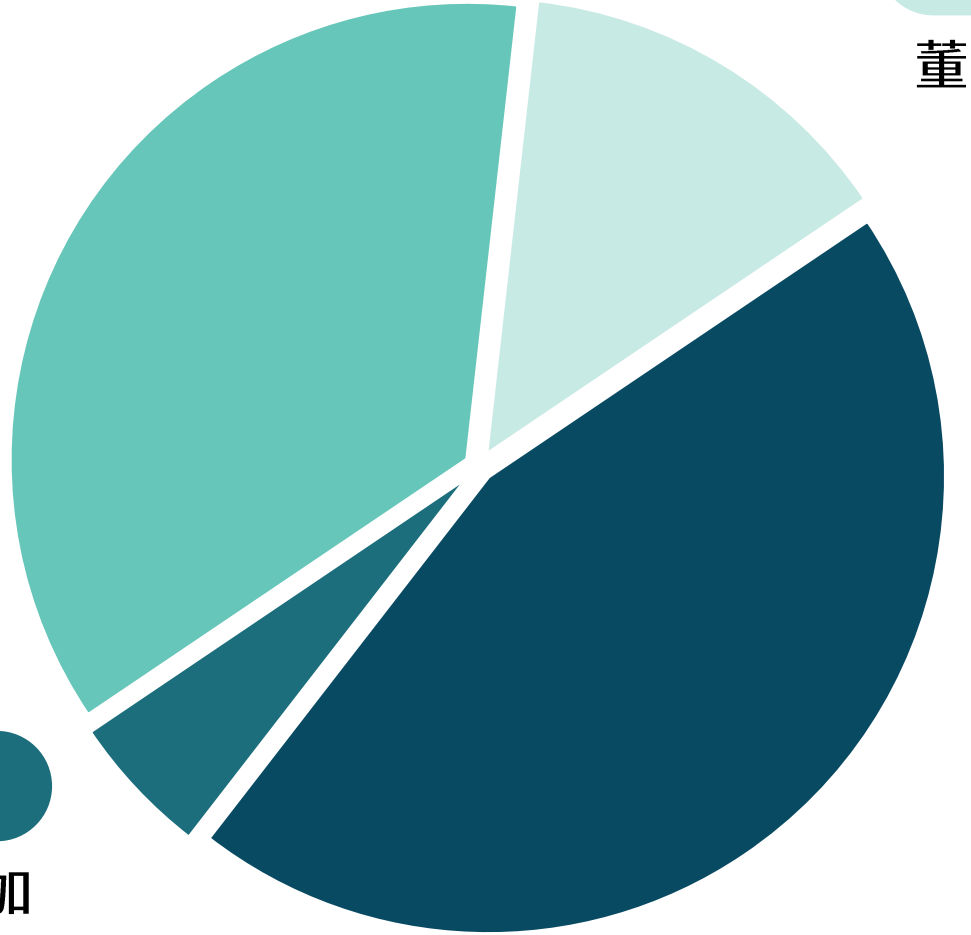
AI 相關安全投資占資安總預算的比例



各產業AI 相關安全投資占資安總預算的比例



貴公司的資安預算決策來源?



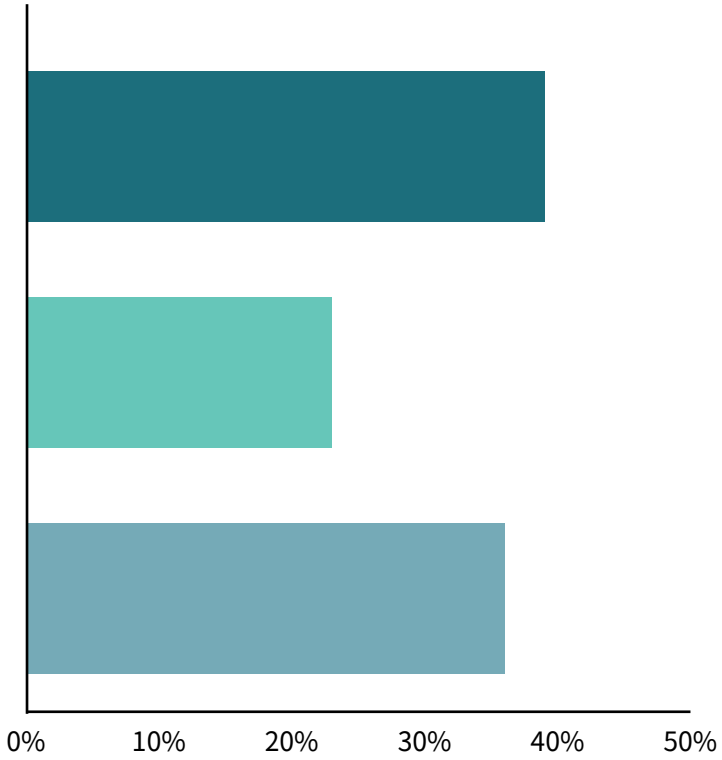
14%
董事會要求

36%
業務轉型需求

45%
法規要求

5%
發生事件後增加

資安財務預算的「支出類型結構」配置



39% **以資本支出為主**
偏重地端軟硬體資產採購、機房與實體設備建置

23% **以營運支出為主**
偏重雲端訂閱制服務、SaaS安全、MSSP託管與定期顧問服務

36% **資本支出及營運支出各半**
資本支出與營運支出結構比例大約各半

2027年的資安預算是增加還是減少?

↑ **增加：AI 專屬防護**
因應生成式 AI / Agentic AI 導入所需之專屬安全防護投資



37%

↑ **增加：法規遵循**
因應境內外法規遵循（資安法、個資法及主管機關要求）



22%

= **持平**
既有資安運作已達飽和，以現有資源維護與小幅調整



32%

↓ **縮減**
受企業整體營運成本控管或經濟大環境影響而壓縮



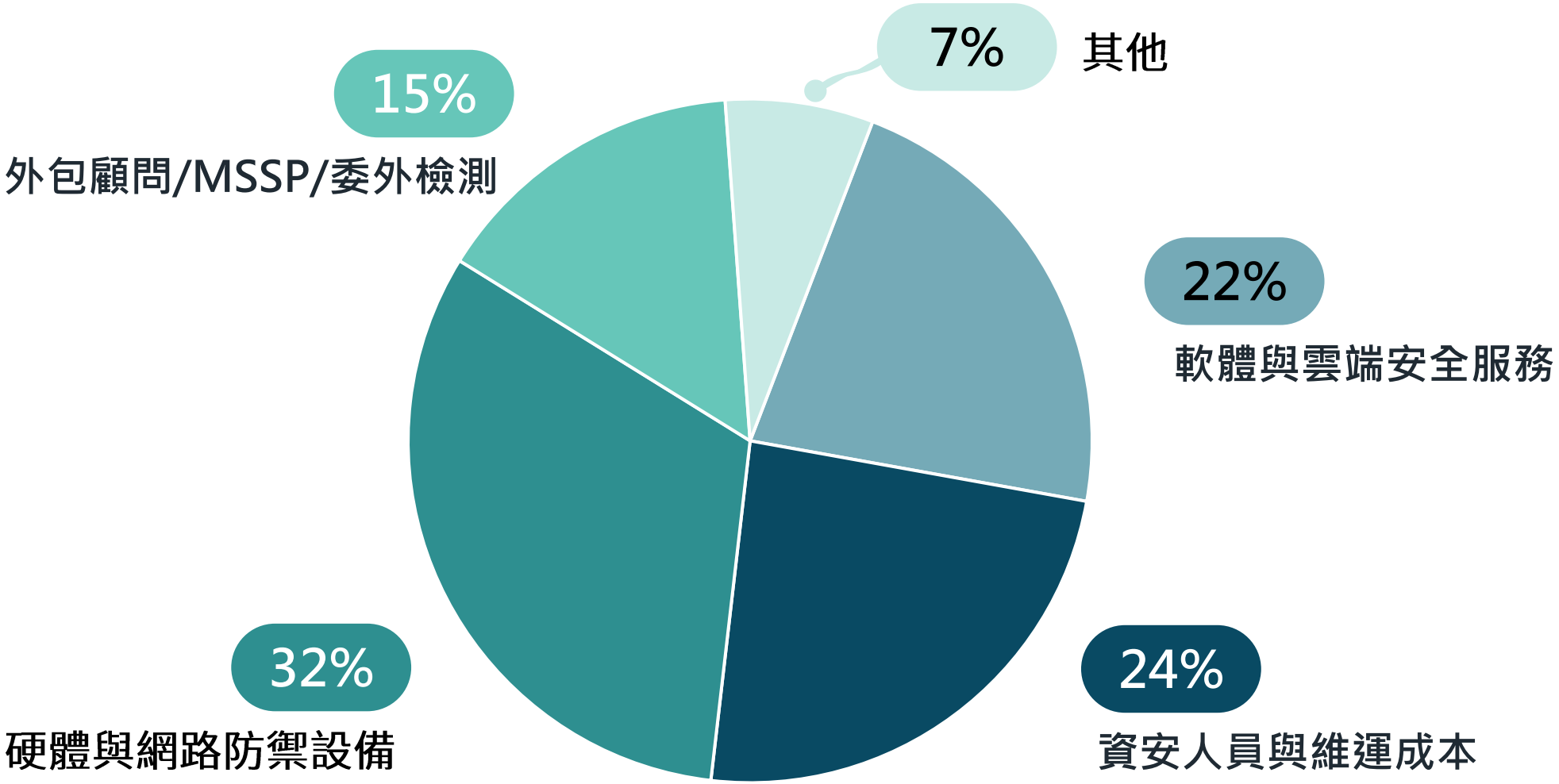
5%

↑ **增加：事件或供應鏈風險**
曾發生資安事件或供應鏈風險升高，董事會要求強化投資

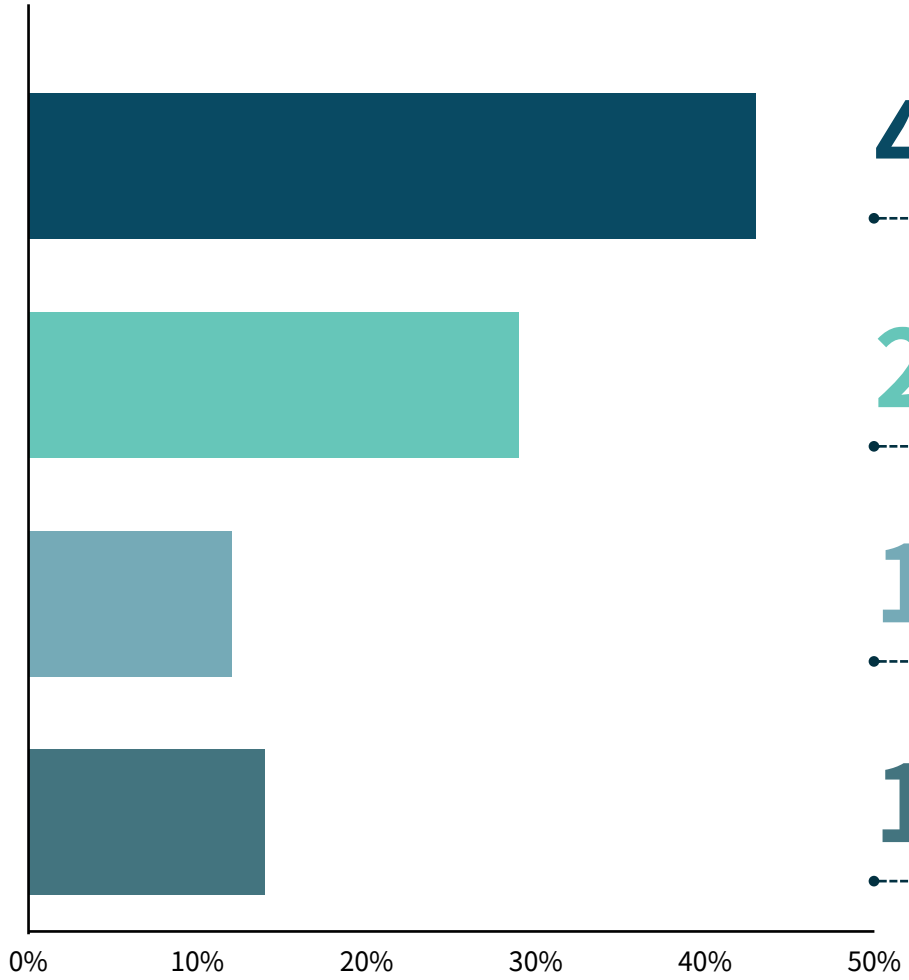


4%

2027年重點資安項目的預算分配比例



衡量資安 ROI / 投資成效的主要方式



43% 以法規合規與稽核達成率為主

29% 以資安事件發生率與避免之潛在財務損失量化衡量

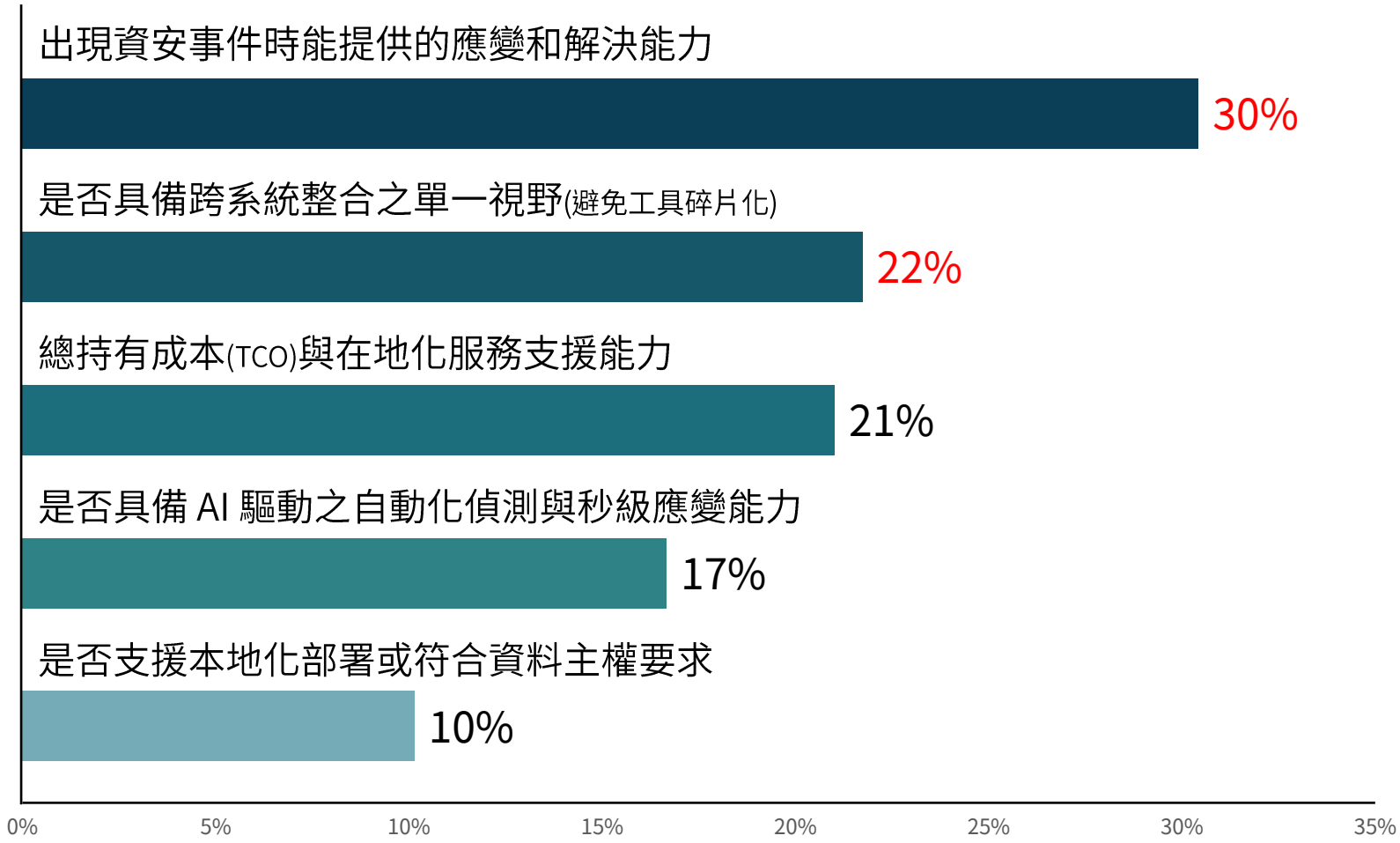
12% 以平均偵測與應變時間(MTTD / MTTR)縮短為指標

14% 目前尚無正式量化衡量機制

2027 年的資安採購優先項目

1. AI 驅動之威脅偵測與自動化回應
2. 端點偵測與應變(EDR / XDR)擴充
3. 零信任架構(ZTA)與微隔離方案
4. 身分與存取管理(IAM)及非人類身分(NHI/ITDR)治理平台
5. SaaS 與 AI 生態系安全平台(SSPM / 跨應用資料流監控)
6. 資料安全態勢管理(DSPM)與雲端安全(CSPM / CNAPP)

資安長最重視的採購評選條件

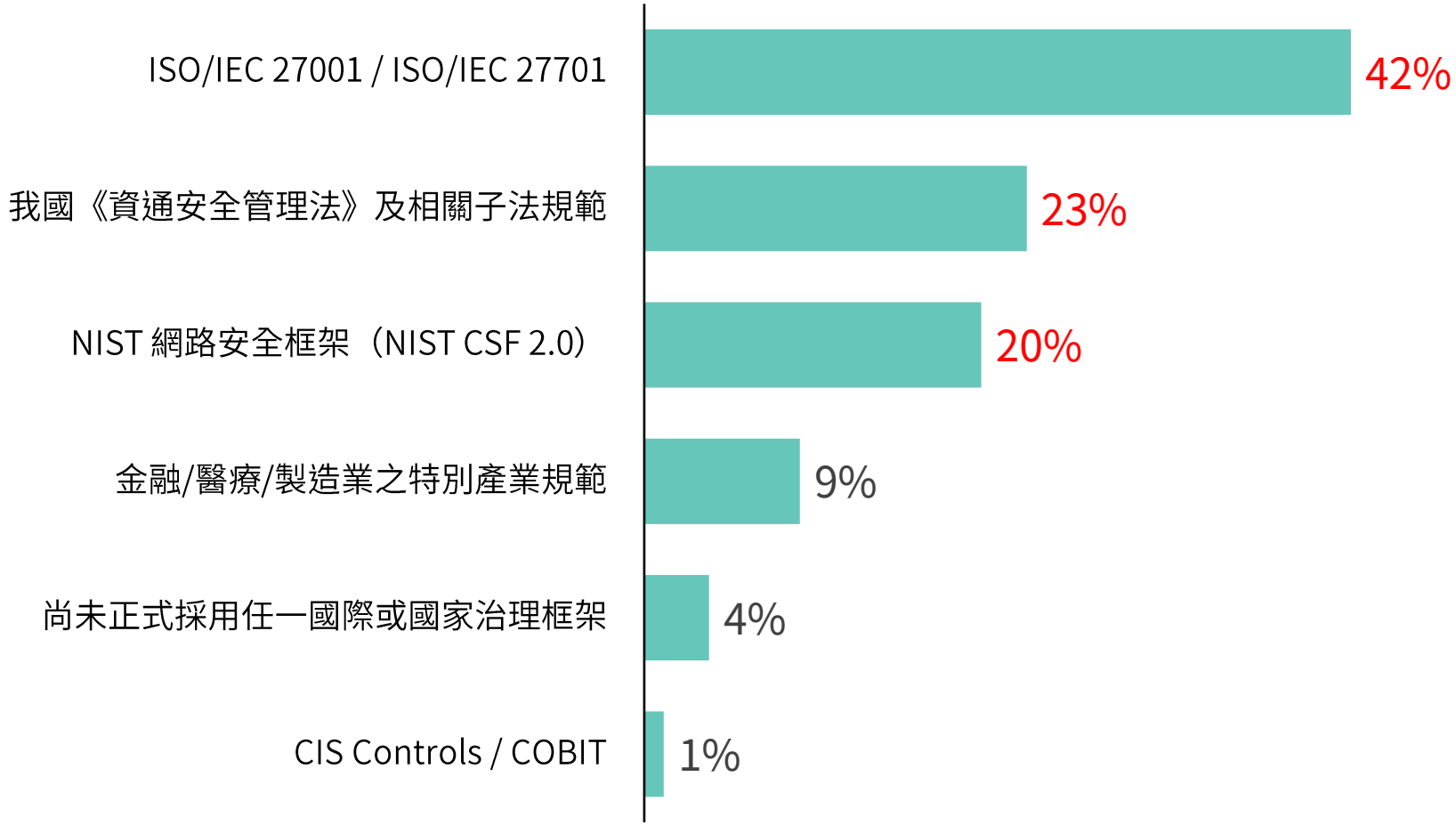




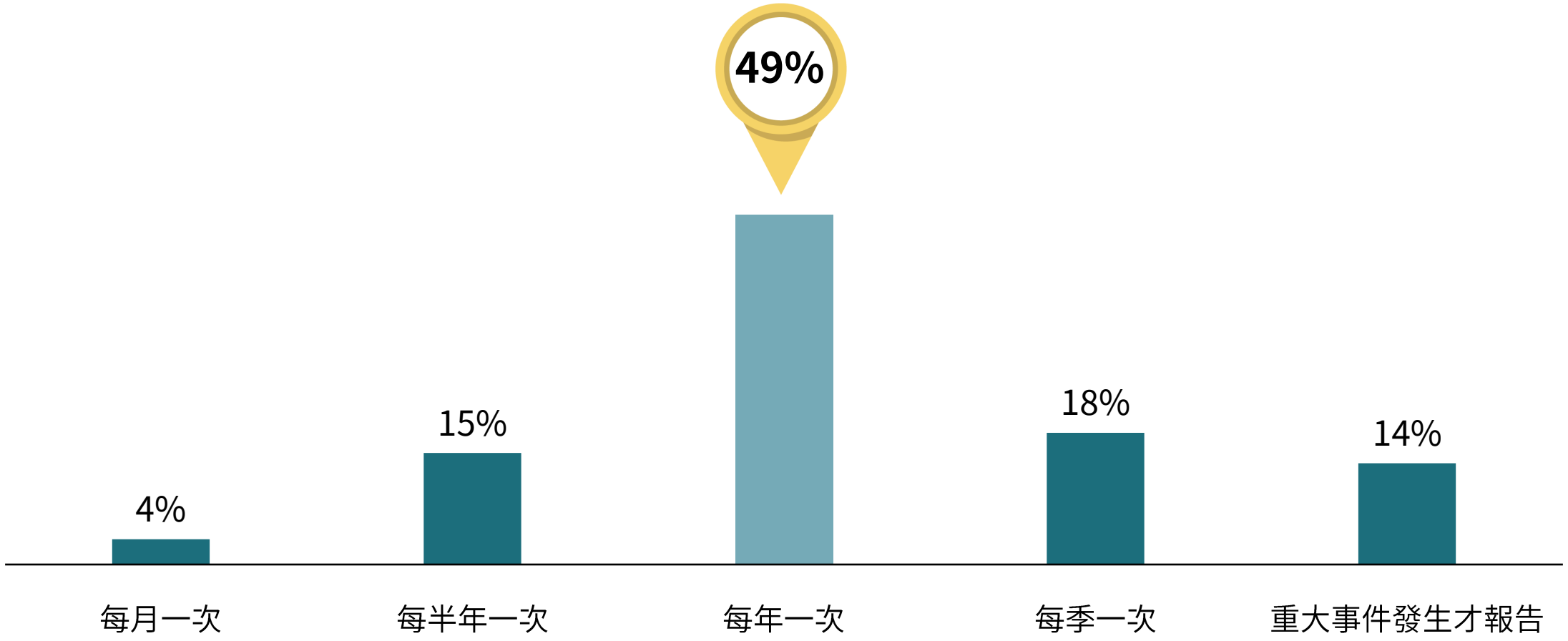
六、資安治理與資安長角色

CIO Taiwan CISO 資安學院

公司主要參採之「資安治理框架與標準」



多久向董事會 / 最高管理階層報告一次資安風險?



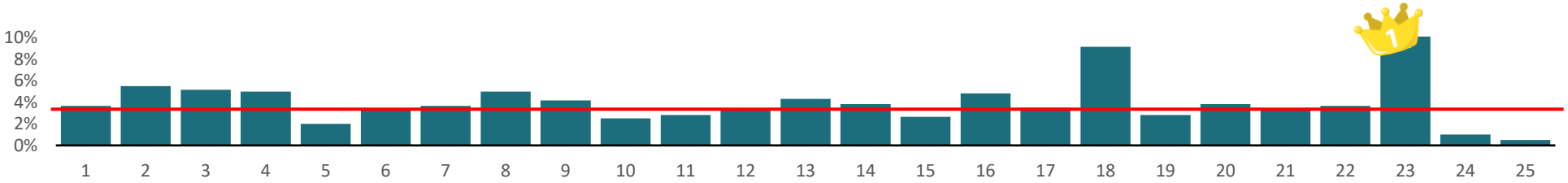
在資安防護中最需要補強的破口?



	治理 Govern				
	識別 Identify	保護 Protect	偵測 Detect	回應 Respond	復原 Recover
設備 Device	1 資產盤點 設備風險評估	2 端點保護 設備強化	3 惡意軟體偵測 設備行為分析	4 隔離受感染設備 鑑識分析	5 設備重建 補救措施實施
應用程式 Application	6 應用程式清單 應用程式風險評估	7 安全編碼實踐 應用程式加固	8 應用程式監控 應用程式日誌分析	9 應用程式緊急修補 事件溯源	10 應用程式還原 程式碼審查
網路 Network	11 網路封包分析 網路弱點管理	12 網路隔離 邊界防護	13 入侵偵測 網路流量分析	14 阻斷惡意連線 網路封鎖	15 網路重構 網路優化
資料 Data	16 資料分類 資料風險評估	17 資料加密 資料備份	18 資料外洩偵測 資料存取稽核	19 資料回復 資料外洩通報	20 資料復原 資料完整性驗證
使用者 User	21 使用者帳號管理 使用者風險評估	22 存取控制 安全意識教育	23 異常行為偵測 使用者行為分析	24 停用可疑帳號 使用者調查	25 帳號復原 存取權限審查

2026年前5名

2027年前5名



CIO Taiwan CISO 資安學院

在2027年最關注推動的區塊

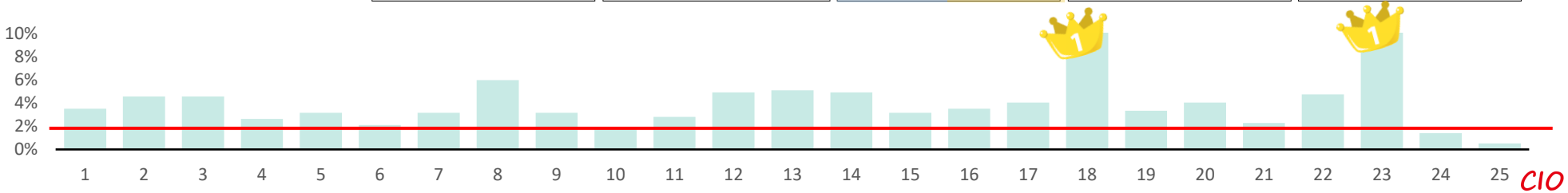


治理 Govern

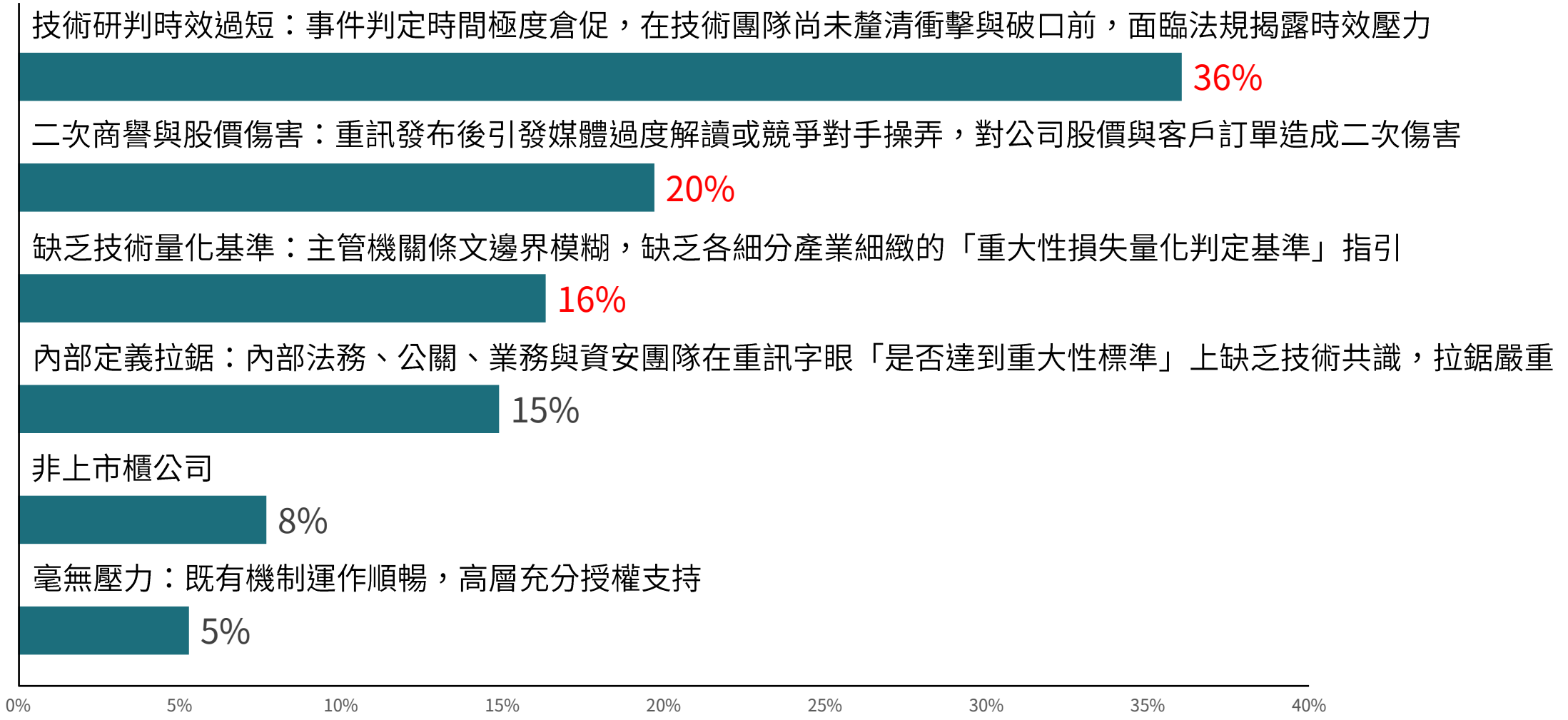
	識別 Identify	保護 Protect	偵測 Detect	回應 Respond	復原 Recover
設備 Device	1 資產盤點 設備風險評估	2 端點保護 設備強化	3 惡意軟體偵測 設備行為分析	4 隔離受感染設備 鑑識分析	5 設備重建 補救措施實施
應用程式 Application	6 應用程式清單 應用程式風險評估	7 安全編碼實踐 應用程式加固	8 應用程式監控 應用程式日誌分析	9 應用程式緊急修補 事件溯源	10 應用程式還原 程式碼審查
網路 Network	11 網路封包分析 網路弱點管理	12 網路隔離 邊界防護	13 入侵偵測 網路流量分析	14 阻斷惡意連線 網路封鎖	15 網路重構 網路優化
資料 Data	16 資料分類 資料風險評估	17 資料加密 資料備份	18 資料外洩偵測 資料存取稽核	19 資料回復 資料外洩通報	20 資料復原 資料完整性驗證
使用者 User	21 使用者帳號管理 使用者風險評估	22 存取控制 安全意識教育	23 異常行為偵測 使用者行為分析	24 停用可疑帳號 使用者調查	25 帳號復原 存取權限審查

2026年前5名

2027年前5名



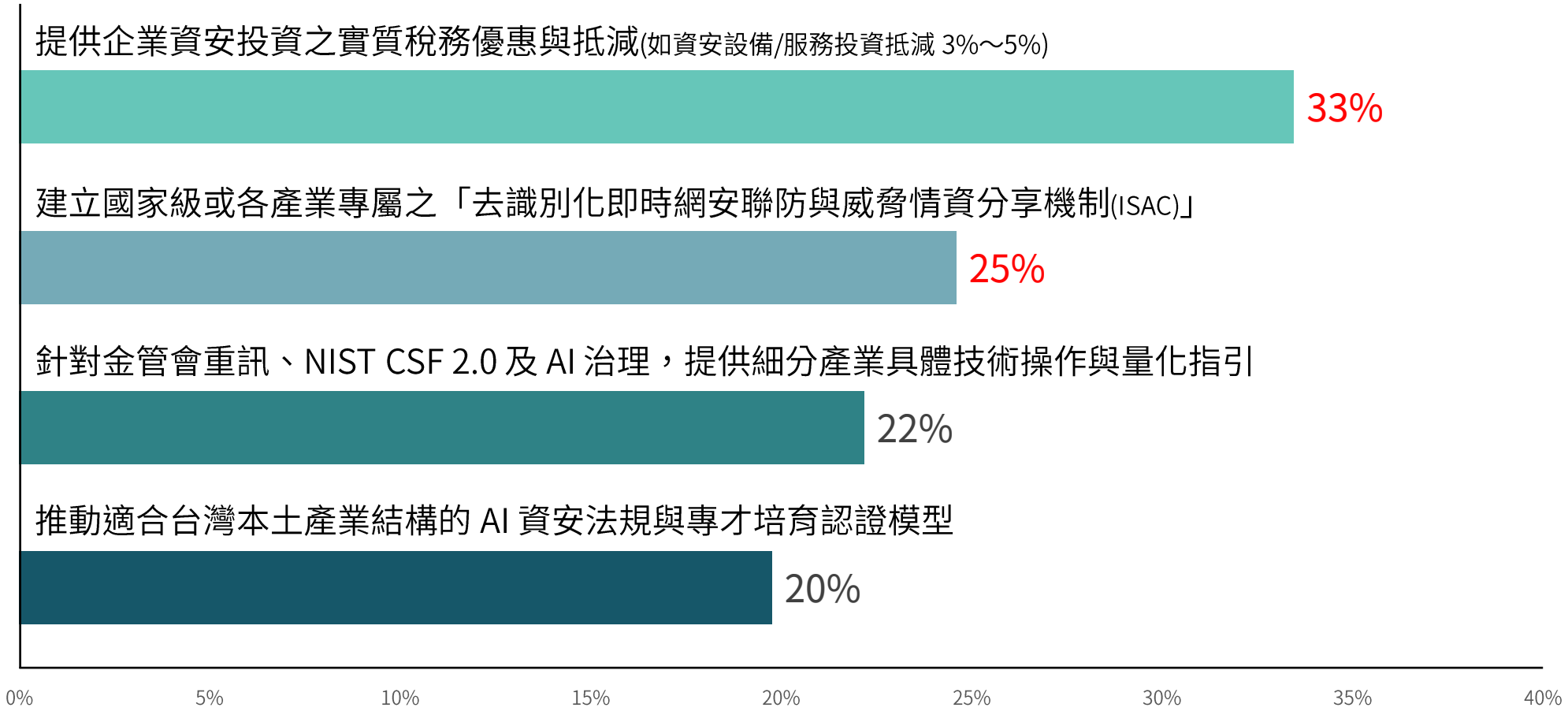
面對「上市櫃公司遭遇重大資安事件必須即時發布重大訊息揭露（重訊）」之規定，您的主要壓力來源為何?



未來一年最具挑戰性的法規要求

- 新興 AI 治理法規落地：針對模型透明度、數據防範與 Agent 越權之合規要求 **30%**
- 重大事件限時通報：未完整鑑識即需於 24/72HR 內揭露，面臨資本市場壓力 **24%**
- 數位營運韌性與強制演練：金融與關鍵產業被要求執行極端情境兵推與嚴格 RTO/RPO **10%**
- 《個資法》修法與專責機關成立：裁罰金額大幅提升、實地稽核常態化與違規強制通報 **9%**
- 《資安法》修法擴大納管：關鍵基礎設施與特定民間企業之防護基準要求大幅提高 **8%**
- 多層級供應鏈連帶監理責任：資安責任延伸至第三方/第四方外包商 **7%**
- 跨境數據流動與資料主權限制：各國數據在地化法規趨嚴，大幅拉升跨國架構營運成本 **6%**
- 跨國雙重合規與標準衝突：多國法規互不採認且要求重疊，造成合規資源嚴重分散 **3%**

資安長最希望公單位為企業資安提供的具體協助



身為資安長的最大痛點?

41% 新技術(如 AI)快速進化，資安團隊難以即時因應

34% 權責不對等，責任重大但決策權與預算有限

7% 個人法律責任與工作壓力過大

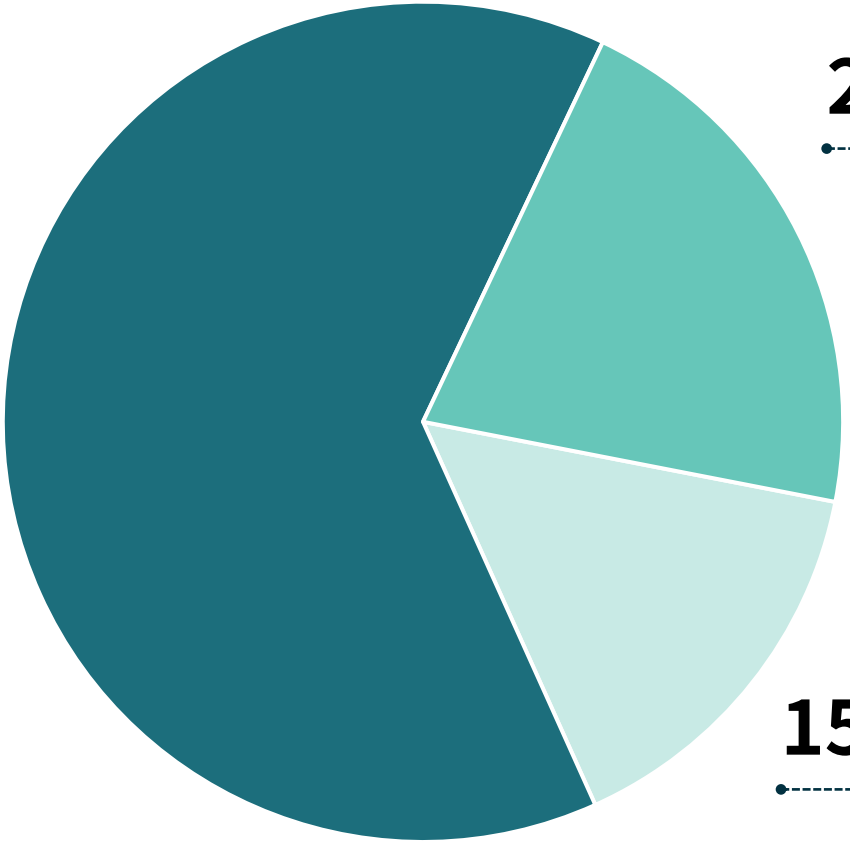
7% 承接很多舊有軟硬體的包袱，可視性太低

5% 找不到人做該做的事

4% 明知供應鏈的廠商有風險，卻僅能建議，無法積極介入

2% 遇到高風險的專案卻沒有否決權

對於資安長是否應比照公司重要成員投保「董監事及重要職員責任保險(D&O）」之態度?

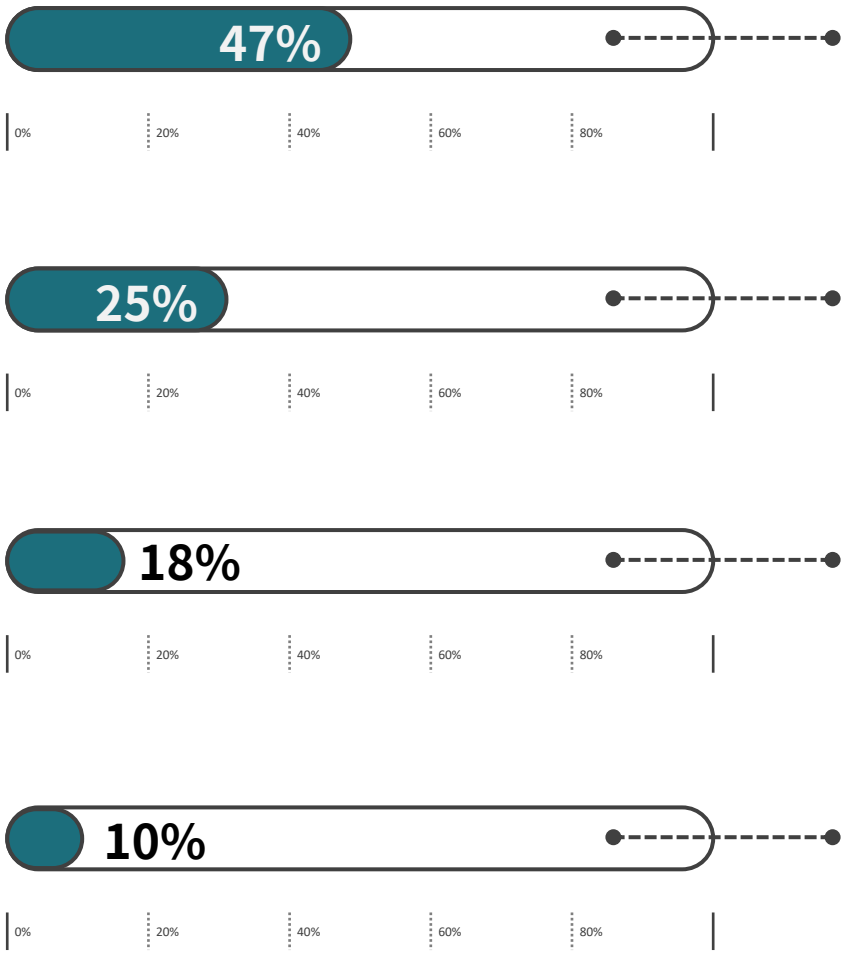


64%
是有必要，但對此只能被動等待

21% 是有必要，會向公司爭取投保

15% 沒有必要，
到時候可能責任會更被加重

身為資安長：未來一年最需提升的能力為何?



AI 與新興科技資安知識

重大資安危機與勒索軟體爆發時的實戰應變、鑑識與媒體公關處置

董事會與高階管理層之風險溝通藝術

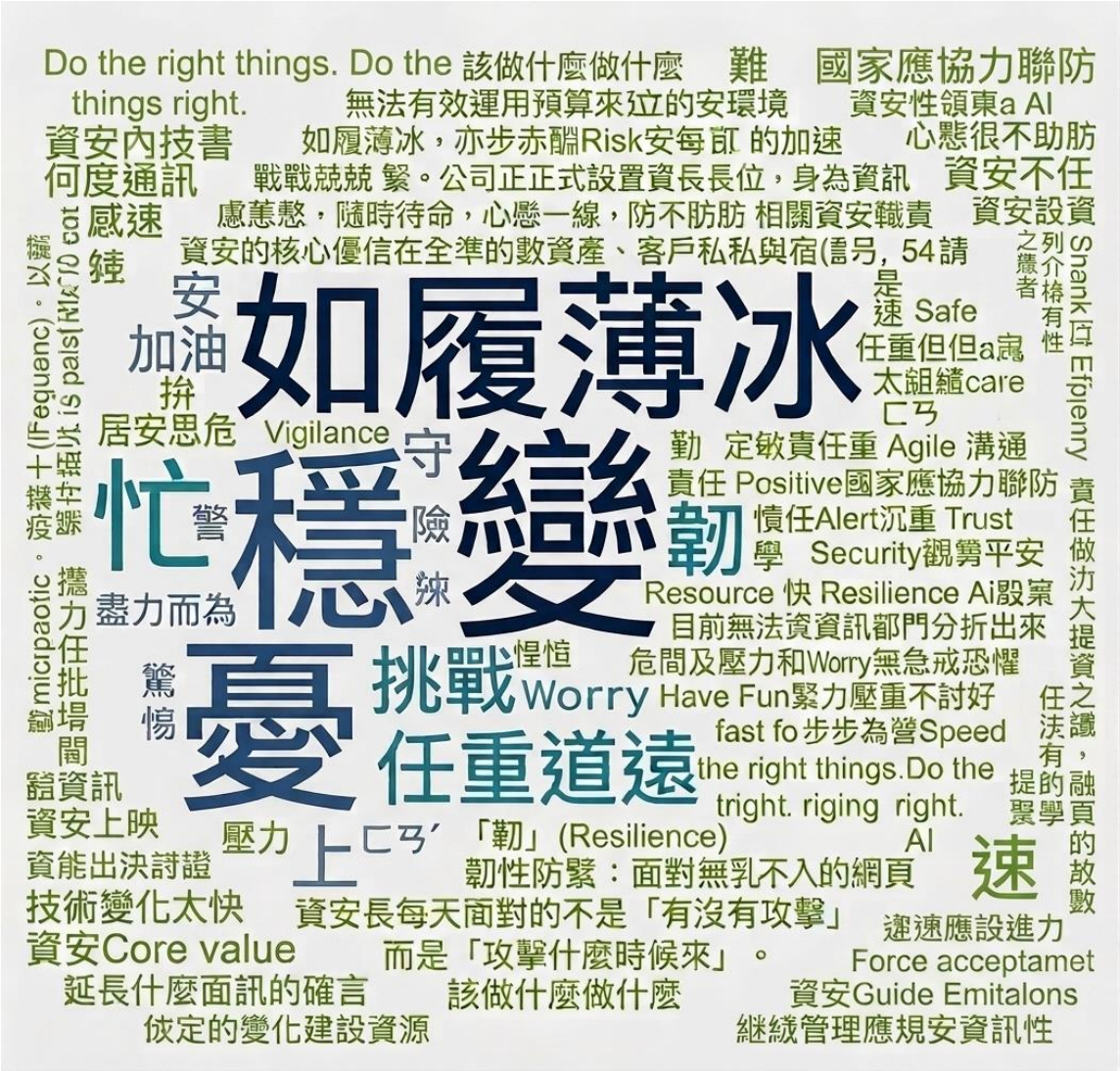
專業的資安長課程，像是CCISO認證，讓管理與資安能力更為提升

您對2027年整體資安風險的能力有沒有信心?

7%	57%	32%	2%
非常有信心	有信心	普通	信心不足



身為企業資安長，您覺得哪個字或詞最能代表您的心情?



如履薄冰 與 變 同票登榜首