

CYBERSEC 2025
臺灣資安大會

4/15 - 4/17
臺北南港展覽二館

CISO
FORUM

CISO FORUM

運用六頂思考帽提升資安決策力

結構化思維如何協助CISO與資安團隊

TEAM
CYBERSECURITY

Prometheus Yang

ISACA/外部專家委員

台灣企業風險治理暨風險量化協會，共同創辦人



Contact



講師簡歷

Prometheus Yang (小P)

CISA, CISM, CRISC, CFE, FAIR-CRQ, QTE(認證董事會科技/資通專家)

充滿熱忱的資通與科技風險治理專業人士，擁有超過20年的金融業資通與科技風險經驗，致力於推動企業風險治理。

- 跨國金融機構北亞資通與科技風險治理官 (Hong Kong)
- 格羅方德半導體公司全球科技風險治理官 (Singapore)
- 企業風險與資通安全治理顧問 (Taiwan)
- ISACA外部專家顧問 (Chicago, USA)
 - 科技風險治理諮詢委員會委員
 - 證照諮詢委員、教材審查委員、命題委員
 - 亞太地區研討會籌備委員
- 台灣企業風險治理暨量化分析協會共同發起人



講師簡歷

Disclaimer (免責聲明)

我在此課程中表達的觀點、意見和資訊僅代表我個人的立場，不代表任何與我相關的組織、機構、公司或主/協辦單位、策略合作夥伴的官方立場或觀點。

其次，我將盡我所能確保課程內容的準確性和時效性，但不對訊息的完整性或在特定情境下的適用性提供任何保證。我鼓勵每位聽眾根據自己的判斷和需要進行進一步的研究和考量。

此外，我對於任何人因依賴在此課程中提供的訊息而可能產生的直接或間接損失不承擔責任。每位聽眾應當對自己的決策和行為負責。

最後，我希望本次課程能夠提供有價值的見解和資訊，但請記住這些內容僅供參考，並應在完整的了解和考量後作出任何決策。

In this presentation, the views, opinions, and information expressed are solely my own and do not represent the official stance or views of any organizations, institutions, or the hosting entity associated with me.

Furthermore, I will make every effort to ensure the accuracy and timeliness of the content presented, but I do not guarantee the completeness or applicability of the information in specific situations. I encourage all audience members to conduct further research and consideration based on their own judgment and needs.

Additionally, I do not assume responsibility for any direct or indirect losses that may result from reliance on the information provided in this presentation. Each audience member should be responsible for their own decisions and actions.

Lastly, I hope this presentation will offer valuable insights and information, but please remember that the content is provided for reference only and should be considered thoroughly before making any decisions.

資安/資安風險治理的最大挑戰: 溝通而非技術 技術可以修補但溝通難以突破



為什麼會議中共識難達成



表面原因: 我們常以為共識難產是因為「意見相左」，

核心問題: 其實更深層的原因是一往往是「隧道視野」

每個人都局限於自己的視角，而有意無意地忽略其他人的立場或看法。

**隧道視野，是當我們看得很清楚，卻看不見全貌。

當前資安/資安風險治理的常見情境

- 我(二線、三線)有感覺不安全，但別人(一線)說沒有證據 - 三道模型架構下
- 我們明知道有風險，但資源永遠不夠
- 業務只想上線，我想先補漏洞
- 我提出了創新解法，但大家只怕出錯
- 有很多觀點，卻沒人願意拍板決定

當前資安/資安風險治理的最大挑戰

選項	類型	對應帽子	背後設計邏輯
1 「我有感覺不安全，但別人說沒有證據」	● 情緒 vs 事實	紅帽 vs 白帽	情緒與直覺無法被理性接受
2 「我們明知道有風險，但資源永遠不夠」	● 風險 vs 資源	黑帽 vs 黃帽	重視風險與成本觀點衝突
3 「業務只想上線，我想先補漏洞」	● 技術 vs 業務	白帽 vs 黃帽	白帽聚焦事實，黃帽想推動前進
4 「我提出了創新解法，但大家只怕出錯」	● 創意 vs 保守	綠帽 vs 黑帽	新點子容易被風險觀點打槍
5 「有很多觀點，卻沒人願意拍板決定」	● 缺乏統整	藍帽	無決策架構、討論混亂

案例與討論



創新，是企業的引擎；
資安，是企業的安全帶。
真正的資安，讓創新無後顧之憂。

案例與討論

風險情境: 資訊系統原廠公告停止提供(軟/硬體)支援 (End-of-Support, EOS)

- 高階主管: 「升級要多少錢? 會不會影響業務? 」
- 業務單位: 「新系統麻煩, 我不會用, 舊的就好, 就系統沒有壞, 效能比較低, 但還能忍受, 為什麼要花錢升級? 」
- 法遵單位: 「系統未及時升級, 而導致資料外洩, 可能被主管機關裁罰2,000萬」

問題: 從上面情境來看, 你們覺得溝通EOS風險時最難的是什麼?

什麼是六頂思考帽

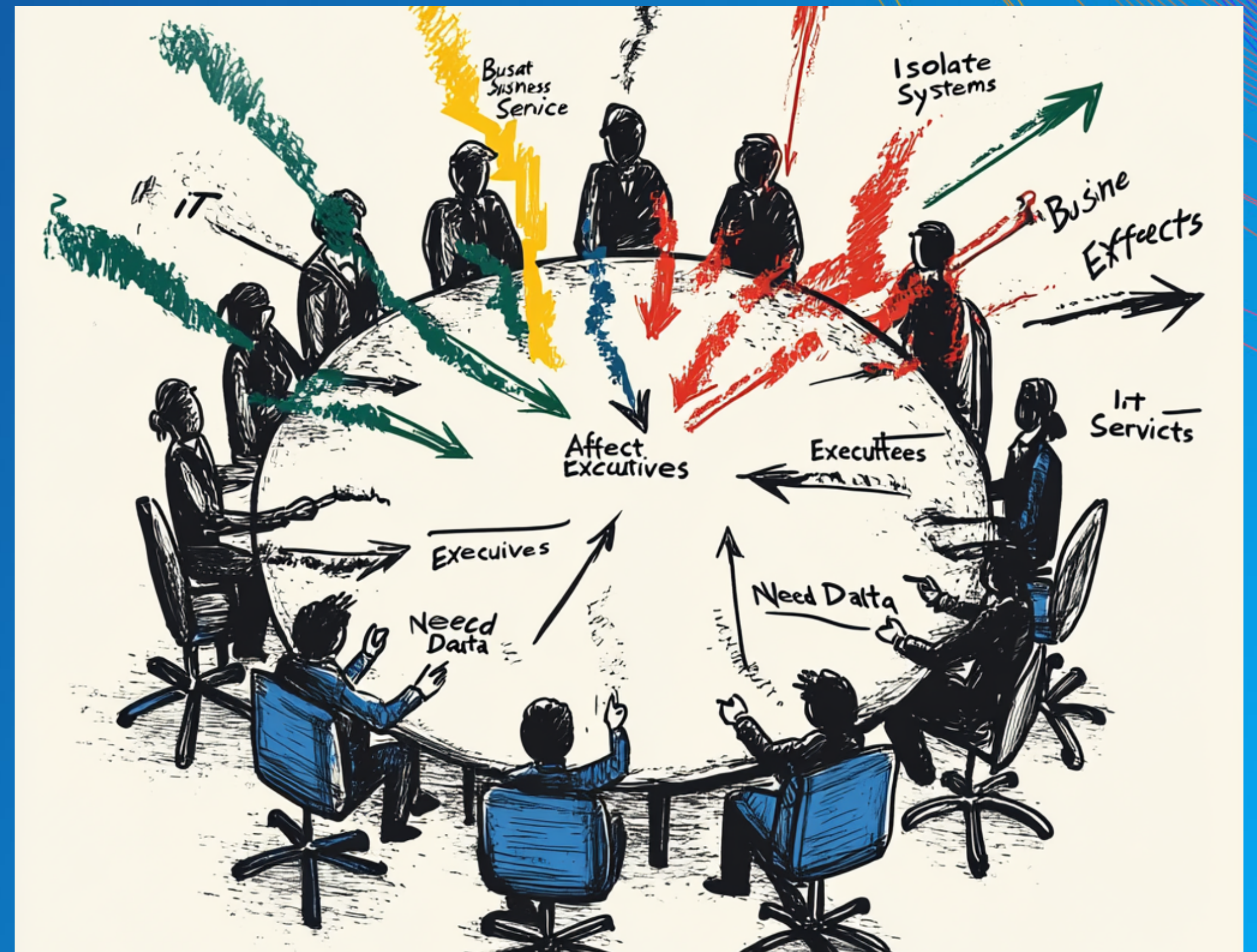
1985 年Edward de Bono（愛德華·德博諾）提出「六頂思考帽」概念為了解決思考過程中的「混亂與重疊」

德博諾觀察到，多數人在討論或思考時會同時使用情感、邏輯、批判與創意等不同思維方式交錯表達，結果常常導致 (例如勒索軟體應對會議)

- 沒有結論: IT主張立即隔離系統，業務部門擔心影響客戶服務，高層要求更多數據，會議結束無共識。
- 情緒與事實混為一談: 業務主管抱怨「資安總是扯後腿」，忽略攻擊已造成50萬美元損失的事實。
- 團隊溝通失效: IT指責業務不配合資通安全訓練，業務反駁IT不懂業務需求，雙方爭執不下。
- 決策效率低落: 因缺乏清晰數據與共識，CISO無法說服高層支付贖金或增設防護，錯失最佳應對時機。

他想要創造一種方法，能讓這些不同的思考「被分類」、「輪流發言」，而不是混在一起。」

德博諾這套方法在管理學、教育、創意產業、心理治療與溝通訓練中廣泛應用。



什麼是六頂思考帽 (續)



帽子	思考模式	用途
白帽	中立、資訊與事實	釐清狀況與背景
黃帽	樂觀、機會與利益	看見正面可能性
黑帽	批判、風險與警示	指出潛在問題
紅帽	情感、直覺	表達不理性的想法
綠帽	創意、可能性	激發創新與替代方案
藍帽	控制、統整、流程導引	主持與協調決策流程

案例與討論

資訊系統原廠公告停止提供(軟/硬體)支援 (End-of-Support, EOS)



事實

- 活動說明
 - 請在輸入框中用名詞寫下 1~3 組與 EOS 案例相關的事實或觀察
 - **專注於客觀數據與現實情況**，尋找EOS的具體影響。請用『你查得到的事實』來回應，而不是感受或想法，例如：『系統將在今年底停止更新』這就是一個白帽式的觀點。
 - 請使用手機或筆電，打開投影畫面上的連結或 QR code
 - 請在輸入框中用名詞寫下1~3組與EOS案例相關的事實

時間限制：1 分鐘輸入時間

案例與討論

資訊系統原廠公告停止提供(軟/硬體)支援 (End-of-Support, EOS)

帽子顏色

案例中的觀點

示例與價值

白帽只關心「事實」，不談感覺、不下結論、不評論價值。

EOS公告、無更新、漏洞未補、系統效能下降

- 原廠公告的EOS日期是什麼？（例如：2025年6月30日）
- 目前有多少系統或設備依賴該軟/硬體？（例如：50台伺服器使用舊版Windows Server）。
- 停止支援後，漏洞修補與安全更新將終止，可能增加多少風險？

● 白帽（事實）

可以運用5W1H協助團隊釐清事實、辨識問題的基本輪廓，為後續的溝通與決策提供客觀基礎

WHO: 哪些人被影響？誰負責？ / WHAT: 是什麼事件？（如勒索攻擊） / WHERE: 發生在哪個系統或區域？ / WHEN: 什麼時候發生？持續多久？何時可以修復？ / HOW 怎麼被發現？影響有多大？

示例：微軟公告Windows 10於2025年10月14日後終止支援，不再提供安全更新、技術支援或錯誤修復，需立即評估替代方案。受影響的系統 _____ 工作站/伺服器 _____, 微軟提供延伸安全更新方案，每台設備第一年每台設備 \$61 美元，第二年 \$122 美元，第三年 \$244 美元。

價值：提供決策所需的事實資料，避免主觀臆測

案例與討論

資訊系統原廠公告停止提供(軟/硬體)支援 (End-of-Support, EOS)



情緒 - 感受, 直覺

- 活動說明
 - 請在輸入框中用名詞寫下 1~3 組與 EOS 案例相關的事實或觀察
 - 請輸入你對這個 EOS 案例的第一直覺感受或潛在情緒反應
 - 不要分析、不要講道理，只要輸入你或他人在這種情況下可能有的情緒或直覺。
 - 請使用手機或筆電，打開投影畫面上的連結或 QR code
 - 請在輸入框中用名詞寫下 1~3 組與 EOS 案例相關的事實

時間限制：1 分鐘輸入時間

案例與討論

資訊系統原廠公告停止提供(軟/硬體)支援 (End-of-Support, EOS)

帽子顏色

案例中的觀點

示例與價值

紅帽只關心「感覺」，不需要理由、不找證據、不怕主觀。

● 紅帽（情緒）

擔心、煩躁、抗拒、恐慌、不安

- IT團隊可能感到壓力或焦慮，因需快速適應新系統
- 業務部門可能抗拒改變，擔心學習曲線影響日常工作。
- CISO直覺認為，高層可能低估EOS的嚴重性，需更強烈警告。

示例：業務單位抱怨「這 MFA 太麻煩了啦！別的公司都沒這樣做，我感覺客戶會抱怨，然後我們業績就會下滑！」，CISO感受到團隊士氣低落，決定優先溝通與支持

價值：理解人性因素，調整策略以提升配合度。

● 尋求事實：「目前我們有多少客戶反映過登入困難？」

● 假設風險與後果：「如果 MFA 被跳過，帳號被盜用的損失是多少？」

案例與討論

資訊系統原廠公告停止提供(軟/硬體)支援 (End-of-Support, EOS)



- 活動說明
 - 請在輸入框中用名詞寫下 1~3 組與 EOS 案例相關的事實或觀察
 - 請輸入你認為這個 EOS 案例中可以帶來的正面機會或價值
 - 站在樂觀角度思考，有沒有可能藉此升級、改善流程或提升安全性？
 - 請使用手機或筆電，打開投影畫面上的連結或 QR code
 - 請在輸入框中用名詞寫下 1~3 組與 EOS 案例相關的事實

時間限制：1 分鐘輸入時間

案例與討論

資訊系統原廠公告停止提供(軟/硬體)支援 (End-of-Support, EOS)

帽子顏色

案例中的觀點

示例與價值

黃帽只關心「希望」，專找機會、好處、正面價值。

● 黃帽（正面）

優化系統、提升安全性、轉型契機、創新導入、爭取預算

- EOS是升級到更安全、更現代系統的機會（例如：從舊版轉移到雲端解決方案）
- 新系統可能提升效能並降低長期維護成本（例如：每年節省20%維運費用）
- 可藉此推動資安文化，說服高層投資新技術

示例：CISO向高層強調，轉換到新系統能提升營運韌性並贏得客戶信任，並符合最新法規要求（如GDPR）。

價值：鼓勵正向思維，將危機轉為轉機

案例與討論

資訊系統原廠公告停止提供(軟/硬體)支援 (End-of-Support, EOS)



- 活動說明
 - 請在輸入框中用名詞寫下 1~3 組與 EOS 案例相關的事實或觀察
 - 請輸入你對於繼續使用 EOS 系統可能導致的風險或潛在問題
 - 請思考可能發生什麼壞事？從資安、營運、法規、商譽等角度都可以。
 - 請使用手機或筆電，打開投影畫面上的連結或 QR code
 - 請在輸入框中用名詞寫下 1~3 組與 EOS 案例相關的事實

時間限制：1 分鐘輸入時間

案例與討論

資訊系統原廠公告停止提供(軟/硬體)支援 (End-of-Support, EOS)

帽子顏色

案例中的觀點

示例與價值

藍帽只關心「思考過程的管理與組織」，確保討論有結構、有序並達成目標。

資安漏洞、被罰錢、資料外洩、系統當機、稽核缺失

● 黑帽（負面）

- 未更新系統可能成為駭客目標，增加資料外洩風險（例如：WannaCry攻擊利用EOS漏洞）
- 不合法規要求可能導致罰款（如CCPA要求使用受支援系統）
- 升級失敗或延遲可能影響業務連續性（例如：系統停機損失每日10萬美元）

示例：CISO警告，若不即時更換EOS系統，企業可能面臨勒索軟體攻擊，損失遠超升級成本。

價值：識別風險，促使團隊採取行動

案例與討論

資訊系統原廠公告停止提供(軟/硬體)支援 (End-of-Support, EOS)



- 活動說明
 - 請在輸入框中用名詞寫下 1~3 組與 EOS 案例相關的事實或觀察
 - 請輸入你能想到的創意解法或替代方案，面對 EOS 有沒有新作法？
 - 打破框架，想想我們可以怎麼更有創意地解決問題？大膽一點也沒關係！。
 - 請使用手機或筆電，打開投影畫面上的連結或 QR code
 - 請在輸入框中用名詞寫下 1~3 組與 EOS 案例相關的事實

時間限制：1 分鐘輸入時間

案例與討論

資訊系統原廠公告停止提供(軟/硬體)支援 (End-of-Support, EOS)

帽子顏色

案例中的觀點

示例與價值

綠帽只關心「可能性」，專找新點子、新方法、新角度，永遠問：我們還能不能用不一樣的方式來解決？

● 綠帽（創意）

雙軌系統、虛擬化隔離、教育訓練計畫、雲端遷移、SaaS替代

- 是否能開發內部補丁或虛擬化舊系統，延長使用壽命？
- 能否採用開源替代方案，取代EOS產品？（例如：用Linux取代舊Windows）
- 是否能與第三方簽約，委外提供延長支援？

示例：CISO提議過渡性解決方案，自行開發修補軟體或與原廠簽訂延長維護服務。

價值：激發新想法，應對資源或時間限制

案例與討論

資訊系統原廠公告停止提供(軟/硬體)支援 (End-of-Support, EOS)



- 活動說明
 - 請在輸入框中用名詞寫下 1~3 組與 EOS 案例相關的事實或觀察
 - 請輸入你認為在 EOS 案例中需要的決策或管理步驟
 - 請思考：誰該負責決定？該有什麼樣的推動流程或資源安排？
 - 請使用手機或筆電，打開投影畫面上的連結或 QR code
 - 請在輸入框中用名詞寫下 1~3 組與 EOS 案例相關的事實

時間限制：1 分鐘輸入時間

案例與討論

資訊系統原廠公告停止提供(軟/硬體)支援 (End-of-Support, EOS)

帽子顏色

案例中的觀點

示例與價值

藍帽只關心的是思考過程的管理，
確保討論有結構、有序並達成目標

成立專案小組、制定時程表、跨部門合作、風險優先順序、
高層決策

● 藍帽（統整）

- 應建立EOS應對時間表：評估（1個月）、測試新系統（3個月）、部署（6個月）
- 需整合各部門意見，平衡技術、預算與業務需求
- 定期檢視進度，確保與企業策略一致（如數位轉型目標）

示例：CISO召開跨部門會議，制定遷移計畫，並每月追蹤進度，確保2025年EOS前完成轉換。

價值：統籌各方觀點，確保決策有序推進

案例與討論

資訊系統原廠公告停止提供(軟/硬體)支援 (End-of-Support, EOS)

帽子顏色	案例中的觀點	價值
● 白帽 (事實)	EOS公告、無更新、漏洞未補、系統效能下降 原廠公告的EOS日期是什麼？(例如：2025年6月30日) 目前有多少系統或設備依賴該軟/硬體？(例如：50台伺服器使用舊版Windows Server)。 停止支援後，漏洞修補與安全更新將終止，可能增加多少風險？	示例：CISO查閱報告，發現企業有70%的核心系統運行即將EOS的軟體，需立即評估替代方案。 價值：提供決策所需的事實資料，避免主觀臆測
● 紅帽 (情緒)	擔心、煩躁、抗拒、恐慌、不安 IT團隊可能感到壓力或焦慮，因需快速適應新系統 業務部門可能抗拒改變，擔心學習曲線影響日常工作。 CISO直覺認為，高層可能低估EOS的嚴重性，需更強烈警告。	示例：員工抱怨「又要換系統，太麻煩」，CISO感受到團隊士氣低落，決定優先溝通與支持 價值：理解人性因素，調整策略以提升配合度。
● 黃帽 (正面)	優化系統、提升安全性、轉型契機、創新導入、爭取預算 EOS是升級到更安全、更現代系統的機會(例如：從舊版轉移到雲端解決方案) 新系統可能提升效能並降低長期維護成本(例如：每年節省20%維護費用) 可藉此推動資安文化，說服高層投資新技術	示例：CISO向高層強調，轉換到新系統能提升營運韌性並贏得客戶信任，並符合最新法規要求(如GDPR)。 價值：鼓勵正向思維，將危機轉為機遇
● 黑帽 (負面)	資安漏洞、被罰錢、資料外洩、系統當機、稽核缺失 未更新系統可能成為駭客目標，增加資料外洩風險(例如：WannaCry攻擊利用EOS漏洞) 不符合法規要求可能導致罰款(如CCPA要求使用受支援系統) 升級失敗或延遲可能影響業務連續性(例如：系統停機損失每日10萬美元)	示例：CISO警告，若不即時更換EOS系統，企業可能面臨勒索軟體攻擊，損失遠超升級成本。 價值：識別風險，促使團隊採取行動
● 綠帽 (創意)	雙軌系統、虛擬化隔離、教育訓練計畫、雲端遷移、SaaS替代 是否能開發內部補丁或虛擬化舊系統，延長使用壽命？ 能否採用開源替代方案，取代EOS產品？(例如：用Linux取代舊Windows) 是否能與第三方簽約，委外提供延長支援？	示例：CISO提議過渡性解決方案，自行開發修補軟體或與原廠簽訂延長維護服務。 價值：激發新想法，應對資源或時間限制
● 藍帽 (統整)	成立專案小組、制定時程表、跨部門協作、風險優先順序、高層決策 應建立EOS應對時間表：評估(1個月)、測試新系統(3個月)、部署(6個月) 需整合各部門意見，平衡技術、預算與業務需求 定期檢視進度，確保與企業策略一致(如數位轉型目標)	示例：CISO召開跨部門會議，制定遷移計畫，並每月追蹤進度，確保2025年EOS前完成轉換。 價值：統籌各方觀點，確保決策有序推進

案例與討論

星巴克門市全面取消現金支付，只保留電子支付（信用卡、行動支付等）



白帽:

- 「根據我們的資料，目前已有 92% 顧客使用非現金支付，現金結帳比例持續下降。」
- 「使用無現金支付，櫃檯結帳平均可節省 7 秒，尖峰時段能提高 5% 的服務效率。」
- 「目前人員每月仍需花 8 小時點現金與做交接帳，出錯率是電子支付的 3 倍。」

紅帽:

- 我有點擔心老年顧客會感到被排除，畢竟不是每個人都有智慧型手機。
- 完全不收現金會讓某些顧客覺得不方便甚至不被尊重，可能會有情緒反彈。
- 我感覺這政策會在社群媒體上被某些族群放大批評。

黑帽:

- 如果行動支付系統故障怎麼辦？停機時間可能導致營運中斷。
- 這也可能產生負面公關風險，特別是在資訊落差較大的區域門市。
- 會不會出現大量客訴、甚至被監管機關質疑歧視不使用科技的消費者？

案例與討論

星巴克門市全面取消現金支付，只保留電子支付（信用卡、行動支付等）



黃帽:

- 轉向無現金可以讓我們品牌形象更現代、環保，也符合 ESG 推動方向。
- 減少現金處理的人力成本與錯帳問題，是長期可觀的節省與效率提升。
- 這也可以讓顧客更快速完成交易，提升顧客體驗與回轉率。

綠帽:

- 我們可以設計『數位支付體驗日』逐步推行，從特定門市測試起步。
- 或許可以針對熟齡顧客，推出簡單的教學活動或導購協助切換支付工具。」「我們甚至可以結合會員 APP 推動『無現金回饋點數活動』來鼓勵轉型。

藍帽

- 我們先從白帽數據開始討論，再讓紅帽反映顧客感受，最後用黃帽與綠帽提出可行方案。
- 根據今天的討論，建議我們先在 10 間高使用率門市進行無現金試點，並同步監控客訴與滿意度。
- 下一步由行銷團隊設計轉換溝通策略，兩週後我們再回來看初步成效。」

案例討論總結

資訊系統原廠公告停止提供(軟/硬體)支援 (End-of-Support, EOS)

你們剛才看到的，是一場跨部門決策的縮影，每一頂帽子，代表了一種在組織內經常出現的聲音

- 白帽：誰掌握了數據與事實？(資安專業與威脅情報分析)
- 紅帽：誰是最早產生情緒反應的使用者？(同理溝通、理解員工與高層的情緒反應)
- 黑帽：誰對風險特別敏感？(評估風險、預判阻力與代價)
- 黃帽：誰看到的是機會與價值？(建立支持資安的正面文化)
- 綠帽：有沒有人願意突破框架想辦法？(推動創新、提出可行方案)
- 藍帽：誰可以整合大家、拉回焦點？(領導決策流程、整合觀點、推動合作)

KEY TAKEAWAYS 重點總結與實務應用

運用時機與技巧

思維結構化，讓資安溝通不再混亂

- 六頂思考帽幫助 CISO 分離情緒與事實、風險與創意
- 有效應對「技術 vs 業務」的跨部門溝通斷層

使用時機:

- 團隊會議或討論陷入僵局時: 當團隊意見分歧、爭論不休或無法達成共識時，可以使用六頂思考帽，讓每個人都從不同角度（如事實、情感、創意等）重新審視問題，避免情緒化爭執，提升討論效率。
- 需要創意解決方案時: 在腦力激盪或產品開發階段，特別是戴上「綠帽」（創意思維）時，能激發新想法，幫助團隊跳出框框，找到創新解決方案。
- 做重要決策時: 無論是個人還是團體，在面對複雜決策時，可以用六頂思考帽全面評估：用「白帽」分析數據、「紅帽」表達直覺、「黑帽」找出風險、「黃帽」看到潛在好處等，從而做出更周全的決定。
- 衝突解決或溝通改善時: 當不同立場的人需要合作時，六頂思考帽能讓各方冷靜下來，按部就班地從不同視角看待問題，減少誤解並促進共識。
- 個人反思或計劃時: 在制定個人目標、職業規劃或處理生活中的難題時，可以獨自使用六頂思考帽，幫助自己更有條理地思考，避免偏向單一觀點。
- 培訓或教育訓練時: 在課堂、工作坊或領導力培訓中，六頂思考帽可以用來教導學生或員工如何批判性思考、團隊合作或解決問題。

KEY TAKEAWAYS 重點總結與實務應用

運用時機與技巧

決策角色清晰，CISO不只戴一頂帽子

思考帽	CISO在討論時的角色
● 白帽（事實）	分析數據、威脅情報、弱點評估
● 紅帽（情緒）	感受使用者抗拒與內部壓力
● 黃帽（正面）	評估資安、法遵、商譽風險
● 黑帽（負面）	傳遞機會與正面價值給高層
● 綠帽（創意）	提出創新解法與過渡選項
● 藍帽（統整）	統整決策流程、召集跨部門

KEY TAKEAWAYS 重點總結與實務應用

運用時機與技巧

使用技巧:

- 啟動會議前，明確你想讓大家戴哪一頂帽子：
 - 例如：「今天我們先看白帽與黑帽的觀點，再收集綠帽建議」當團隊意見分歧、爭論不休或無法達成共識時，可以使用六頂思考帽，讓每個人都從不同角度（如事實、情感、創意等）重新審視問題，避免情緒化爭執，提升討論效率。
- 會議卡住時，切換成藍帽角色，幫大家拉回結構與邏輯
 - 問：「我們是不是混在討論情緒與風險？先釐清事實」
- 彙報高層時，用帽子策略鋪陳重點
 - 白帽（現況）→ 黑帽（風險）→ 黃帽（價值）→ 綠帽（方案）

不是每頂帽子都要你戴上，但每頂觀點都值得你思考。

**You don't need to wear every hat—
but every perspective matters.**



**Start today—transform
your cybersecurity meetings
with Six Thinking Hats.**



六頂思考帽工具

總結



CISO的角色早已不再只是防守，更是協調、引導與啟發。
在瞬息萬變的數位環境中，CISO是企業韌性的指揮家。
而六頂思考帽，是他最精準的指揮棒。