CISO 資安學院 CIO Taiwan



2025

CISO Insight

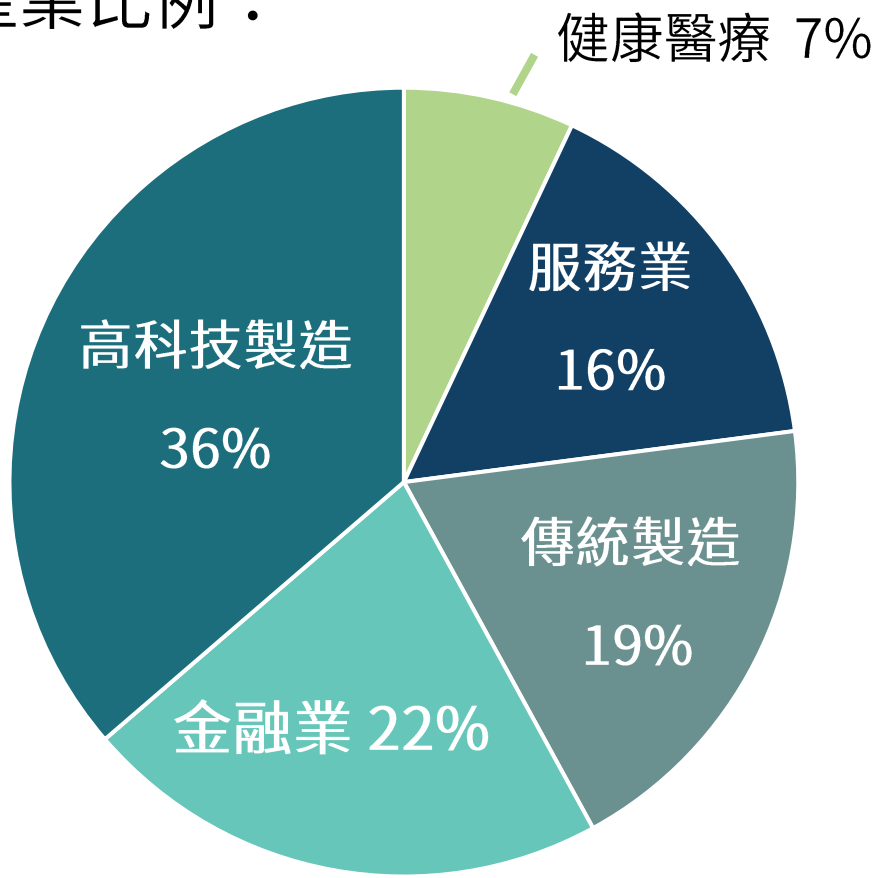
台灣資安長問卷調查

關於CISO Insight 資安問卷調查

- 調查期間：114年8月20日～9月7日
- 有效份數：157
- 調查對象：

  2000大或上市櫃公司資安最高主管

- 產業比例：



目錄



1 受訪者與人力概況

2 資安治理與策略

3 資安預算

4 威脅情勢與資安韌性

5 生成式AI的資安影響

6 供應鏈資安

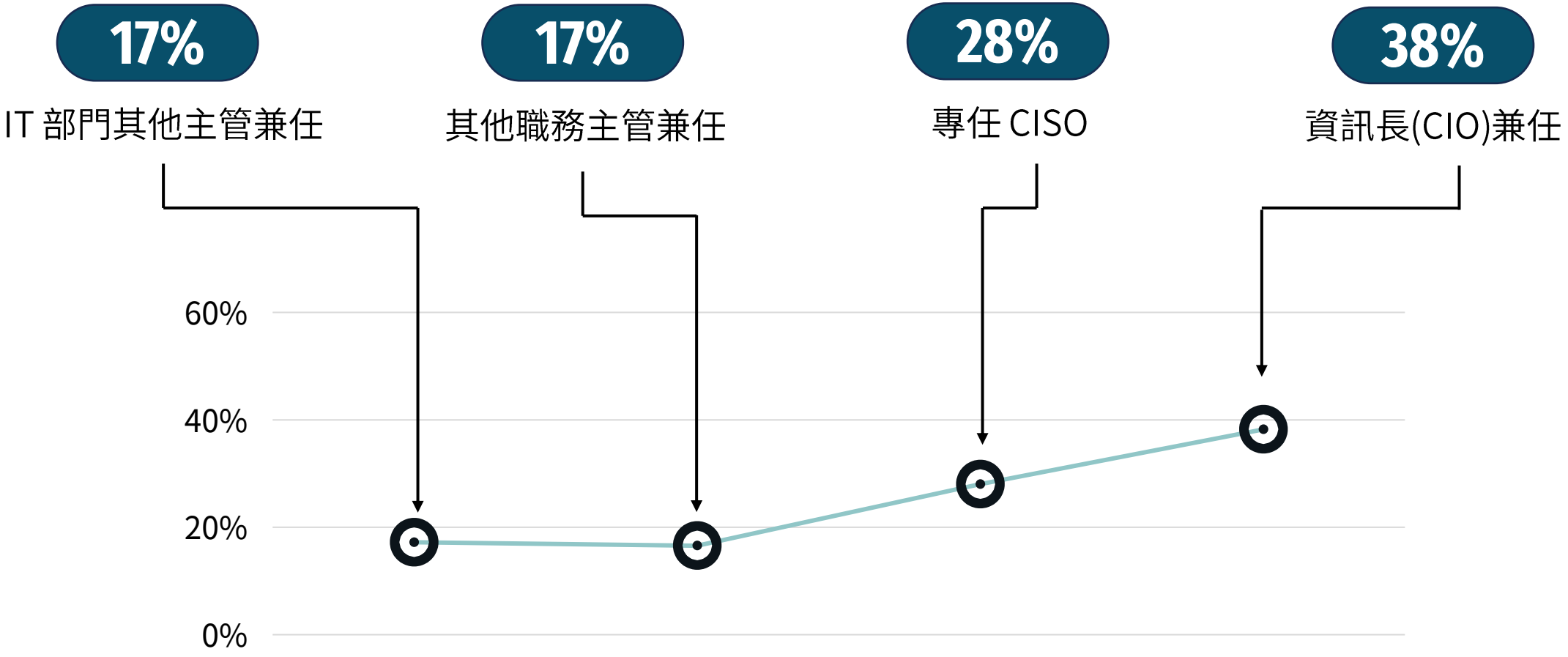
7 法規遵循與合規挑戰

8 其他資安重點與展望

9 關於CISO自己


CISO 資安學院
CIO Taiwan
2025
CISO Insight
台灣資安長問卷調查
一、受訪者與人力概況

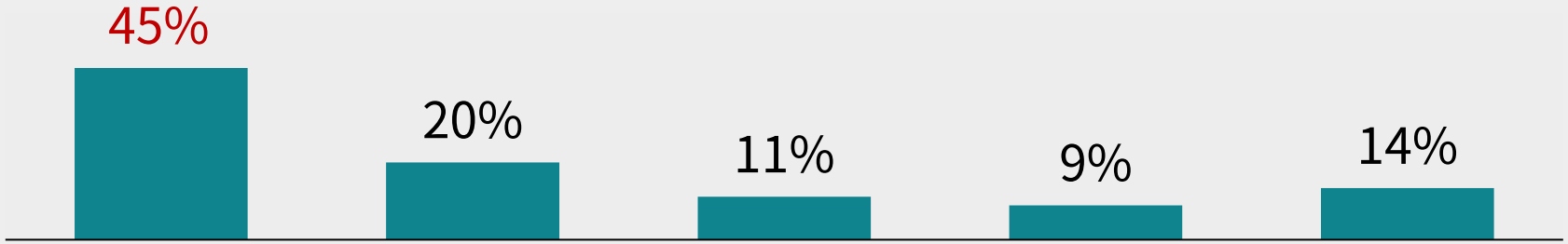
資安長是專任還是兼任?



依產業別來看資安長的專任及兼任

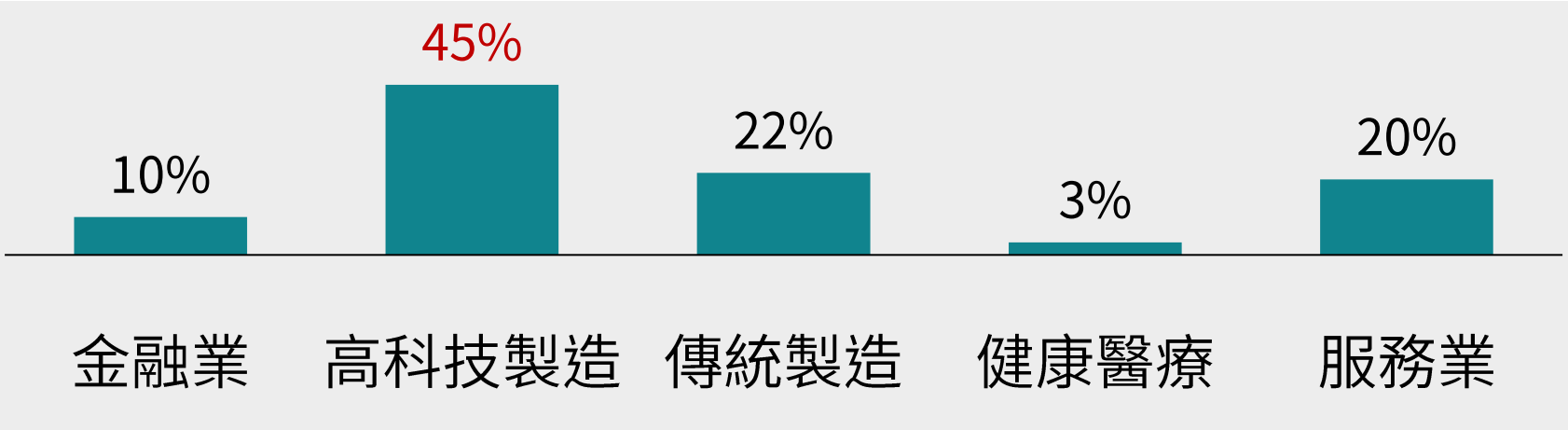
28%

專任 CISO

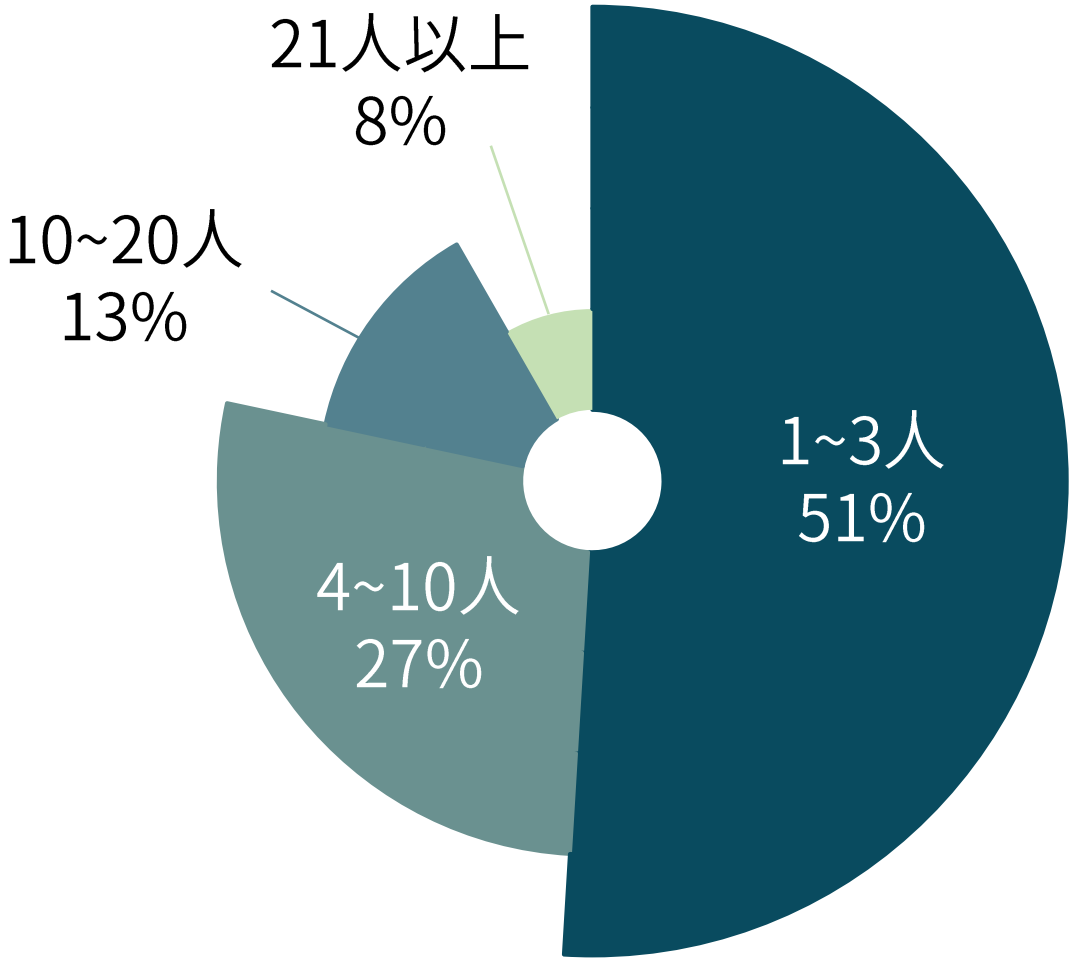


38%

資訊長(CIO)兼任

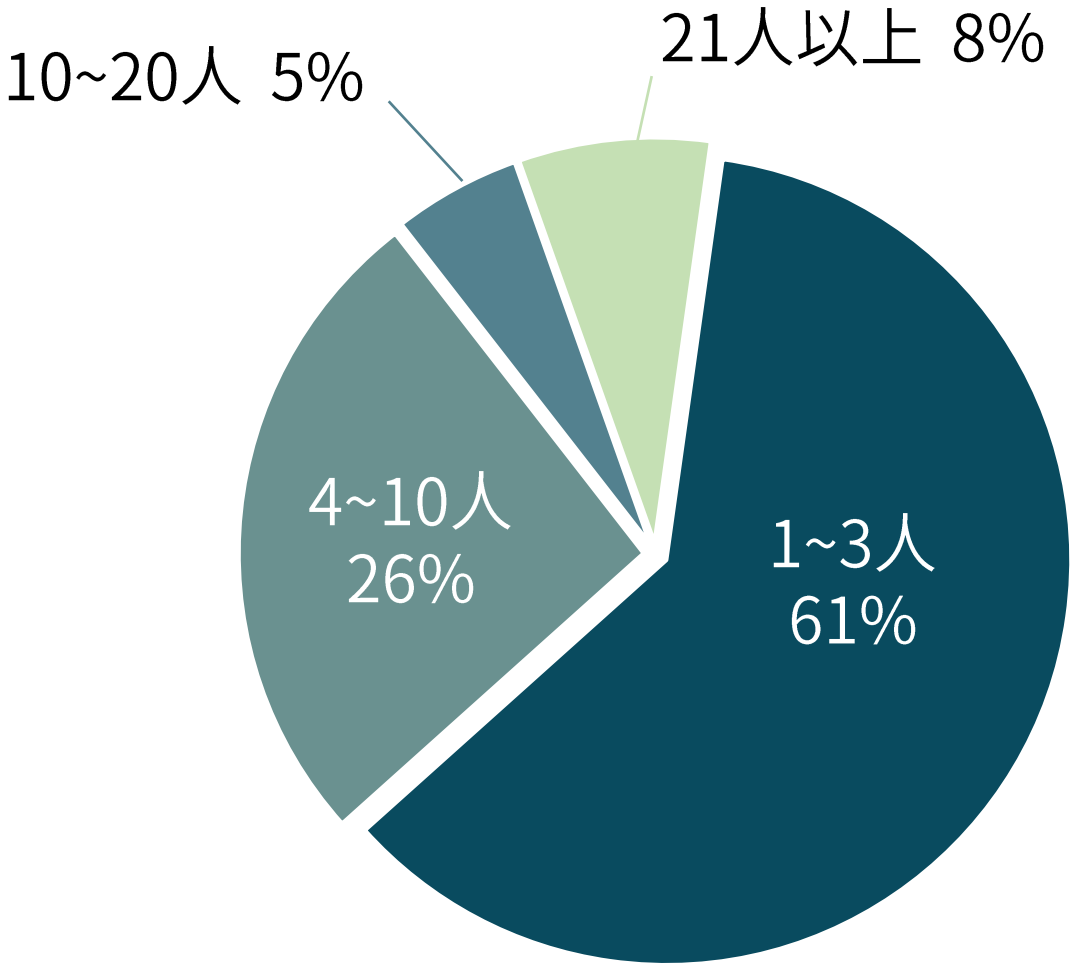


專責的資安團隊人數

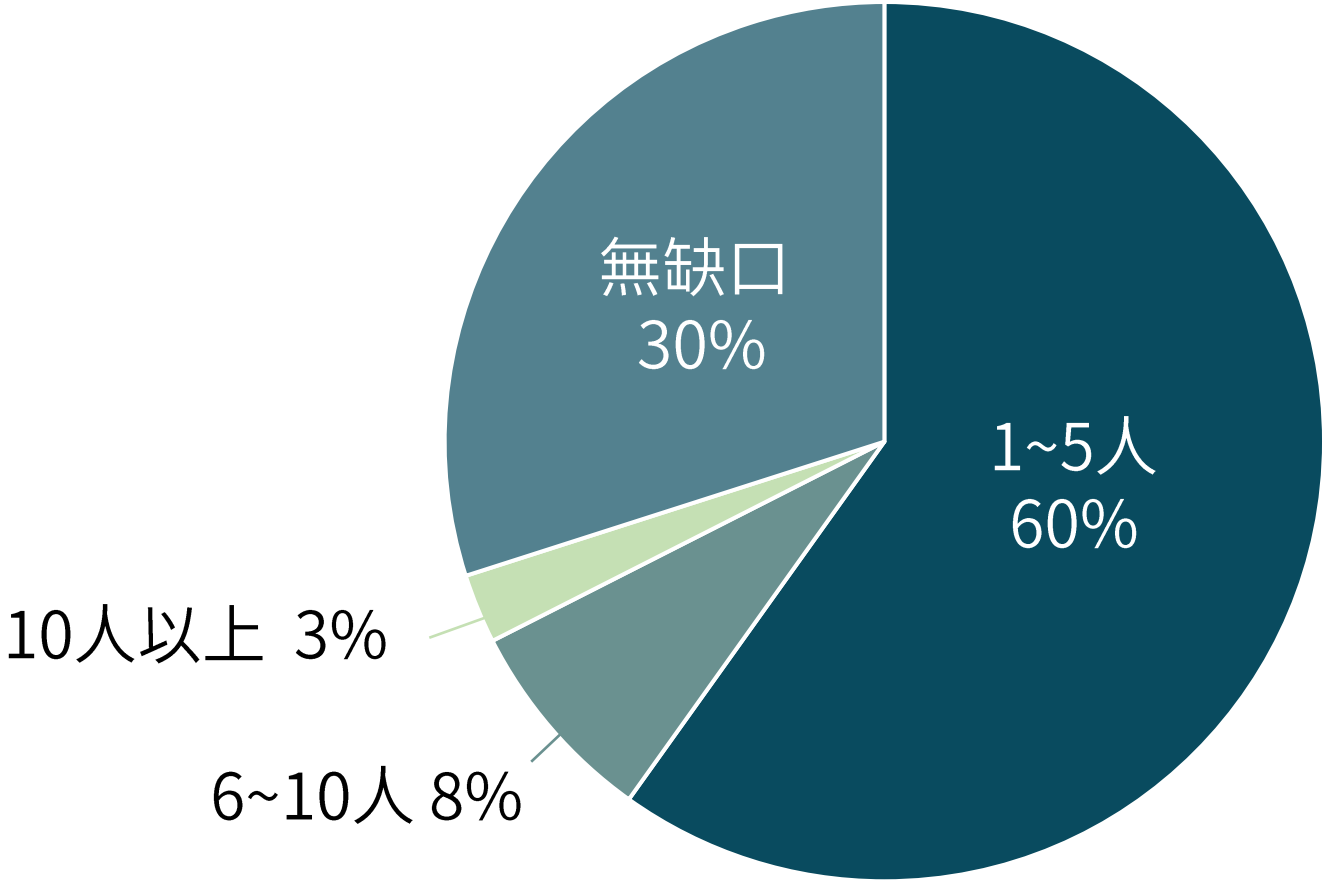


兼職的資安人員人數

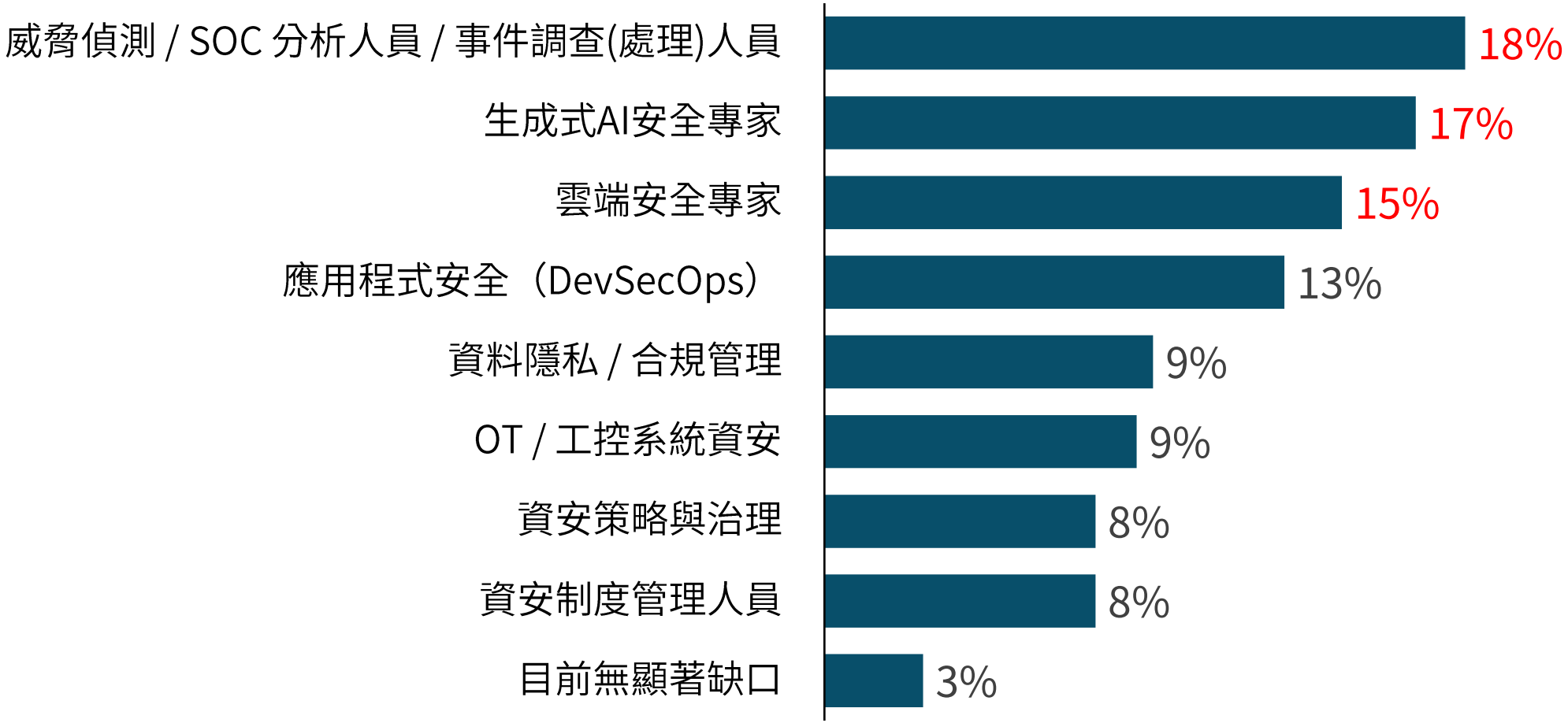
＊兼職代表該員工尚有非資安工作在身



資安人力(含專職與兼職)的編制缺口

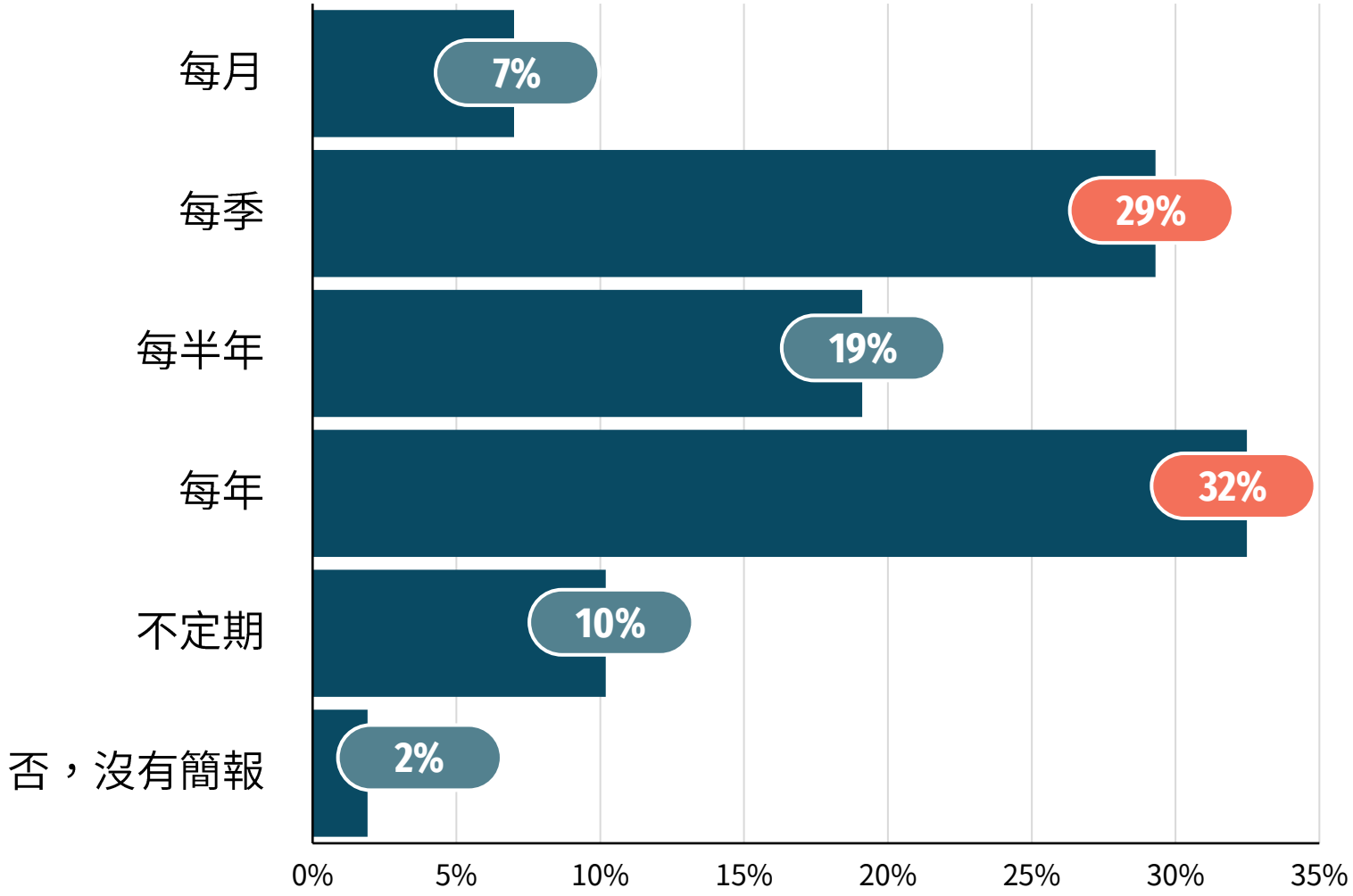


企業資安人才類別缺口

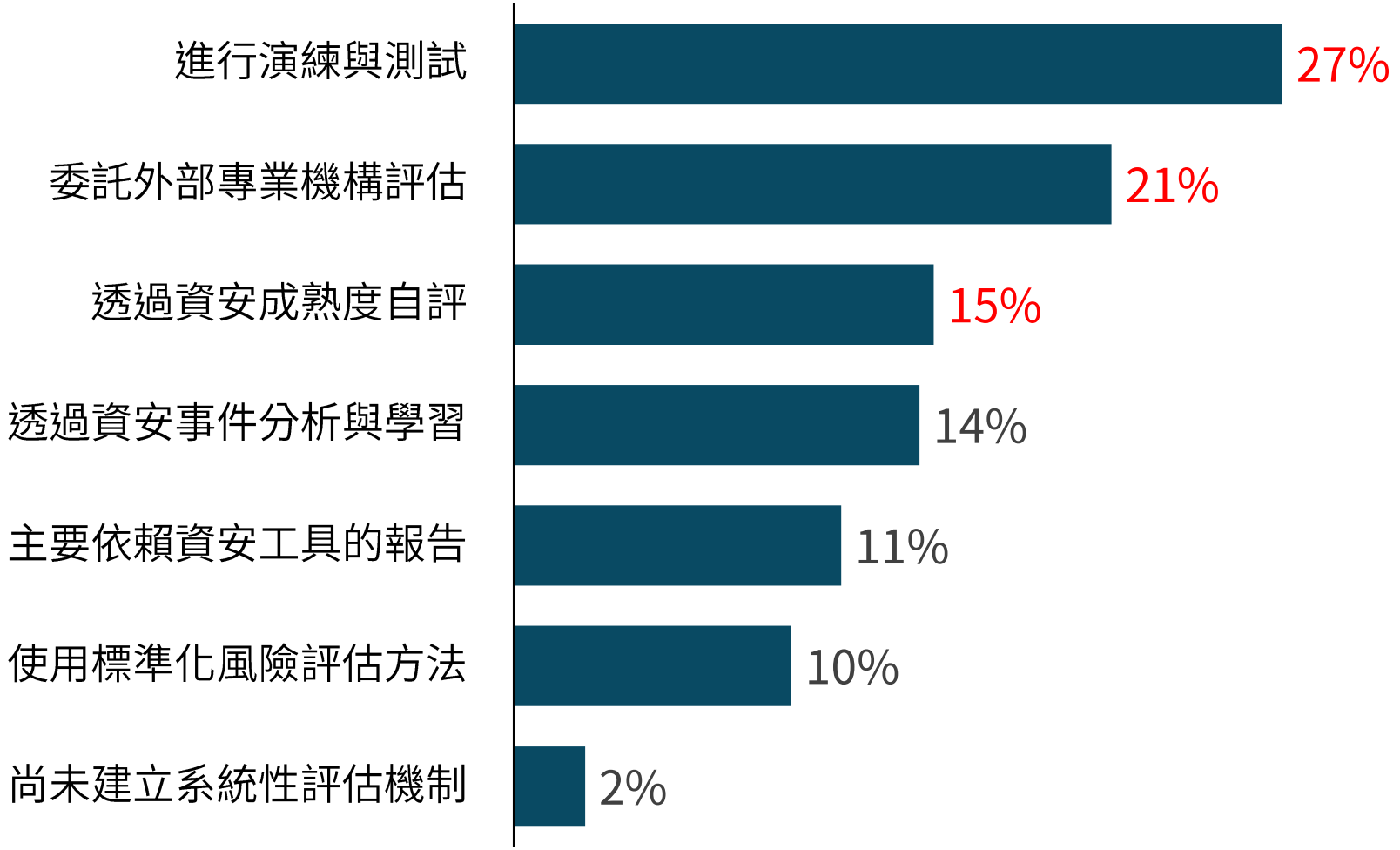

威脅偵測 / SOC 分析人員 / 事件調查(處理)人員
18%
生成式AI安全專家
17%
雲端安全專家
15%
應用程式安全（DevSecOps）
13%
資料隱私 / 合規管理
9%
OT / 工控系統資安
9%
資安策略與治理
8%
資安制度管理人員
8%
目前無顯著缺口
3%


CISO 資安學院
CIO Taiwan
2025
CISO Insight
台灣資安長問卷調查
二、資安治理與策略

是否會向董事會或資安委員會定期進行資安簡報?



您如何進行常態性的整體資安風險評估?



資安防護中最需要補強的破口?

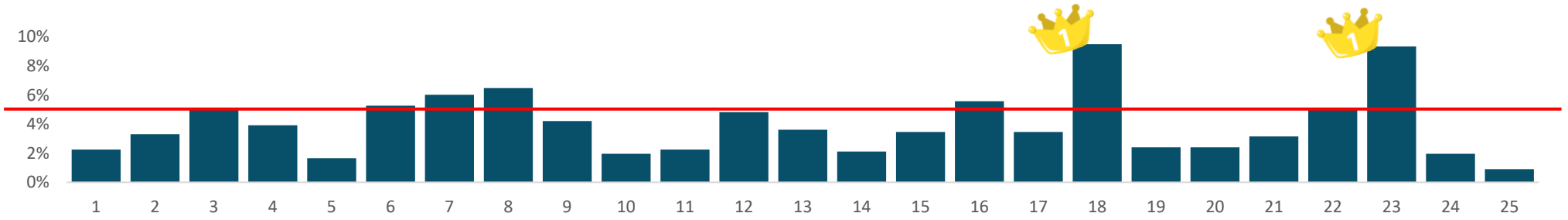


治理 Govern

	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

2024年前5名

2025年前5名



CISO 資安學院 CIO Taiwan

2025年最關注推動的資安治理重點?

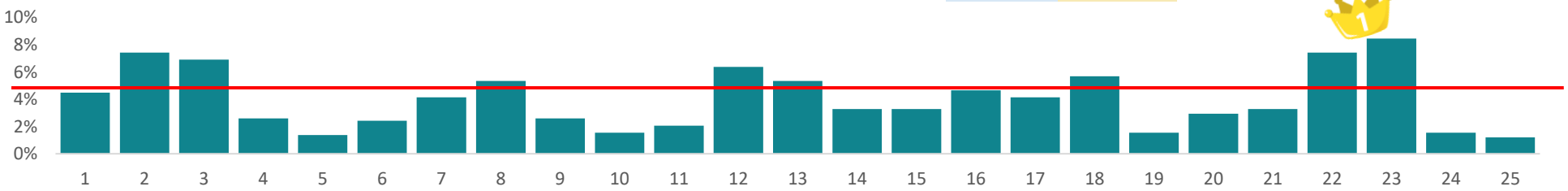


治理 Govern

	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

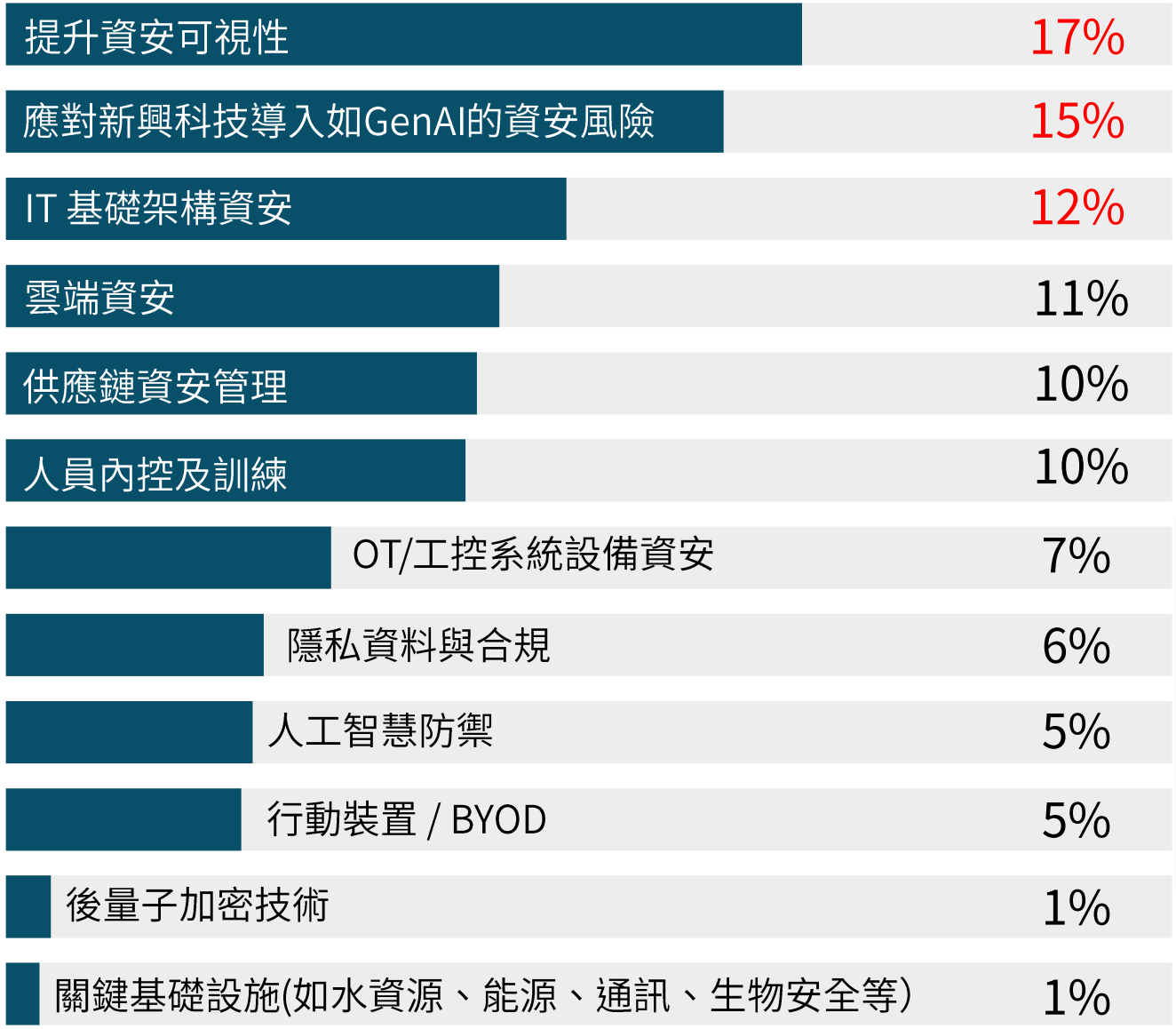
2024年前5名

2025年前5名



CISO 資安學院 CIO Taiwan

另有正在推動或整頓的特別重點項目



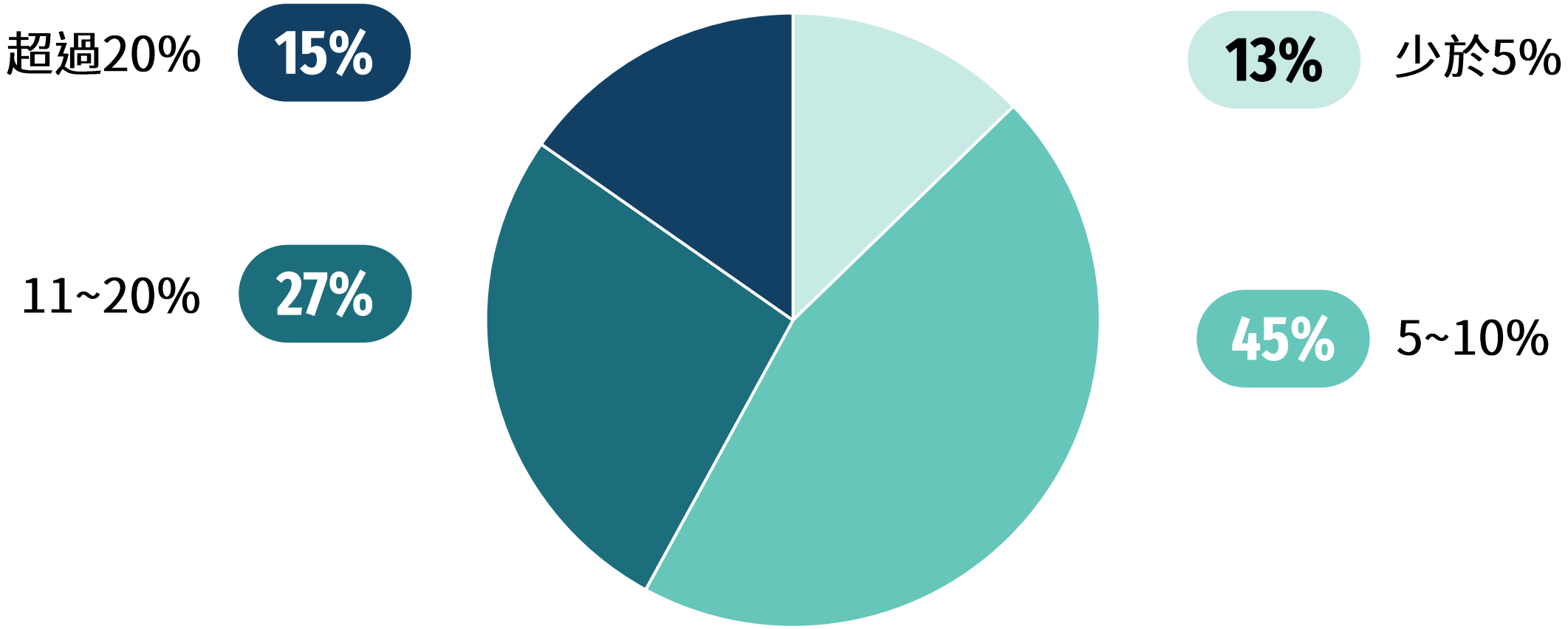
貴公司主事者對資安工作的期許?



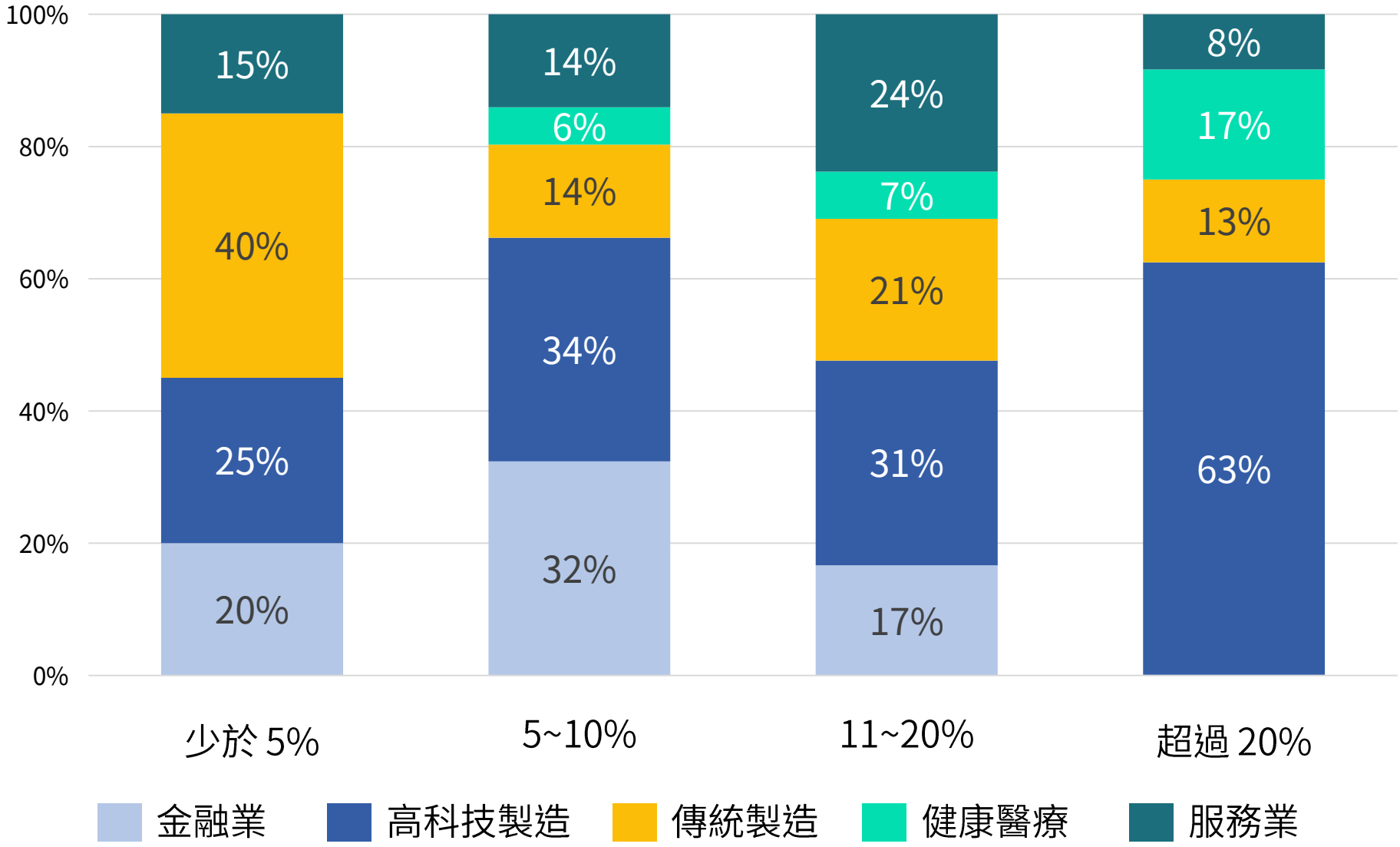
- 46% 符合業務需求及法規就好，不需走太前面
- 43% 做好做滿，成為業界典範
- 9% 既然做再多都有可能出事，那就做好基本防護，出事能儘快恢復就好
- 1% 不清楚長官想法
- 1% 資安是可接受的風險，無須多加著墨


CISO 資安學院
CIO Taiwan
2025
CISO Insight
台灣資安長問卷調查
三、資安預算

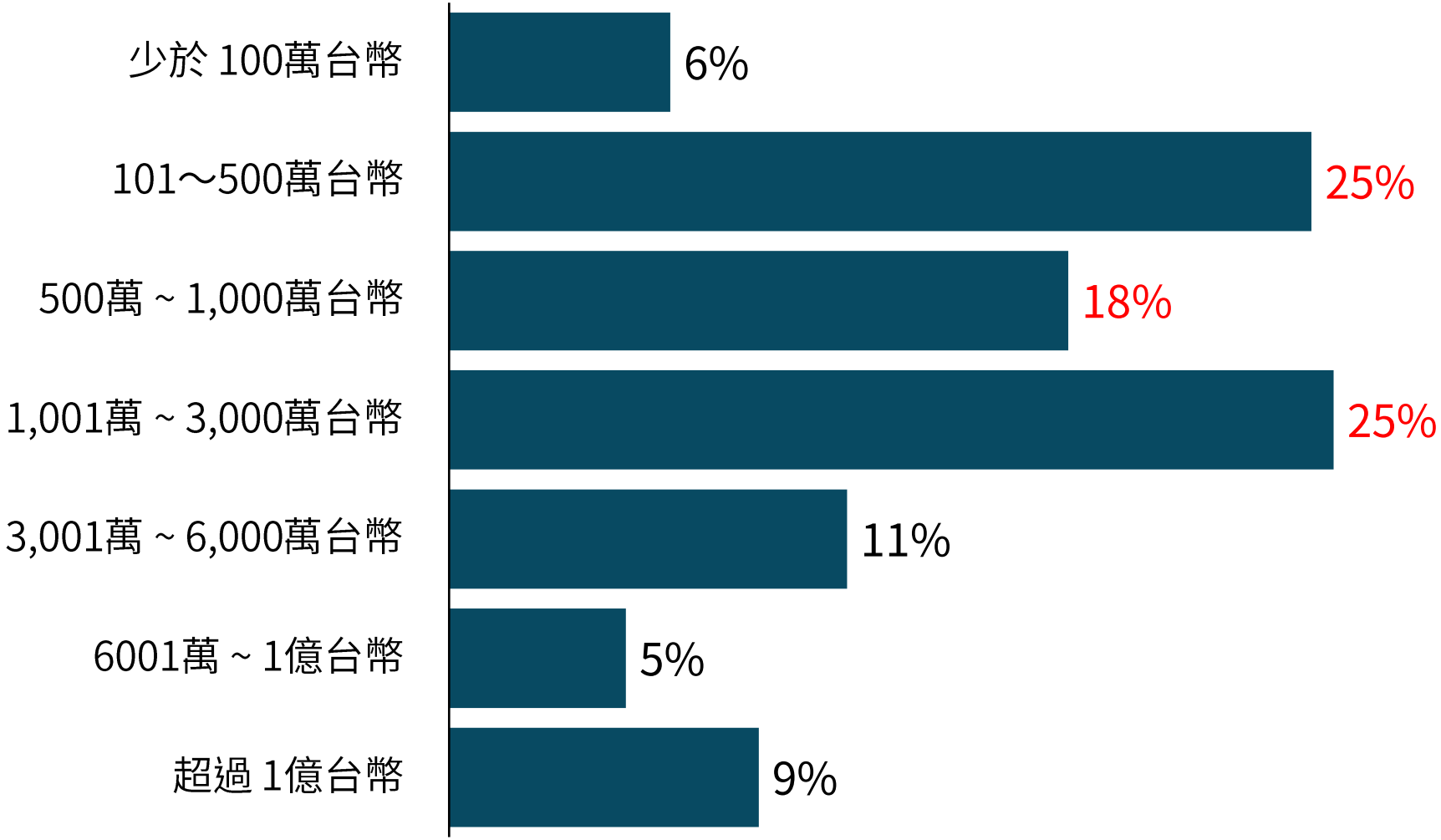
資安年度預算佔 IT 總預算比 - 全產業



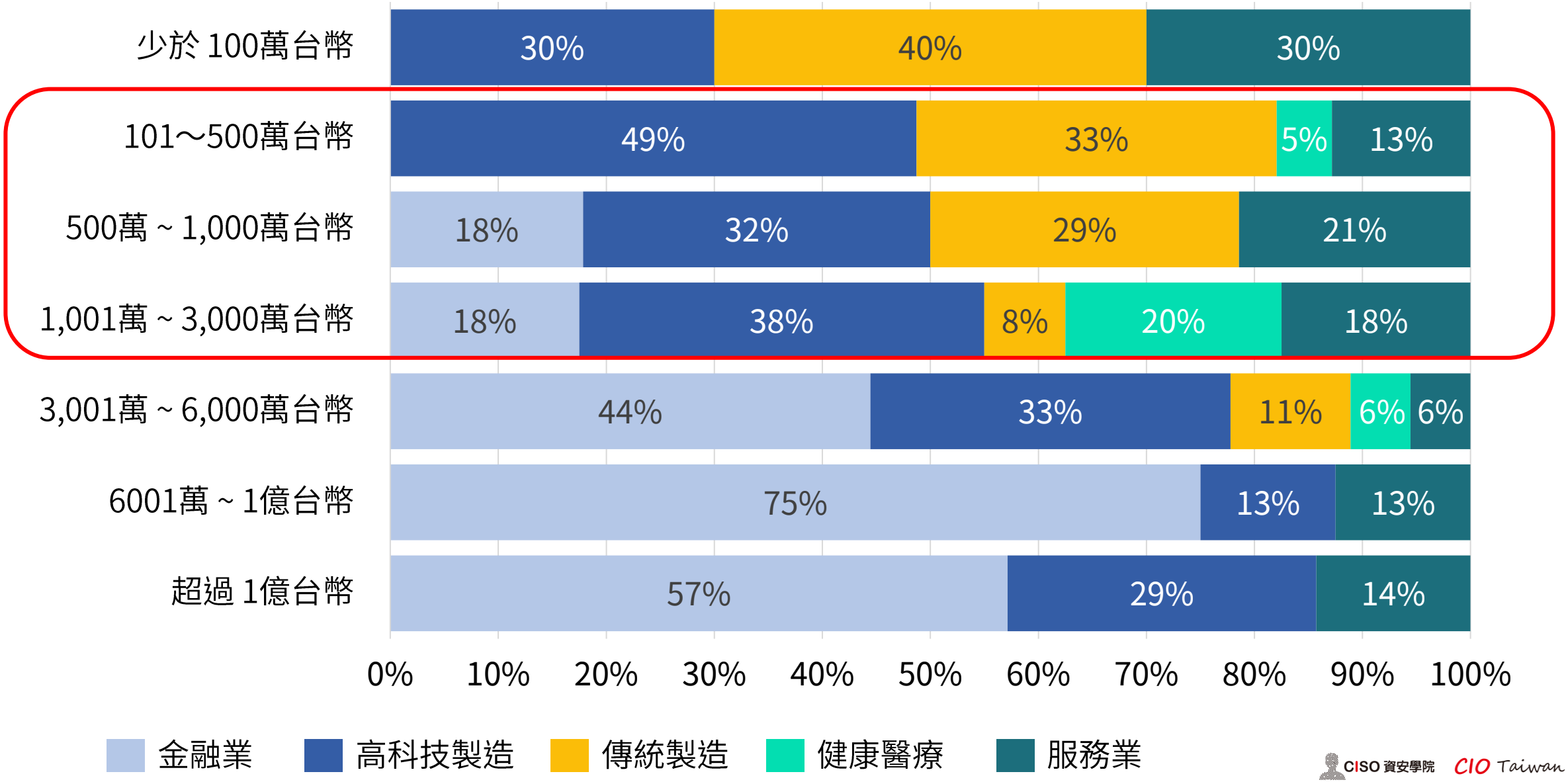
資安年度預算佔 IT 總預算比 - 各產業



2025年資安總預算 – 全產業

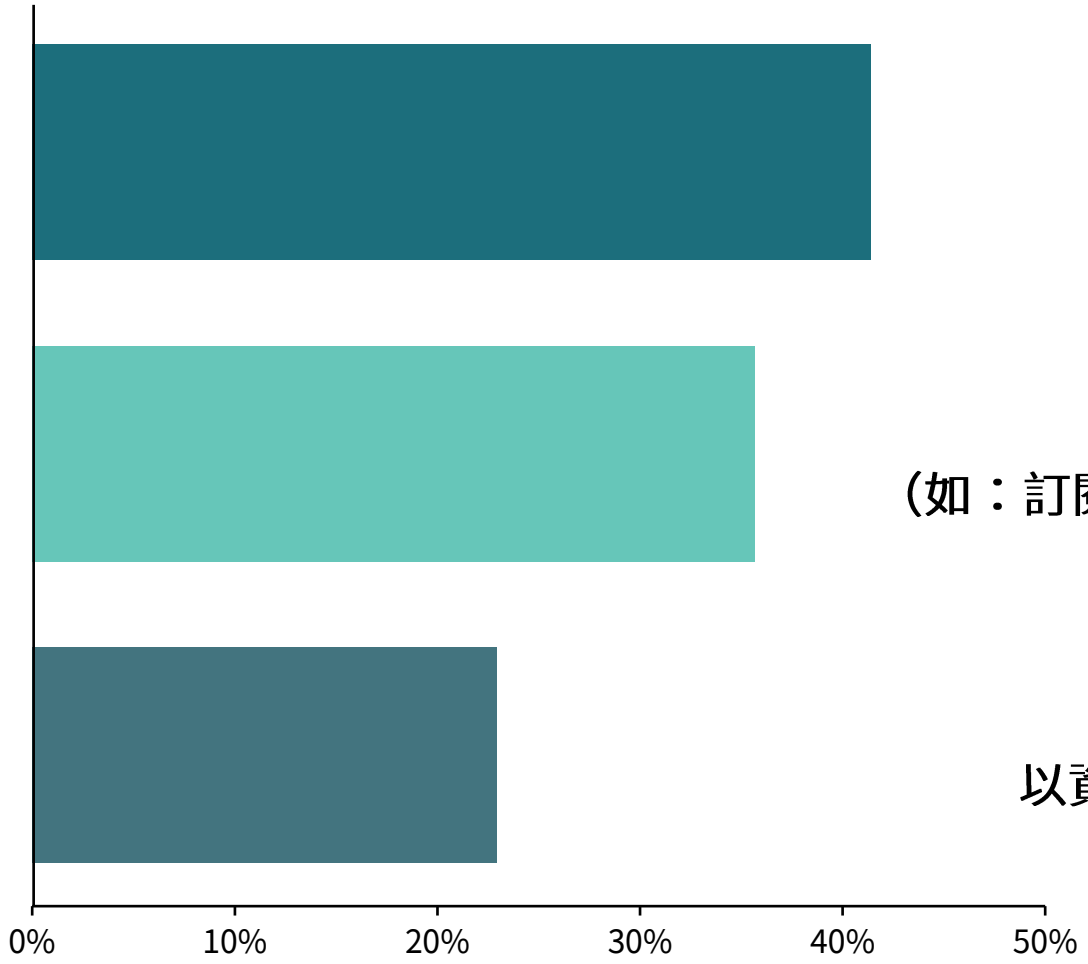


2025年資安總預算 - 各產業



CISO 資安學院 CIO Taiwan

企業資安預算的支出類型佔比



41%

資本支出與營運支出約各半

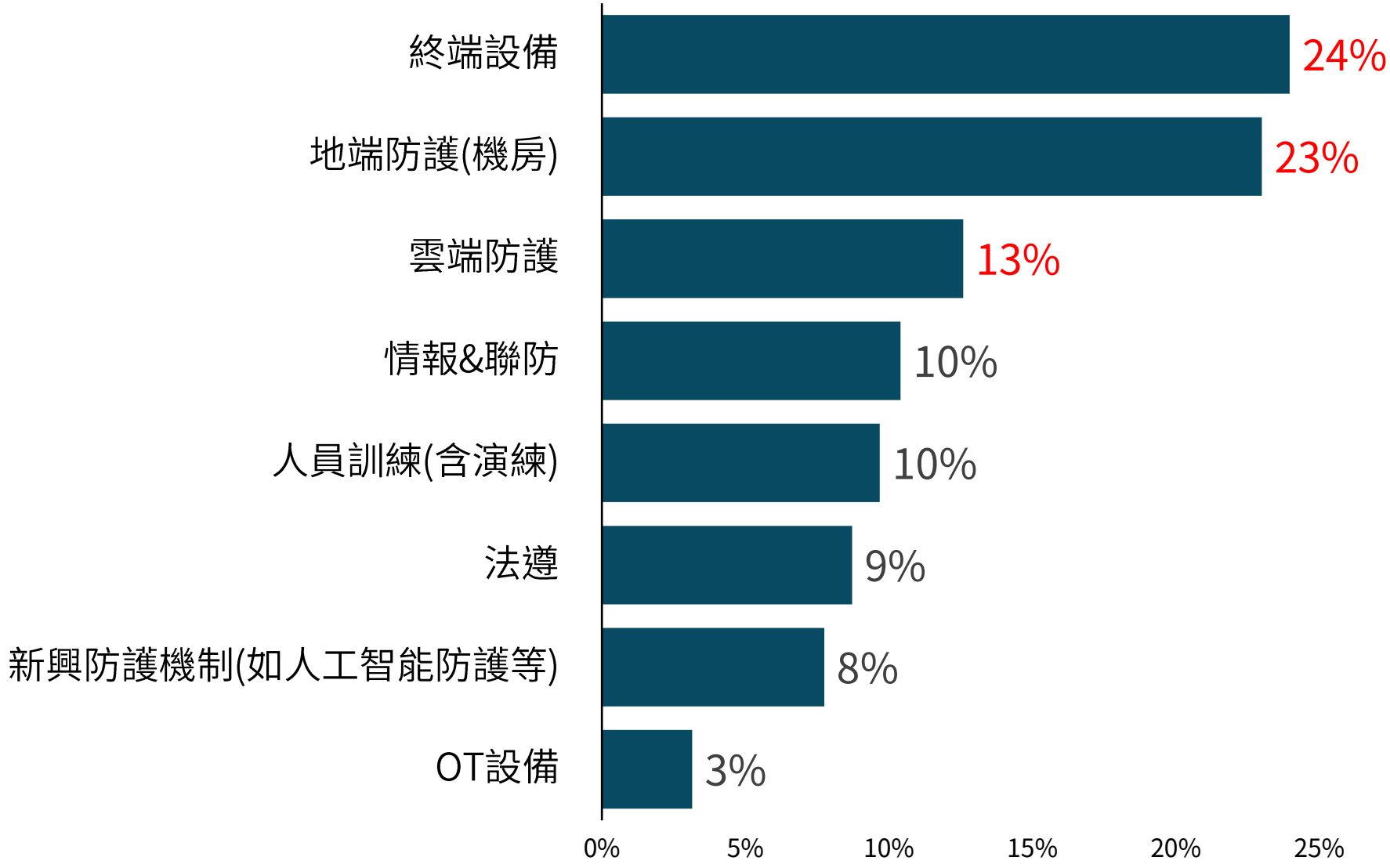
36%

以營運支出為主
（如：訂閱制服務、託管服務、顧問費用）

23%

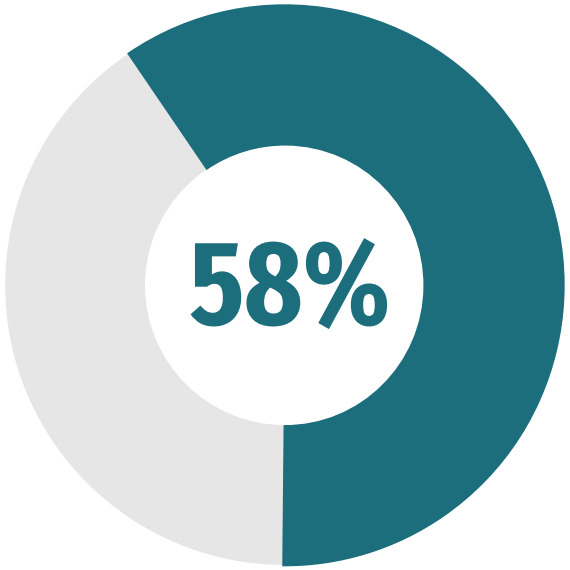
以資本支出為主（如：軟硬體採購）

資安預算的主要投資項目

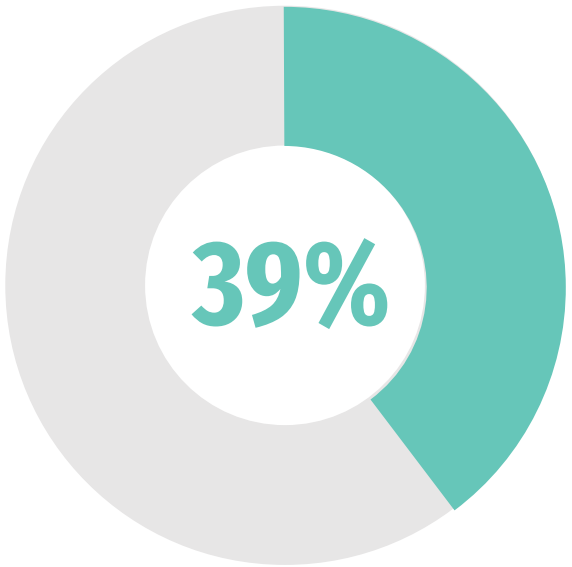


2026年資安預算是否會有變動?

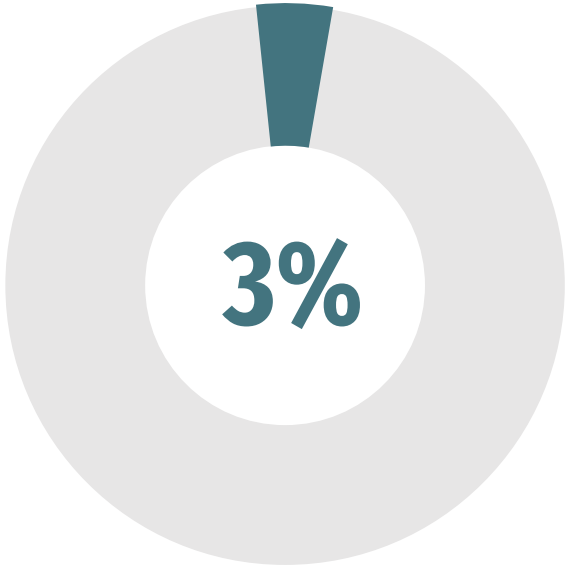
會增加



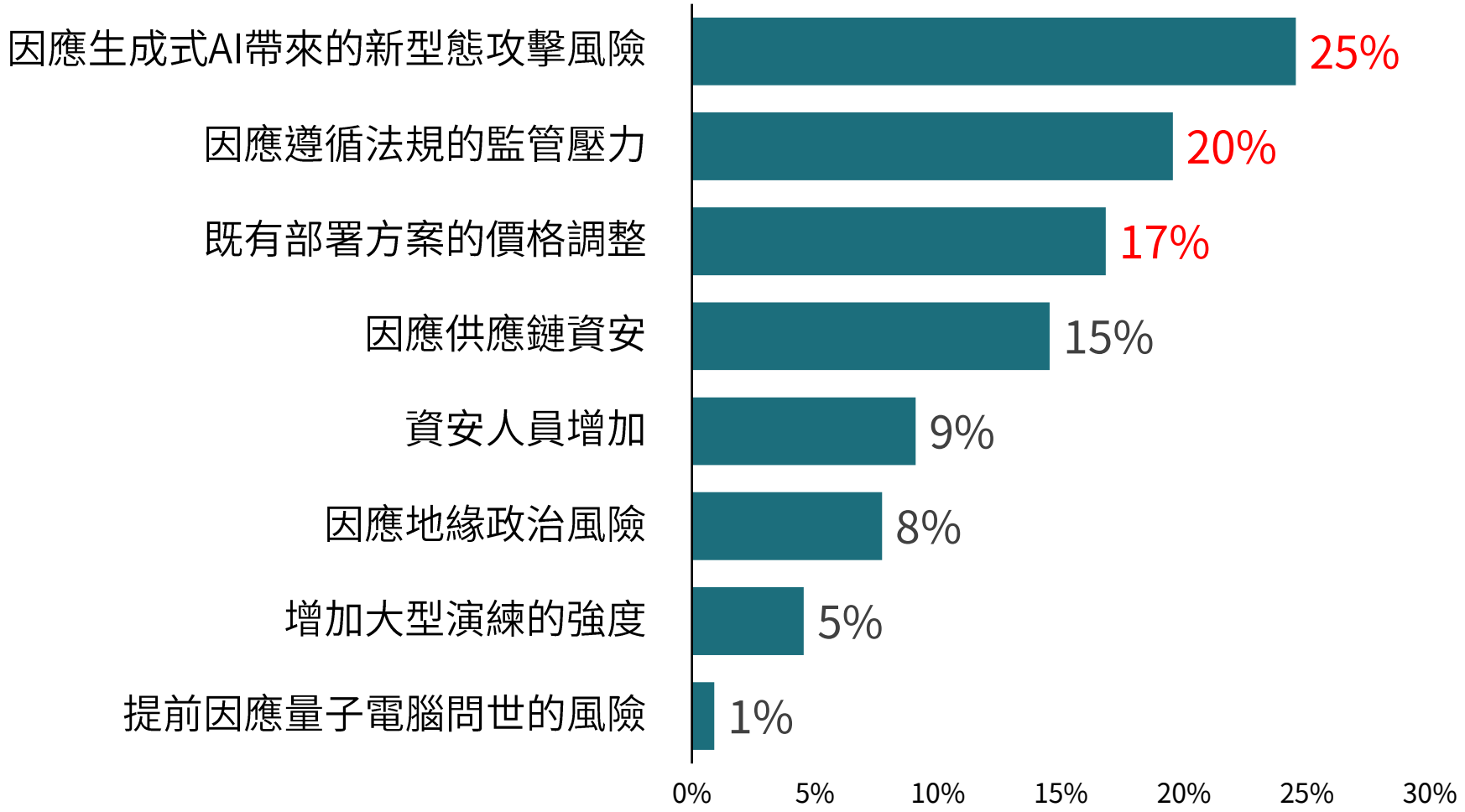
持平不變



會減少

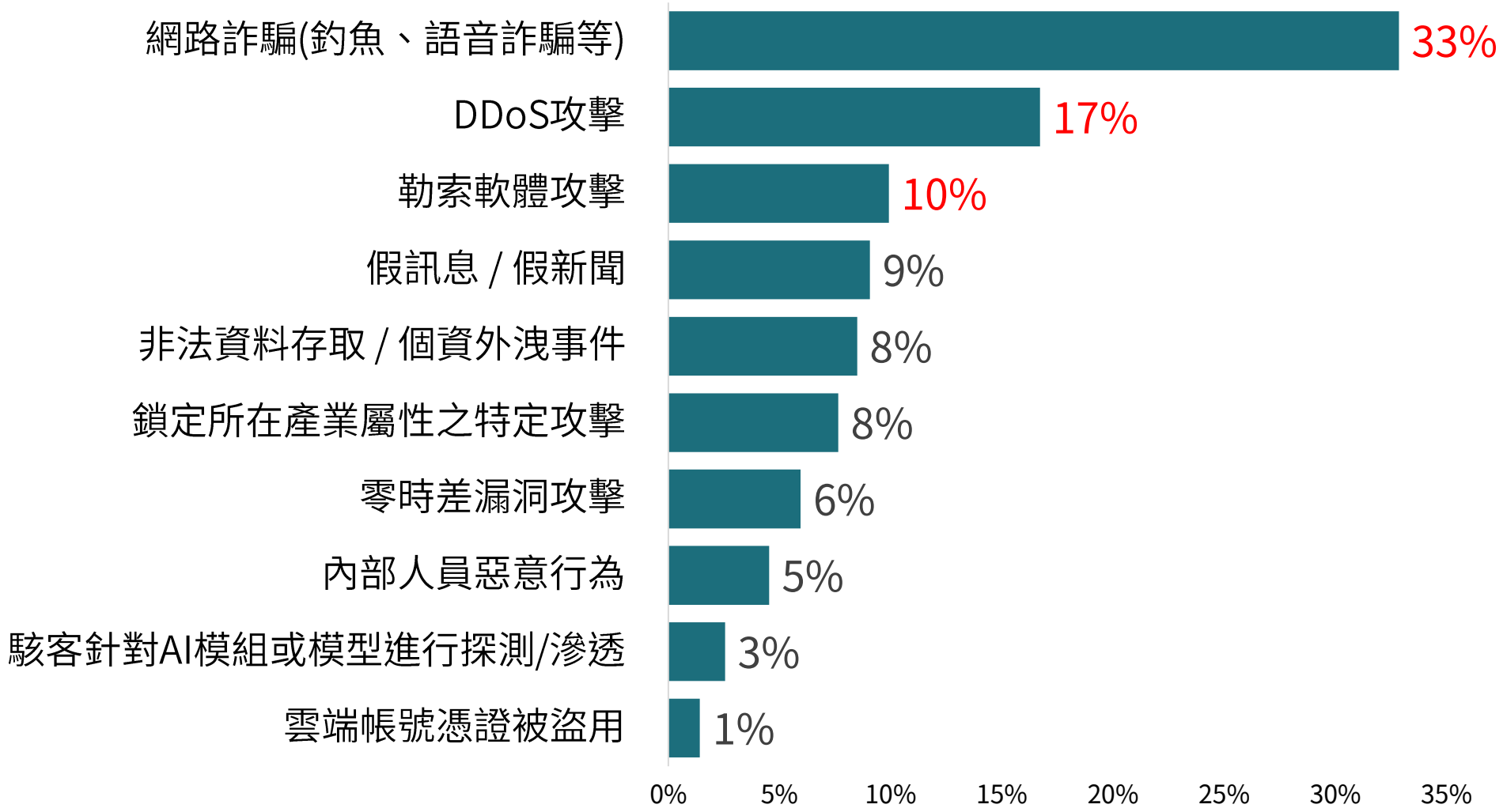


資安預算增加的主要原因




CISO 資安學院
CIO Taiwan
2025
CISO Insight
台灣資安長問卷調查
四、威脅情勢與資安韌性

在過去一年中最常遭受的資安威脅



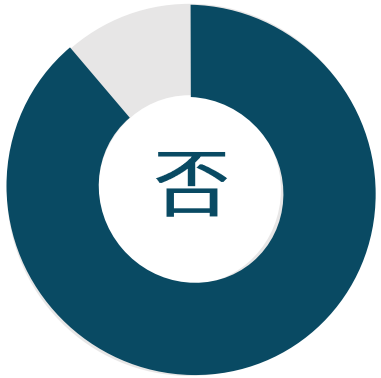
過去一年是否有發生需通報的資安事件?



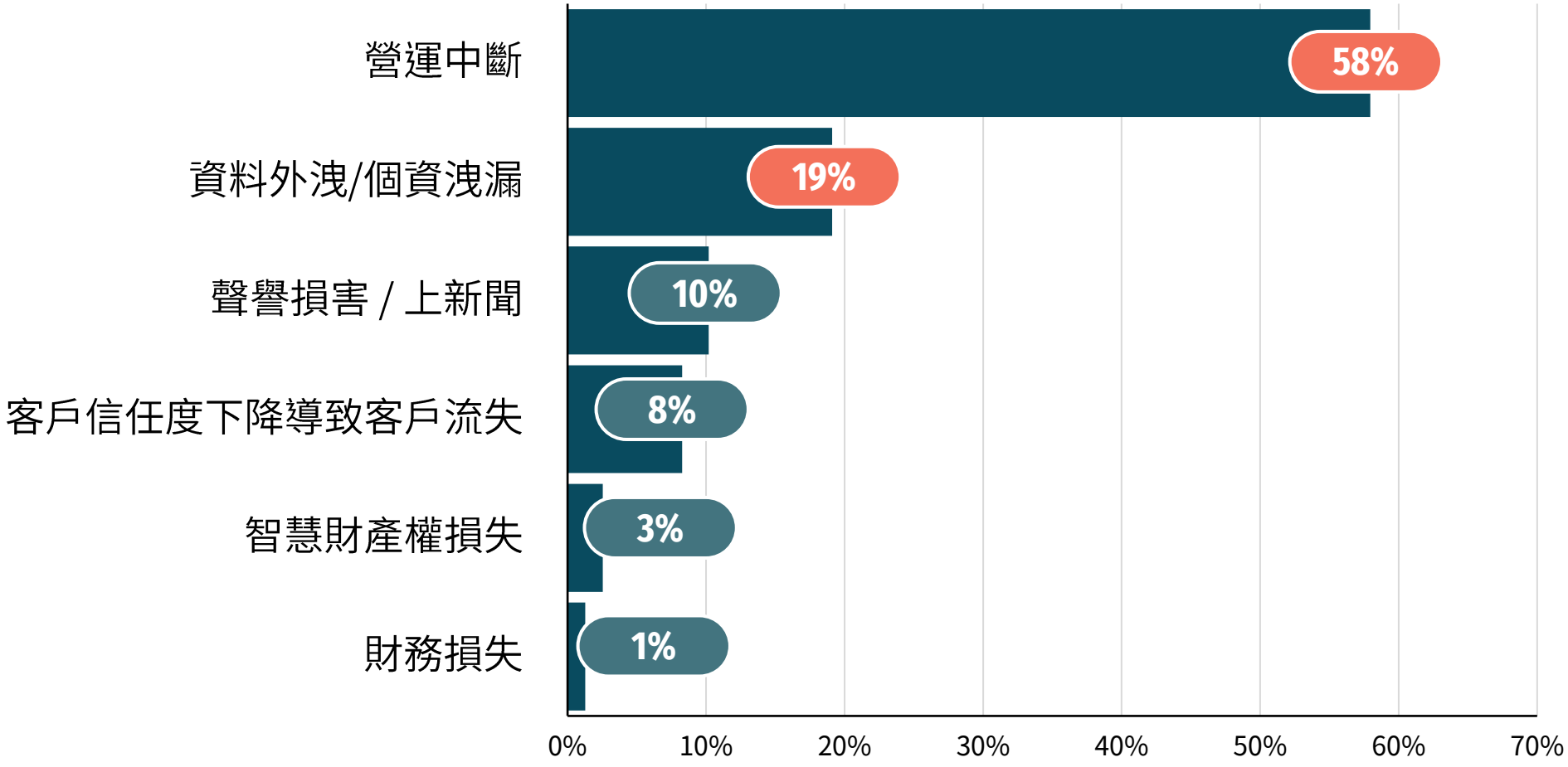


11%

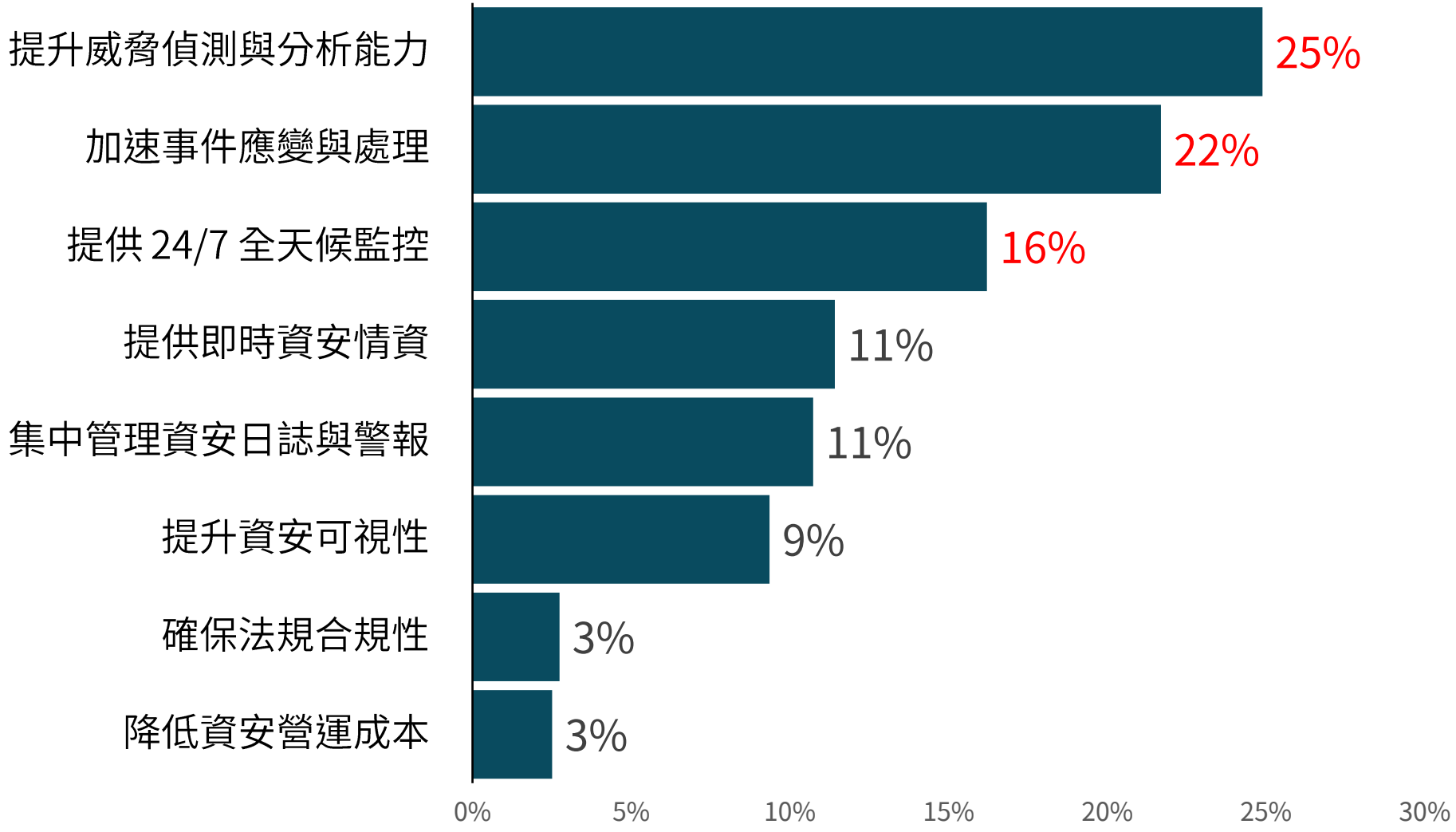
89%



哪種資安攻擊會對企業造成的影響最大?



資安營運中心(SOC)在資安防禦上貢獻度較高的功能



在面對資安事件或疑慮時，內部是否有通報及支援機制?

01 45% 有特定人員協助員工回報資安疑慮或事件

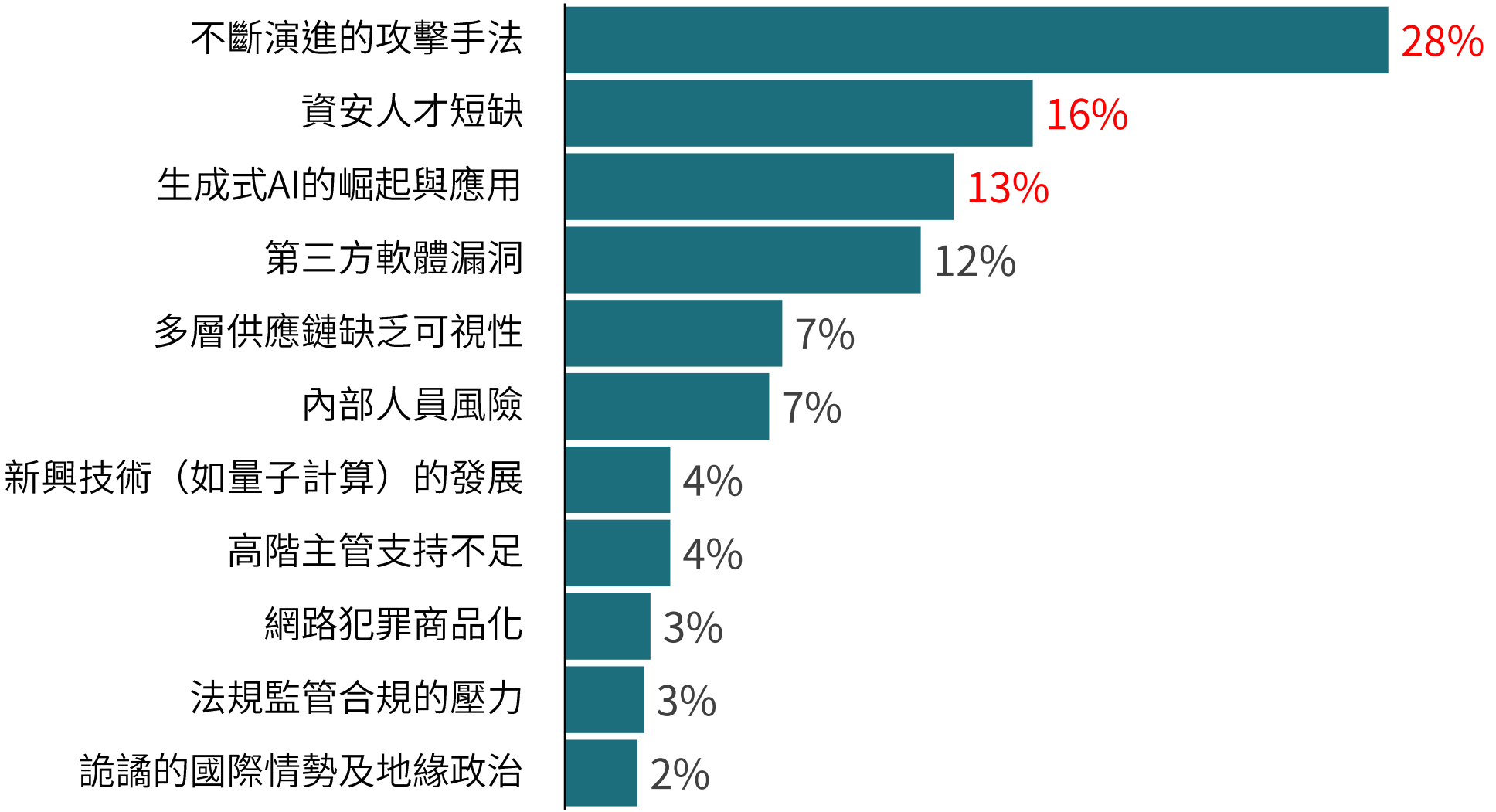
02 35% 設有支援團隊處理資安事件

03 16% 提供外部資安服務協助

04 2% 無特定通報管道

05 2% 設立匿名通報管道

當前資安韌性的最大挑戰



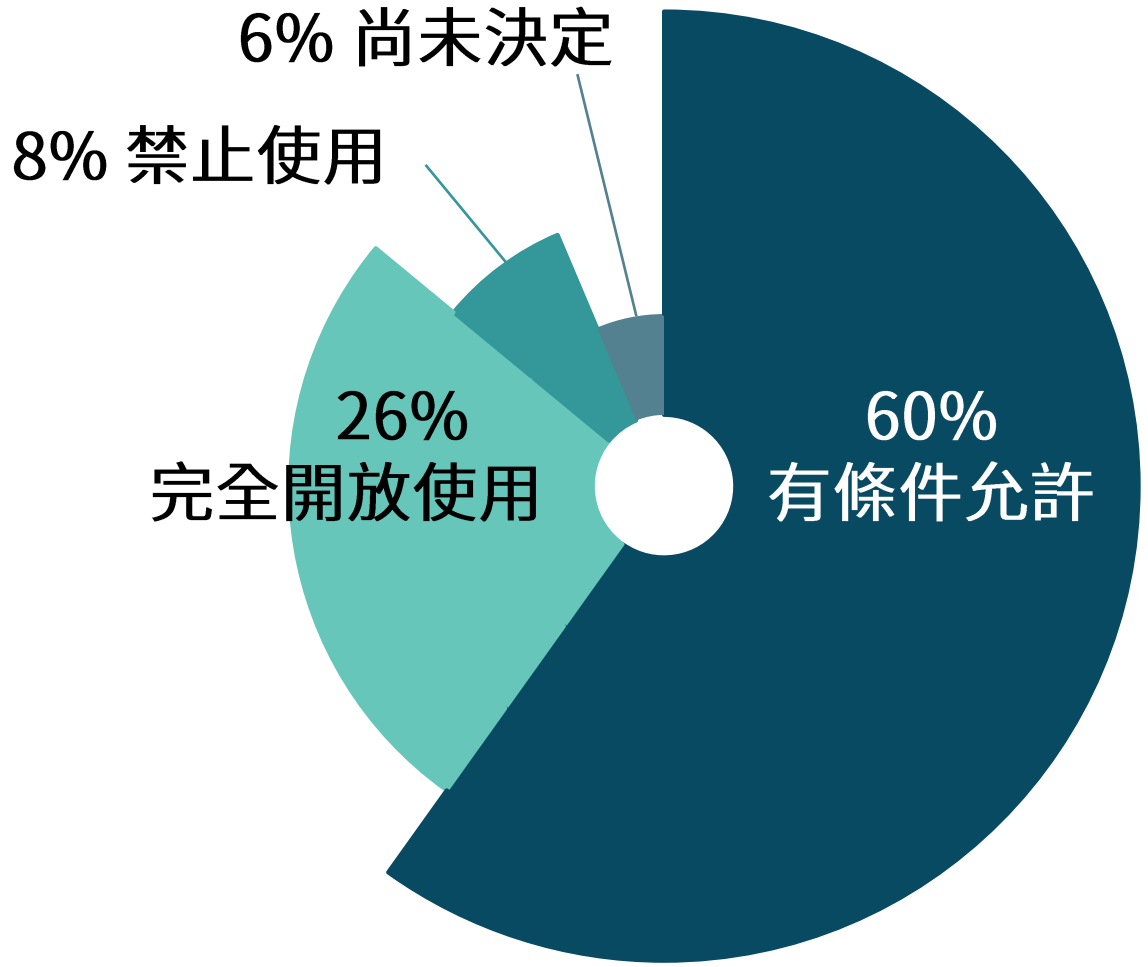
您對所屬企業的資安韌性信心度

22%	48%	28%	2%
非常有信心	有信心	一般	較沒信心

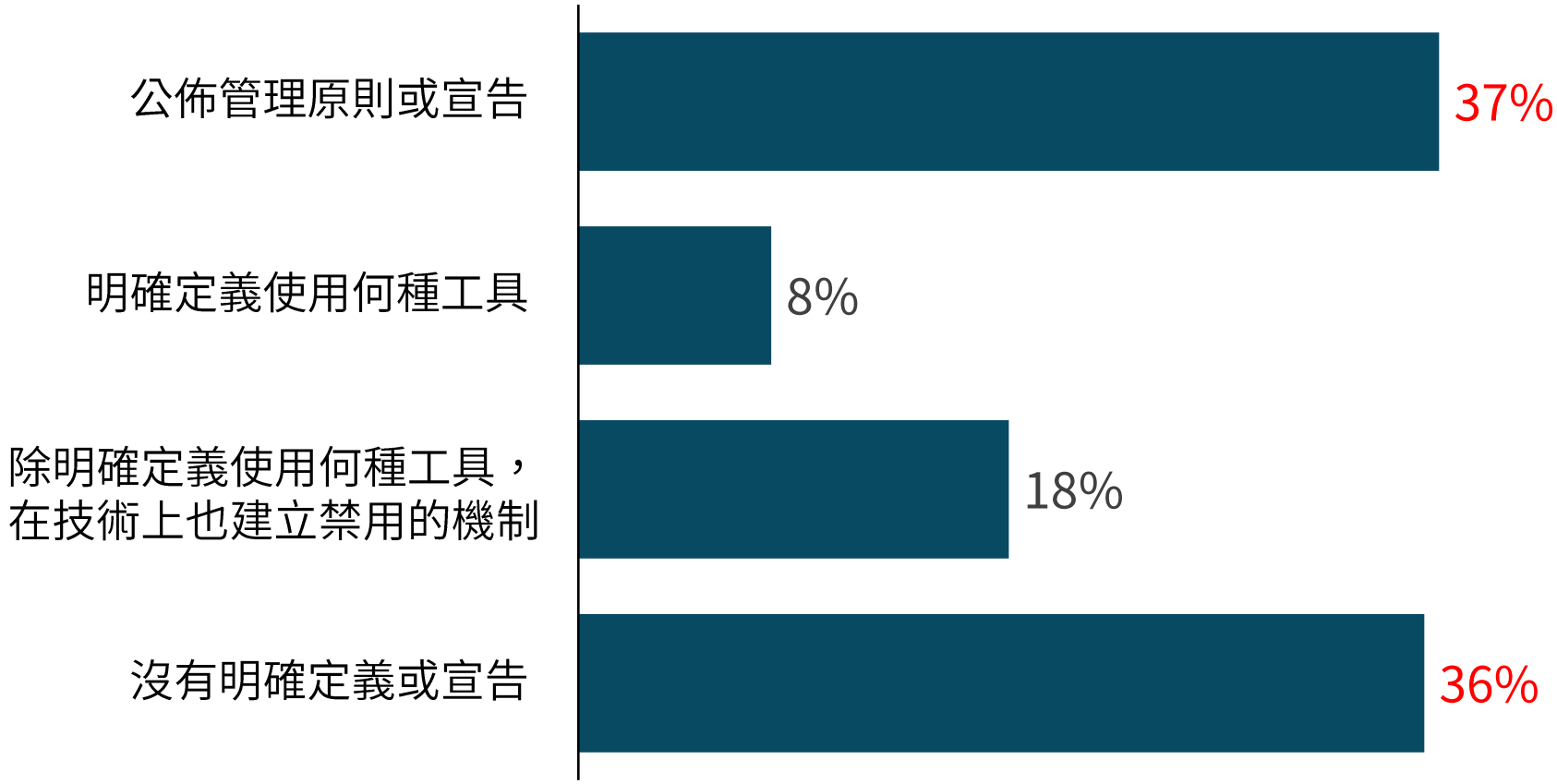



CISO 資安學院
CIO Taiwan
2025
CISO Insight
台灣資安長問卷調查
五、生成式AI的資安影響

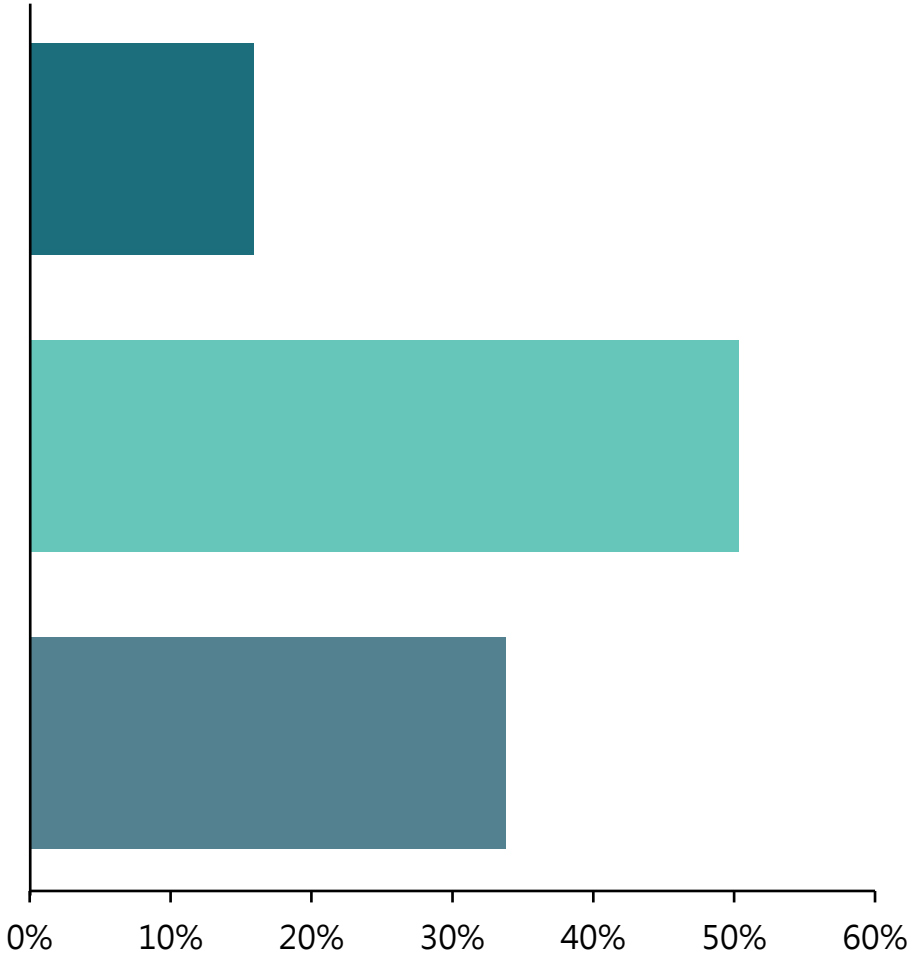
企業是否允許員工使用生成式AI工具?



是否有明確的生成式AI管理機制?



是否有生成式 AI 的資安風險評估機制?



16%

有完整框架(含風險分類與回應流程)，
且在部署AI工具前會進行資安評估

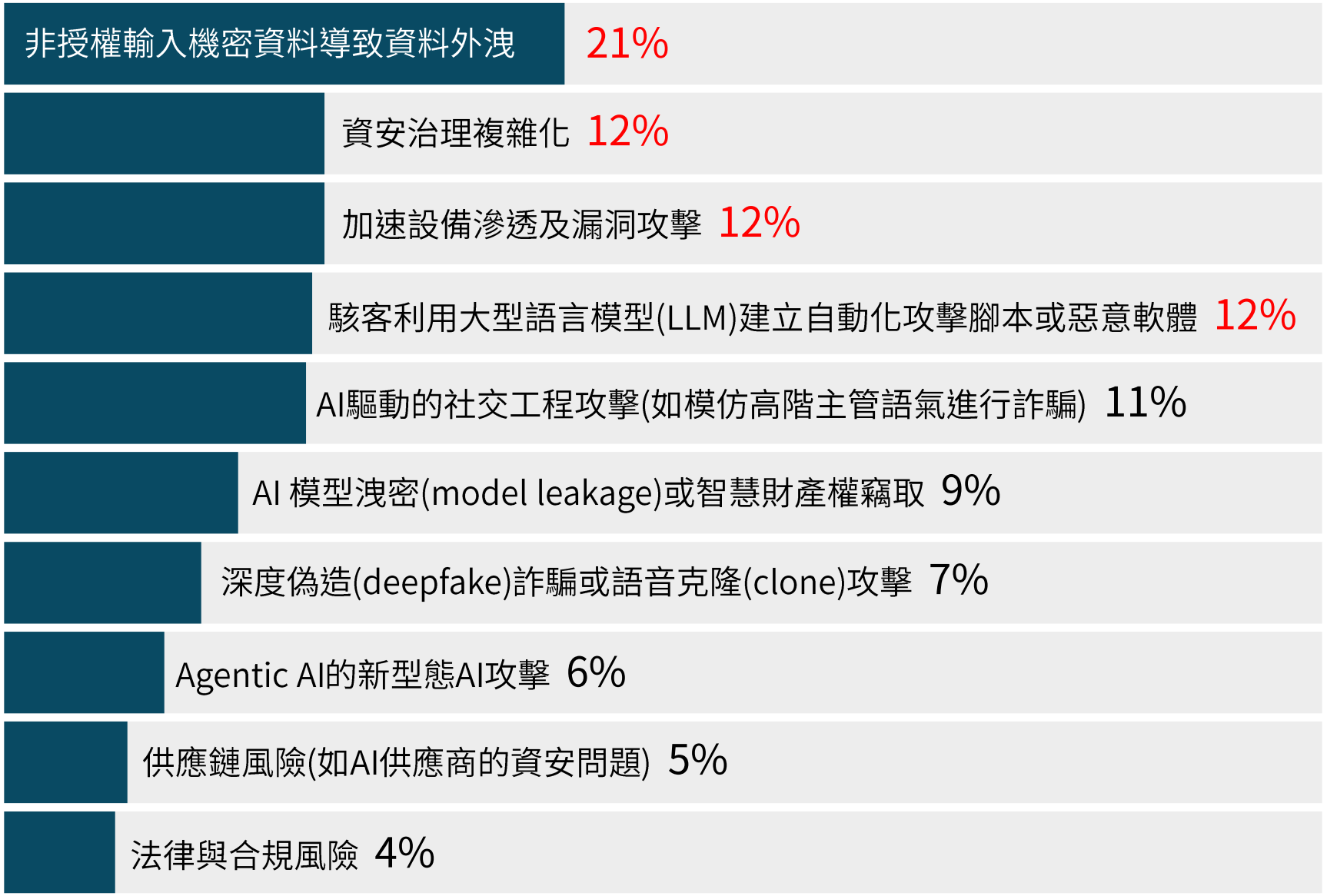
50%

有基本流程但不具一致性，
或僅在部分情況下進行評估

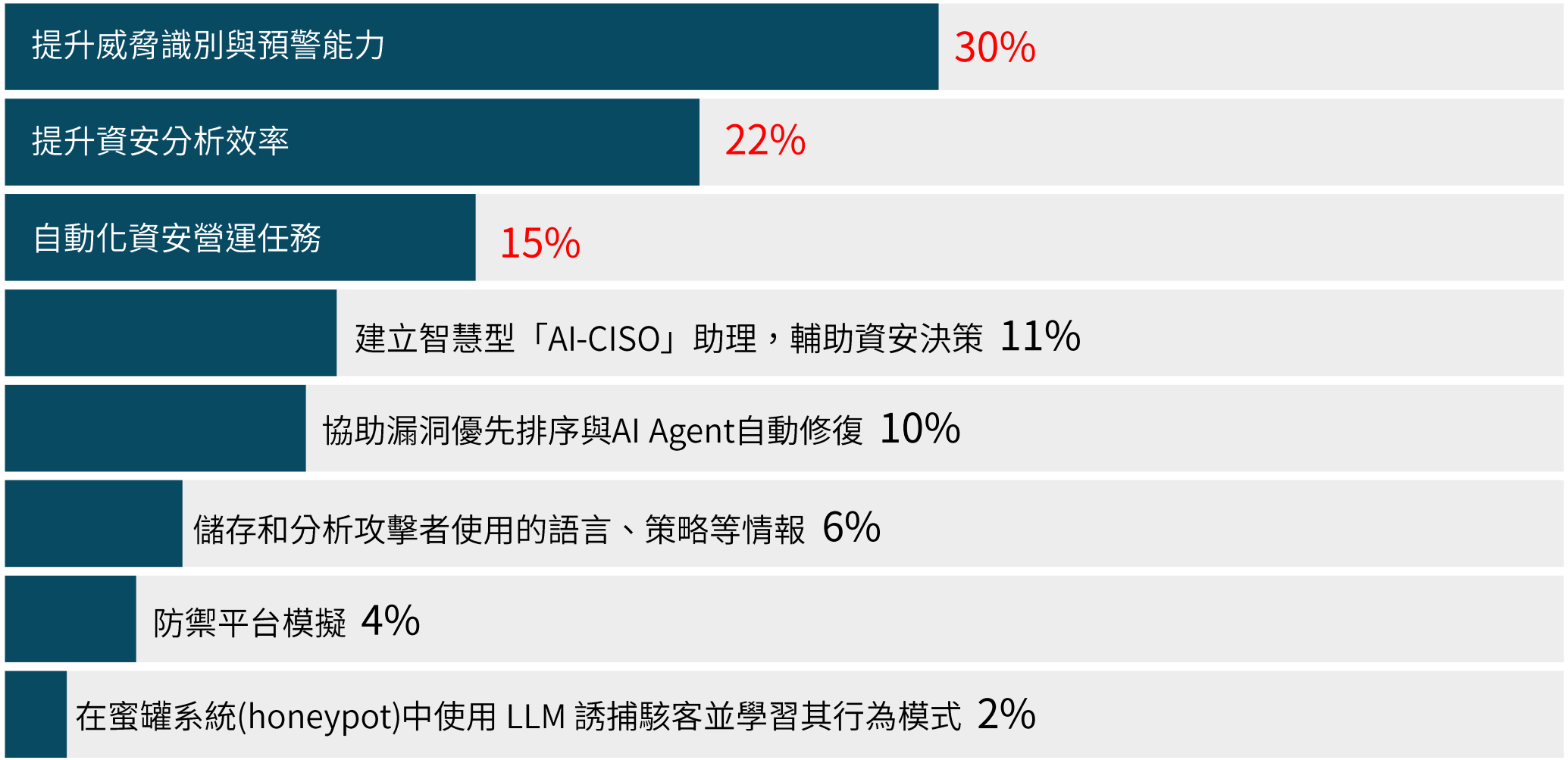
34%

尚未建立，或部署AI工具前不進行資安評估

最關注的生成式AI資安風險類型

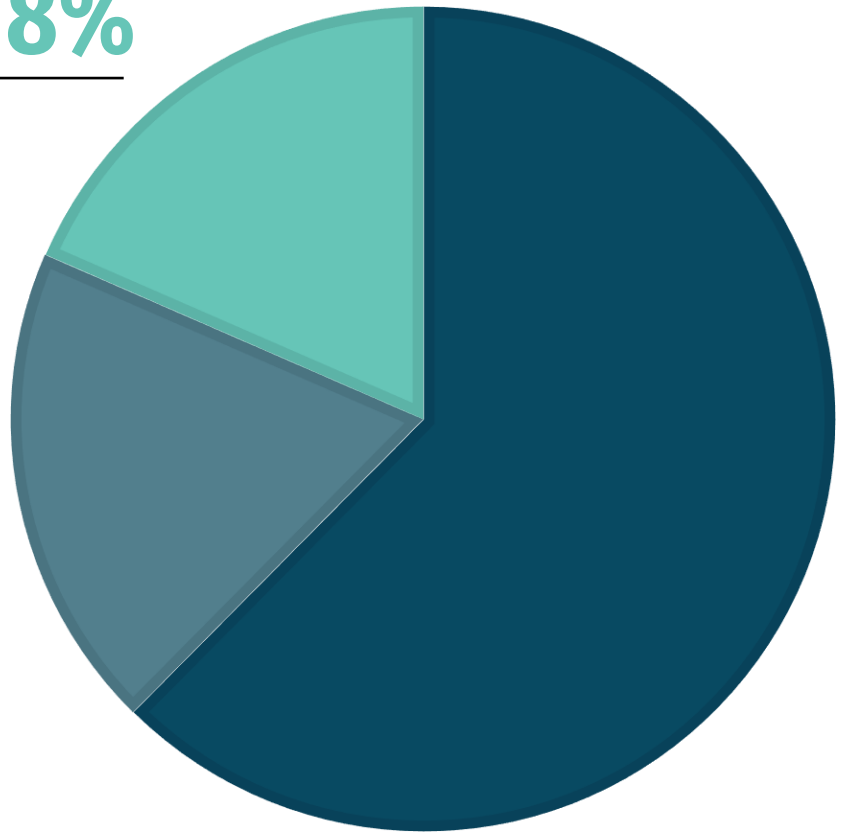


生成式 AI 能為企業資安防禦帶來的機會

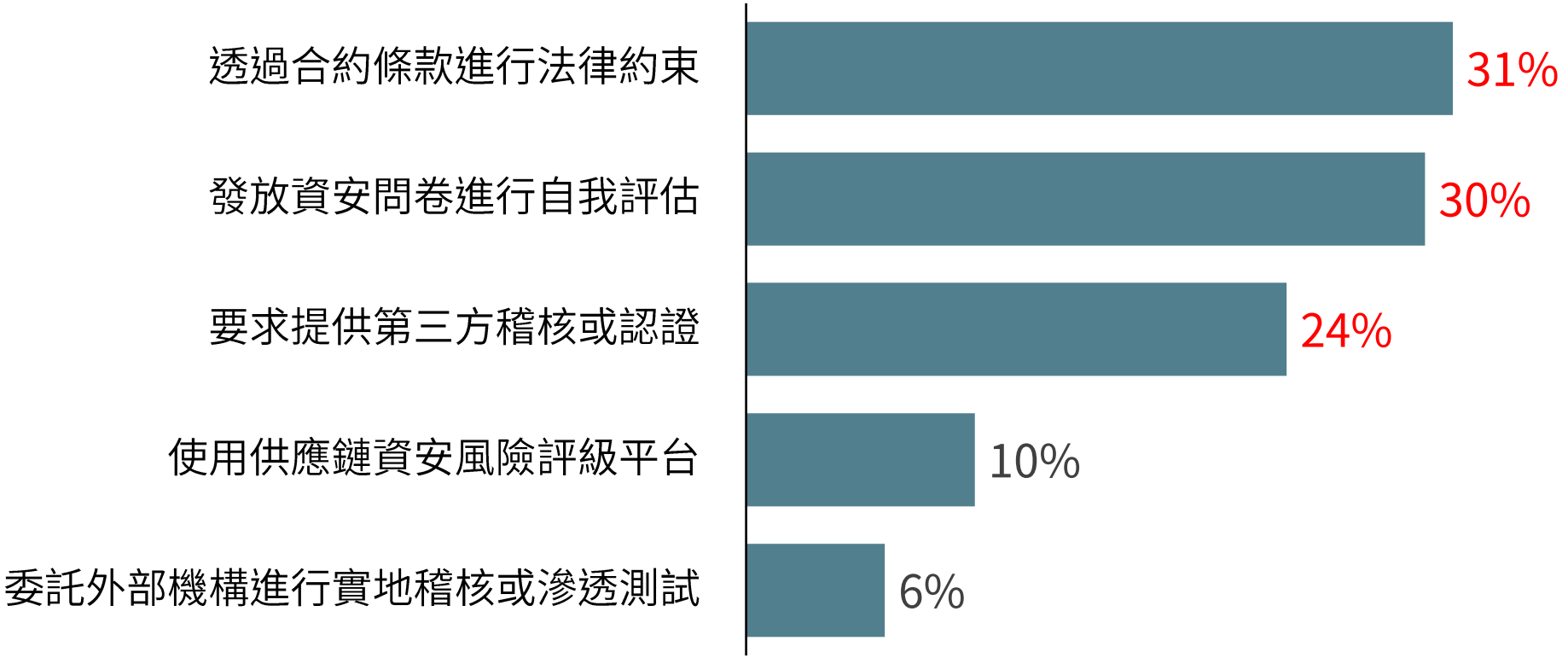



CISO 資安學院
CIO Taiwan
2025
CISO Insight
台灣資安長問卷調查
六、供應鏈資安

是否有針對供應鏈夥伴實施資安審查?



執行供應鏈資安審查的主要方式



供應鏈資安難以落實的關鍵原因



01
33%
供應商的大小不一，
很難適用同一種資安標準

02
20%
難以確認供應商
是否有確實遵守要求

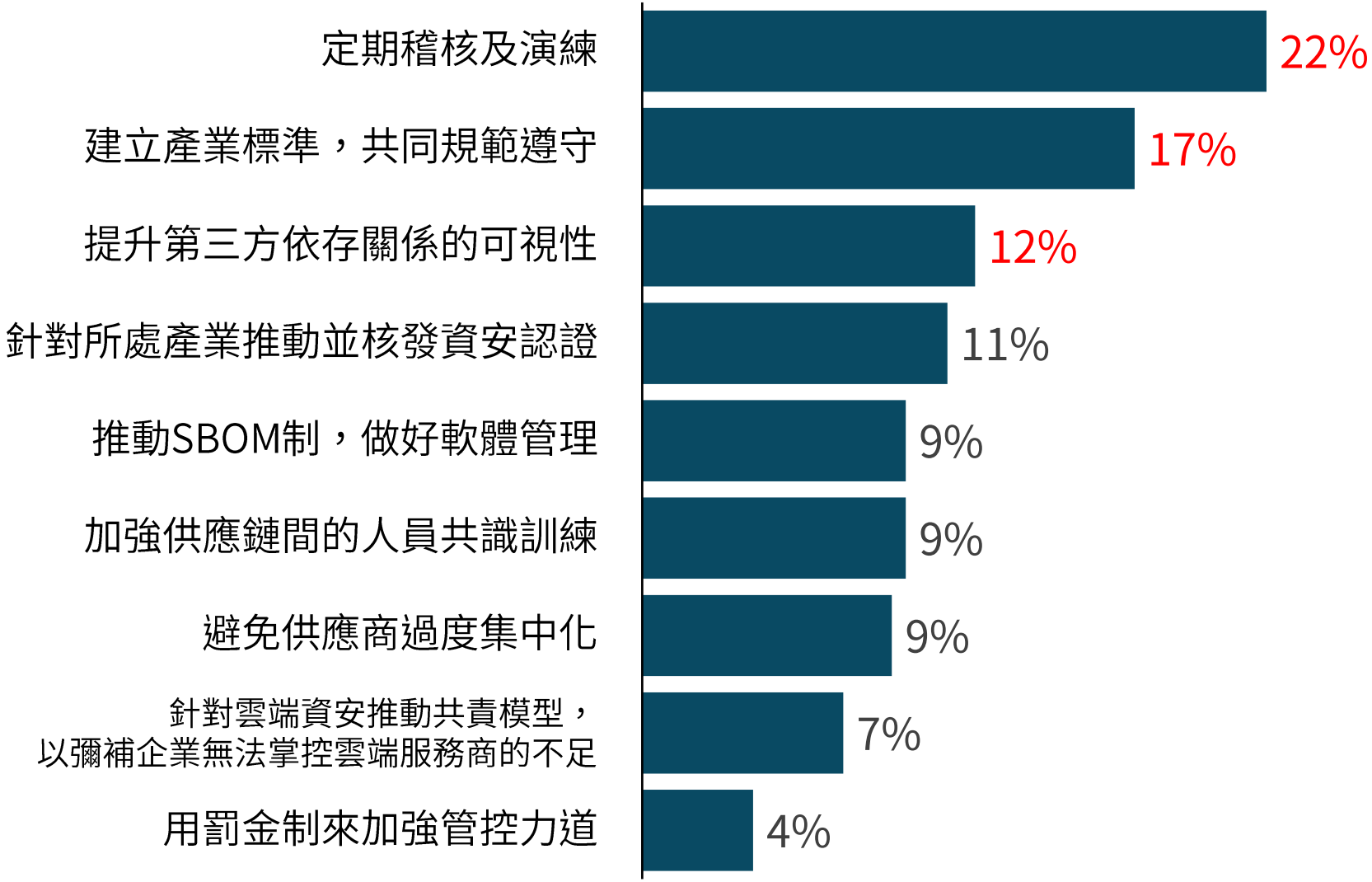
03
15%
上下游廠商間的資安要求
標準不一，增加推行難度

04
13%
缺乏系統性的盤點
及有效的執行策略

05
10%
人力不足

06
7%
軟體開發的資安隱憂防不勝防

可以有效降低供應鏈資安風險的方法



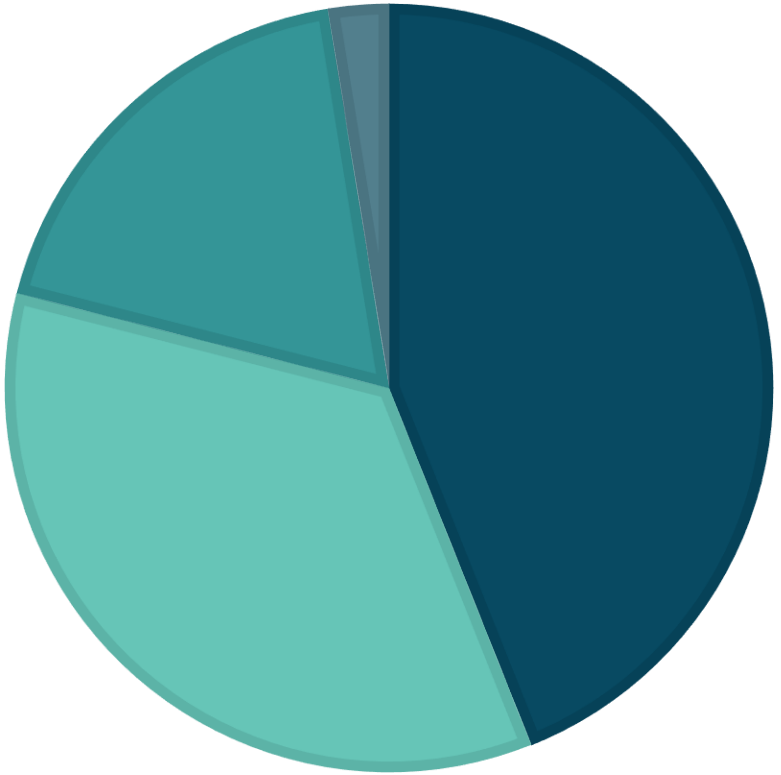
是否已導入SBOM制度?

3%

是，除了內控之外，還應用在第三方的供應鏈管理(提供給業主)

18%

是，應用在內部管理



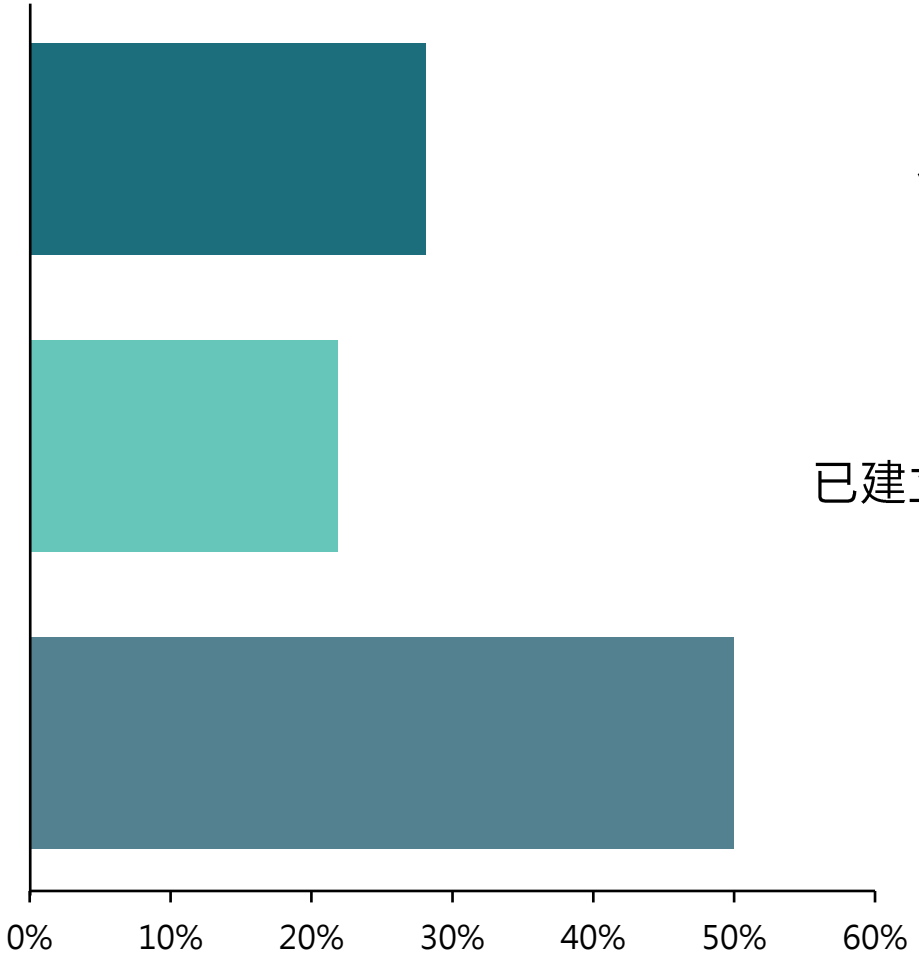
44%

否，目前不考慮導入

35%

否，但已在評估導入

針對所收集的SBOM內容的應用方式



28%

僅收集相關SBOM資訊，未有其他應用機制

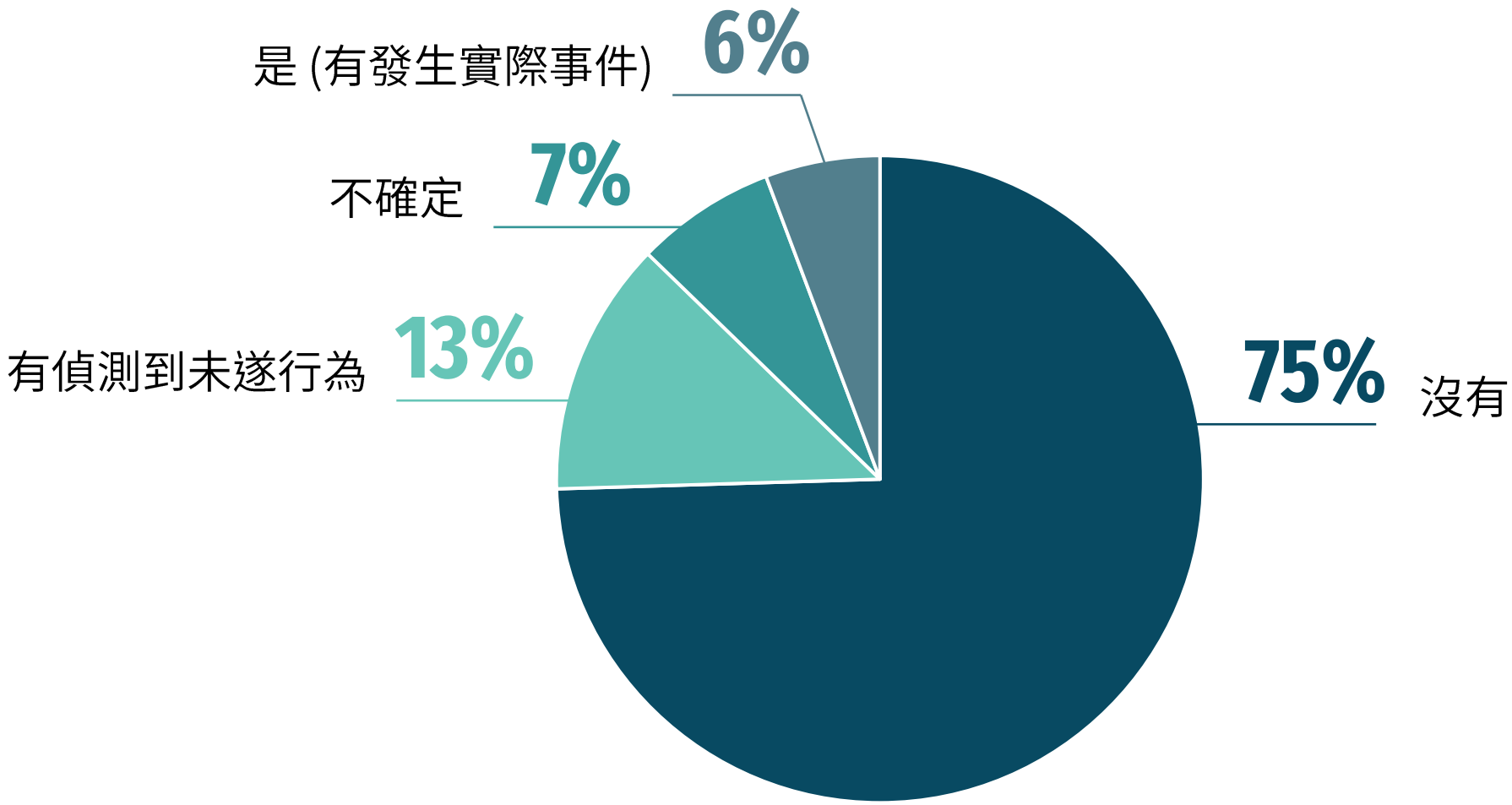
22%

已建立數位管理機制，可提供相關部門搜尋查找

50%

已將SBOM做為漏洞或版本管理之用

是否曾因供應鏈攻擊導致資安事件?




CISO 資安學院
CIO Taiwan
2025
CISO Insight
台灣資安長問卷調查
七、法規遵循與合規挑戰

目前須遵循之主要資訊安全/隱私法規



37% | 資訊安全管理法(台灣)

10% | GDPR(歐盟)

3% | CIRCIA / HIPAA (美國)

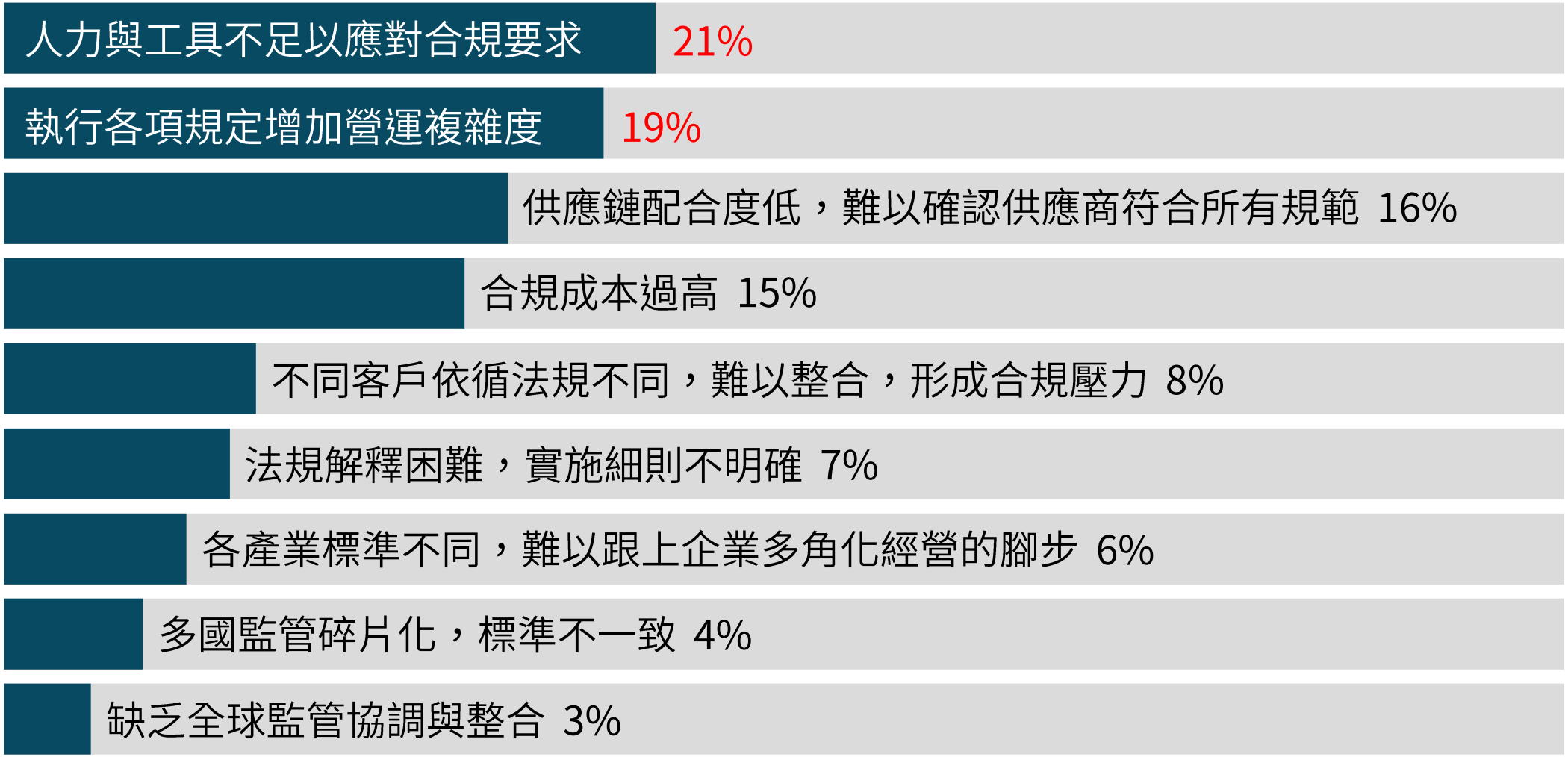
3% | 無明確跨國法規壓力

1% | DORA / NIS2(歐盟)

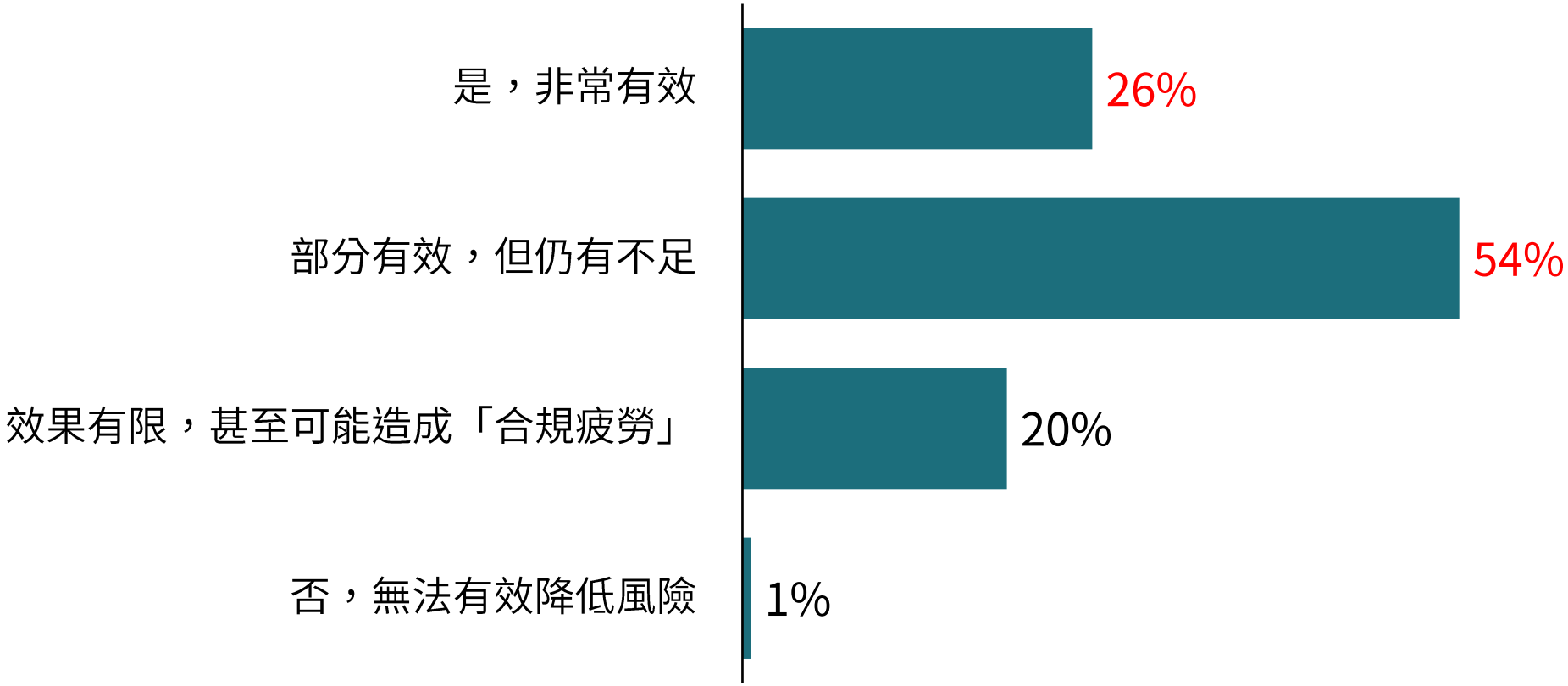
1% | 新加坡網安法

1% | 日本 APPI

合規工作主要挑戰


人力與工具不足以應對合規要求 21%
執行各項規定增加營運複雜度 19%
供應鏈配合度低，難以確認供應商符合所有規範 16%
合規成本過高 15%
不同客戶依循法規不同，難以整合，形成合規壓力 8%
法規解釋困難，實施細則不明確 7%
各產業標準不同，難以跟上企業多角化經營的腳步 6%
多國監管碎片化，標準不一致 4%
缺乏全球監管協調與整合 3%

資安法規是否能有效降低貴公司的資安風險?



CISO 資安學院 CIO Taiwan

2025

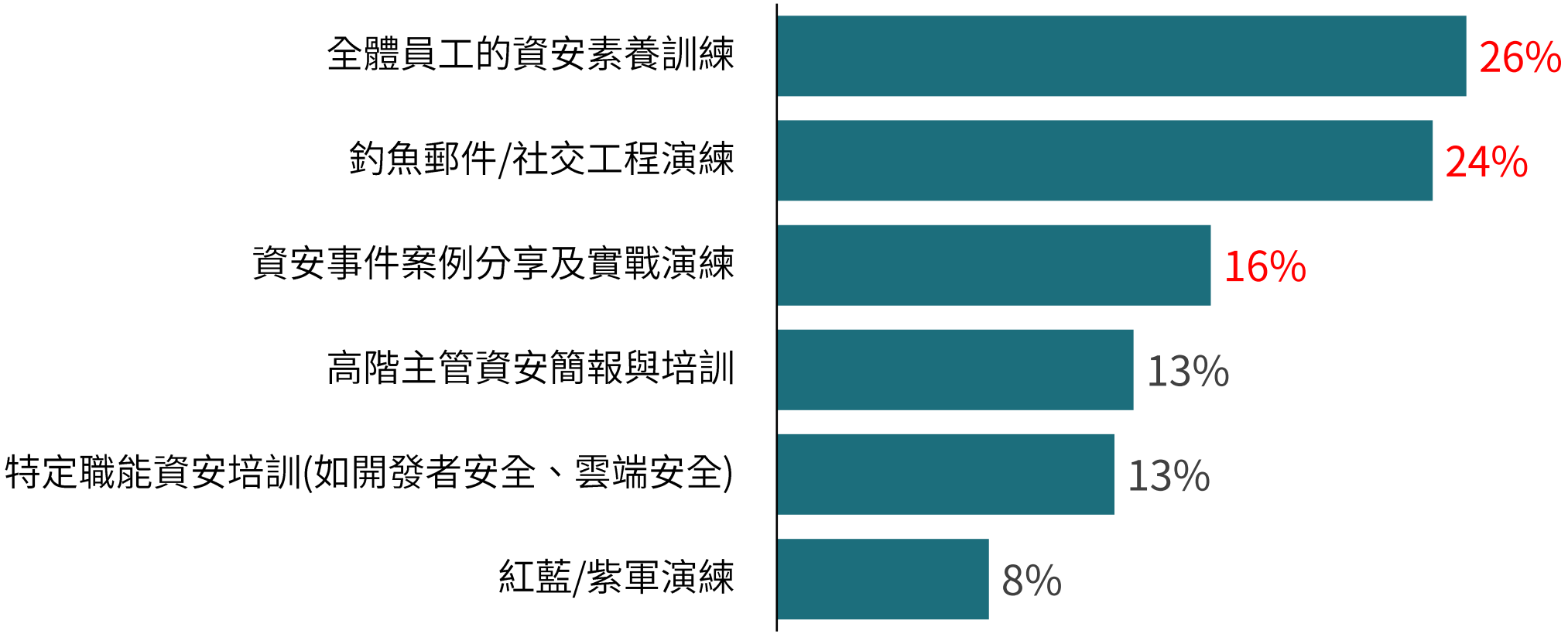
CISO Insight

台灣資安長問卷調查

八、其他資安重點與展望



為員工提供的資安教育訓練



透過哪些方式評估資安教育訓練的成效?



38% 社交工程演練的點擊率與通報率

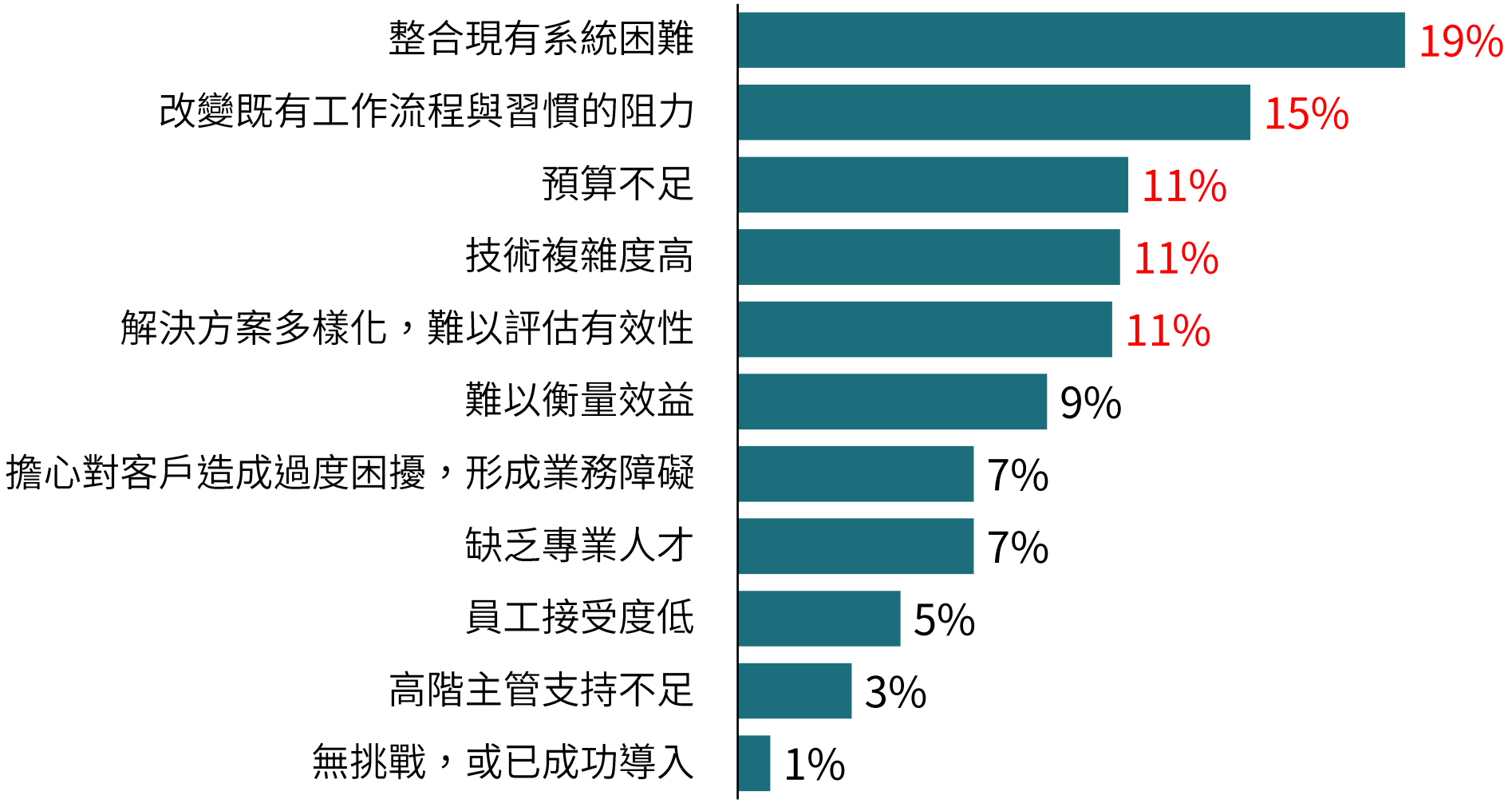
28% 訓練課程後的知識評量或測驗成績

14% 員工行為的觀察與稽核

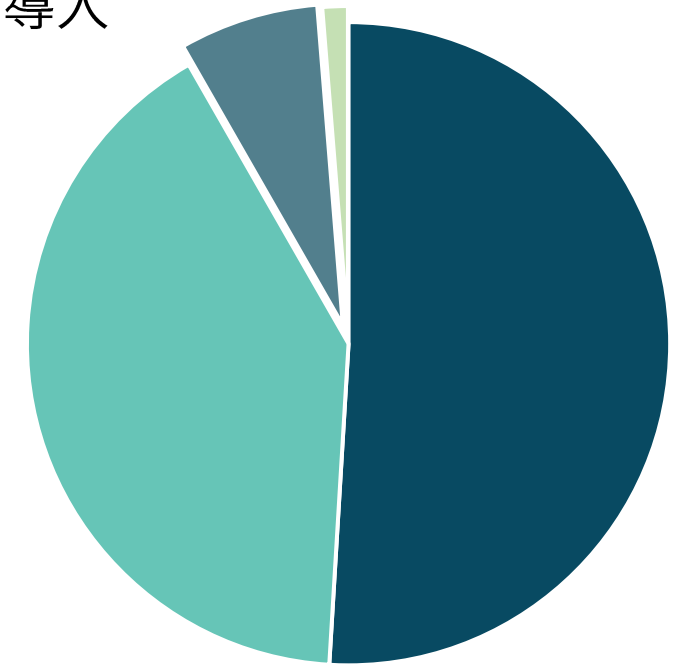
17% 內部資安事件通報數量與品質的變化

3% 尚未建立系統性的成效評估機制

導入零信任架構時遇到的主要挑戰



是否已開始評估或導入量子防禦密碼學(PQC)相關技術?



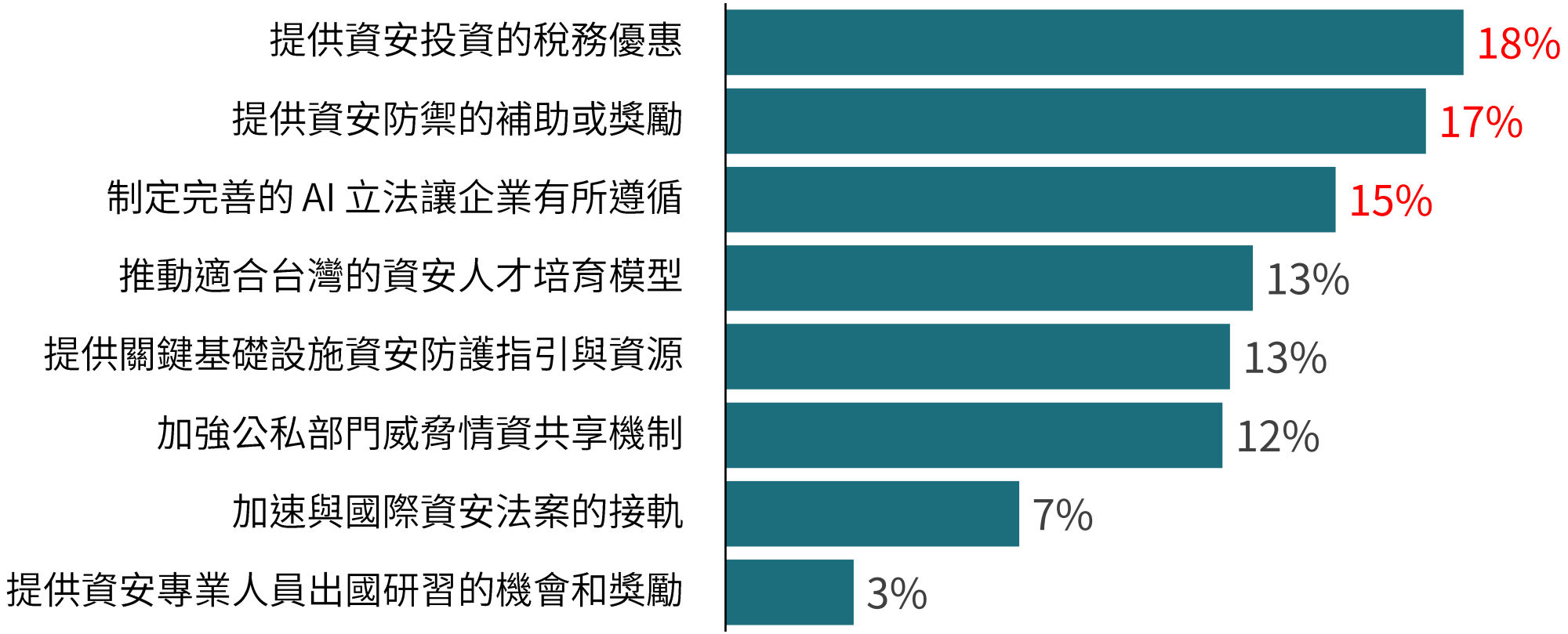
1%
已部分導入或進行概念驗證

7%
已開始評估並規劃導入

41%
有了解但尚未認真評估或導入

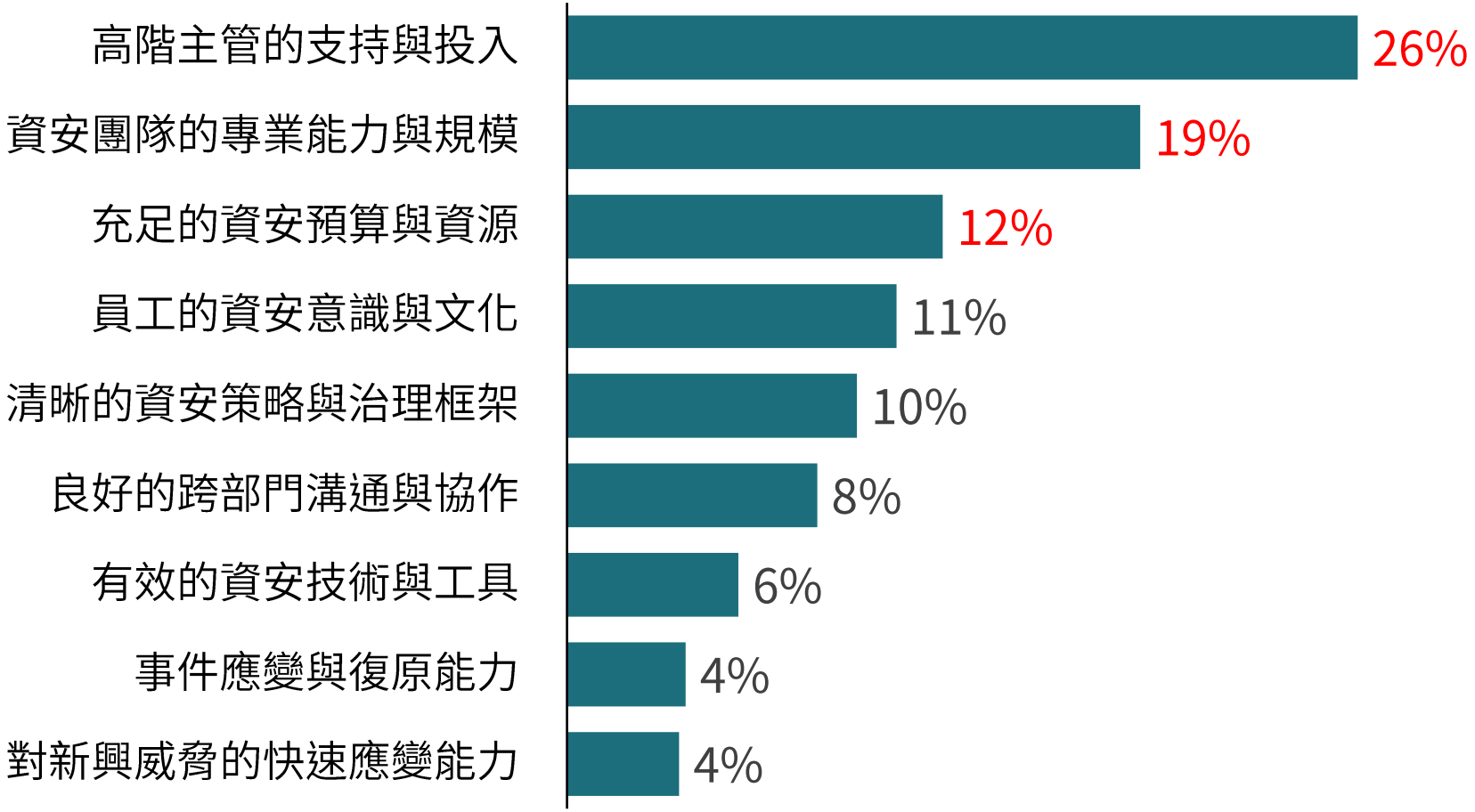
51%
目前沒有了解或相關計畫

希望政府為企業資安提供的協助

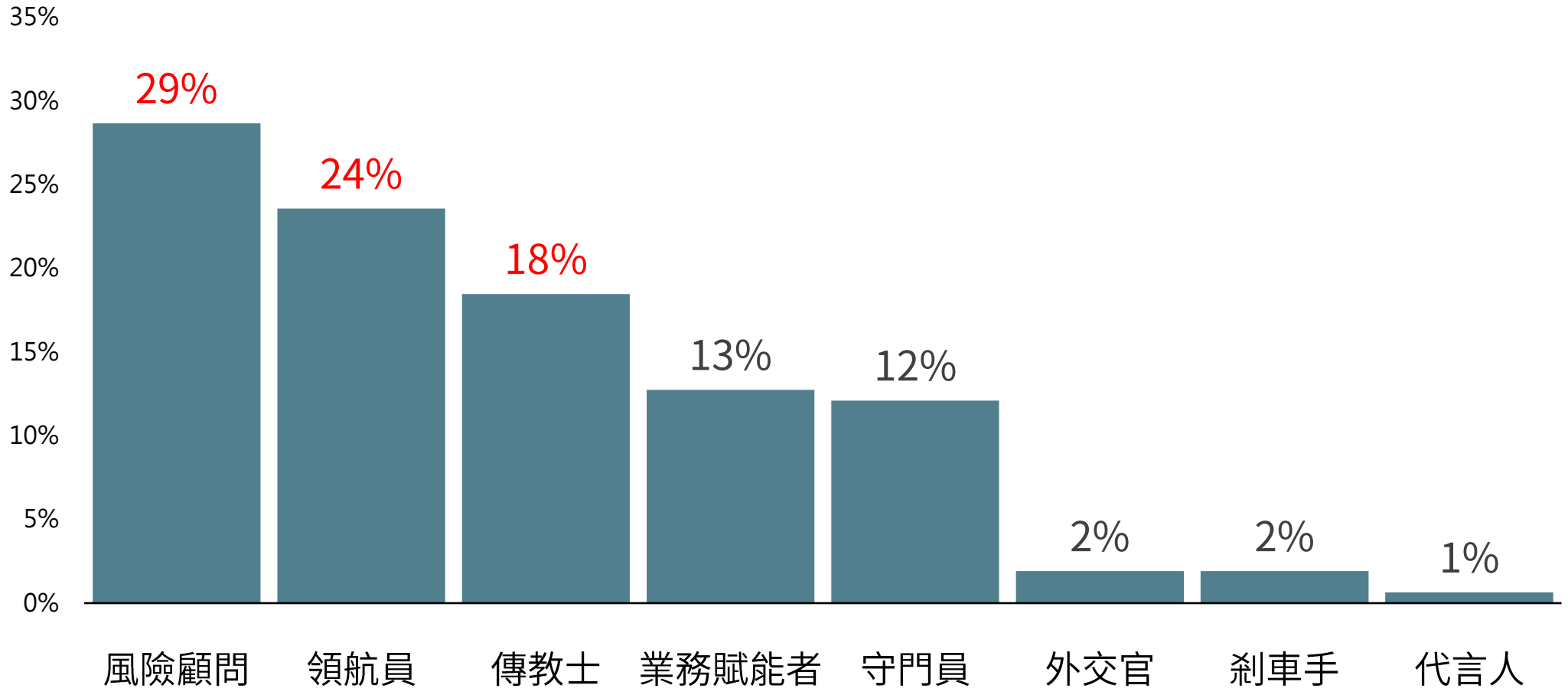



CISO 資安學院
CIO Taiwan
2025
CISO Insight
台灣資安長問卷調查
九、關於CISO自己

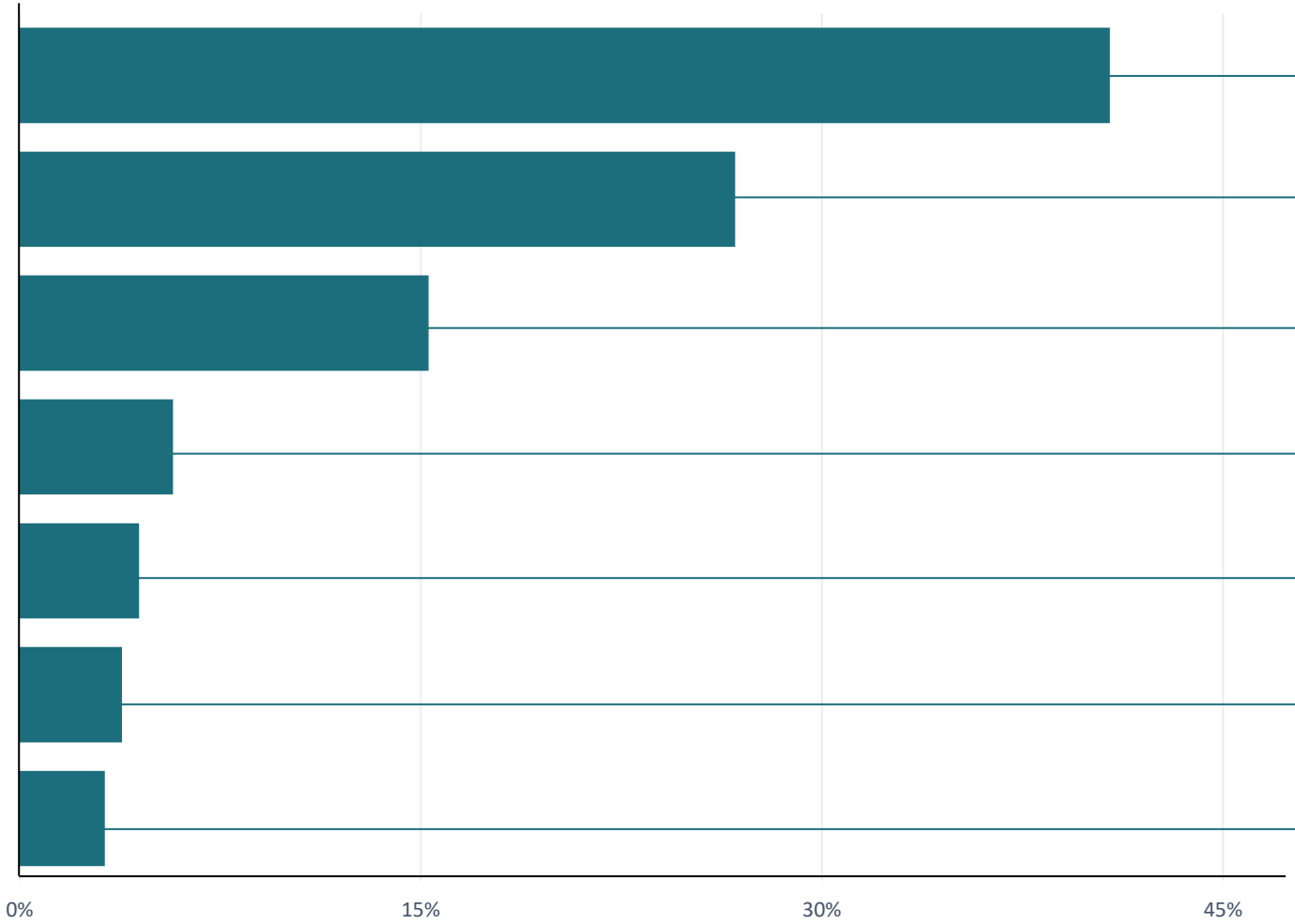
影響資安長成功與否的關鍵因素



您會如何形容資安長的工作?



您最側重的接班人特質?



- 41% 具備跨部門溝通的轉譯能力
- 27% 有業務思維或策略能力
- 15% 對企業文化的全盤掌握
- 6% 有資安乙方經驗
- 4% 實力堅強的技術底子
- 4% 對法遵的了解
- 3% 在不同部門或相關企業有過歷鍊