CYBERSEC 2025 臺灣資安大會 | 4/15-4/17 臺北南港展覽二館

CISO FORUM

CISO FORUM

從數據到決策與治理

如何運用FAIR模型提升企業「管理決策效率」與「資安風險治理」

TEAM CYBERSECURITY

Prometheus Yang

ISACA/台灣企業風險治理暨風險量化協會

外部專家委員/共同創辦人

Contact

講師簡歷

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

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.

當代的 CISO：達摩克里斯之劍再現

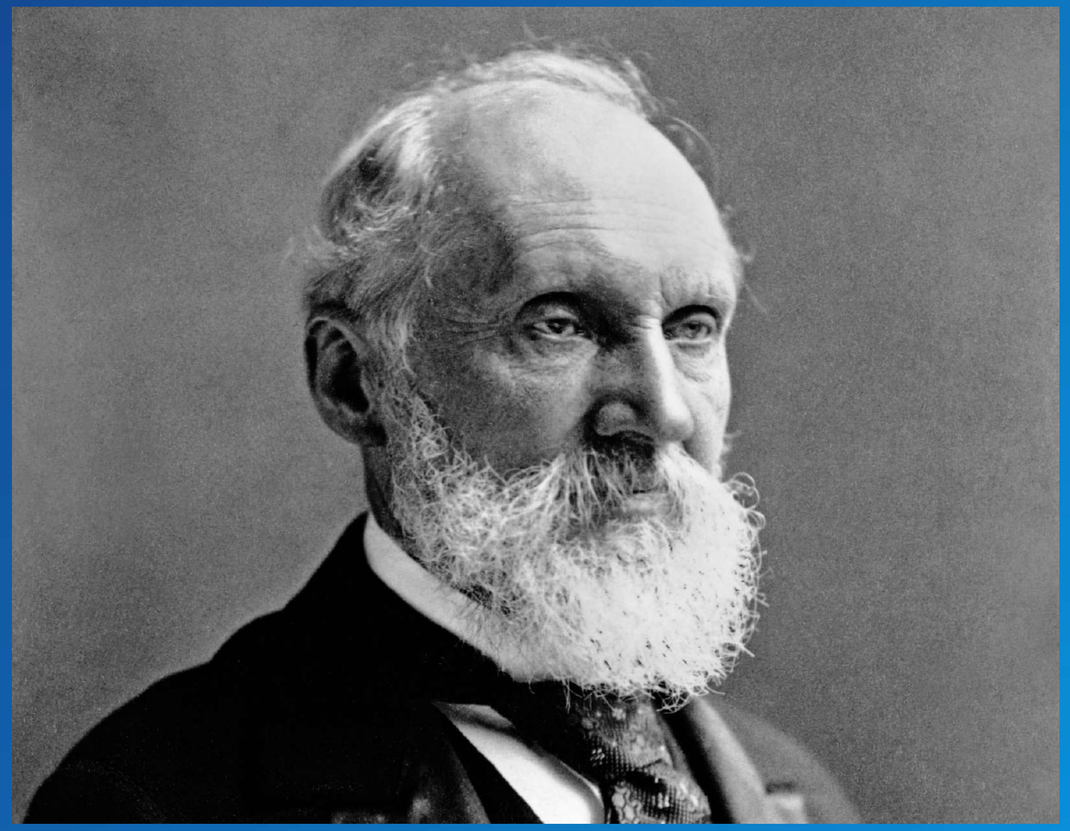
Chief Information Security Officer

首席資訊安全長

or

Chief Imminent Stress Officer
首席超大壓力長

不能以數字表達的風險，就無從真正理解，更遑論有效管理。
If you can't express it in numbers, you don't know it well enough.
—Lord Kelvin（凱文勳爵），英國物理學家



為什麼我們無法有效衡量風險？
三大研究揭示現實差距

- 許多企業在風險量化上面臨挑戰，因為傳統的定性評估（qualitative assessments）缺乏精確數據支持，難以為高階管理層提供可信的決策依據。

— ISACA 白皮書《Cyberrisk Quantification》（2021）

- 僅 52% 的 IT 風險專業人士正在進行某種形式的風險量化，顯示許多企業尚未廣泛採用有效的量化工具。

— AuditBoard《IT Risk Now 會議調查》（2023）

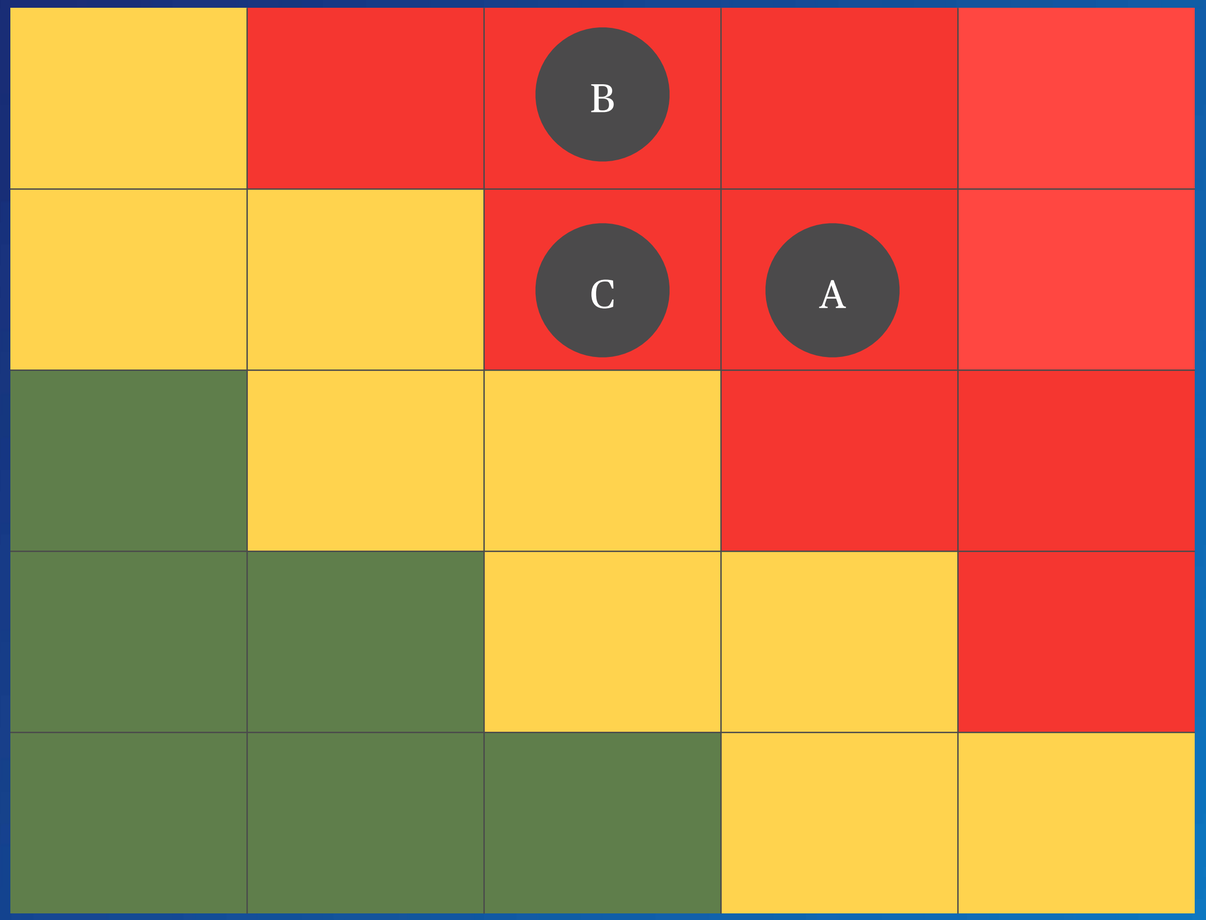
- NIST指出，風險管理需要精準的量化方法，但許多企業因缺乏標準化工具而難以實現數據驅動的決策。

— NIST SP 800-30《Guide for Conducting Risk Assessments》（2012）

資源大戰：公說公有理，婆說婆有理

業務與資安拔河的背後，其實是組織資源配置的哲學問題

你是CISO，擁有1500萬台幣資安預算，需應對三個關鍵風險，你會怎麼選？



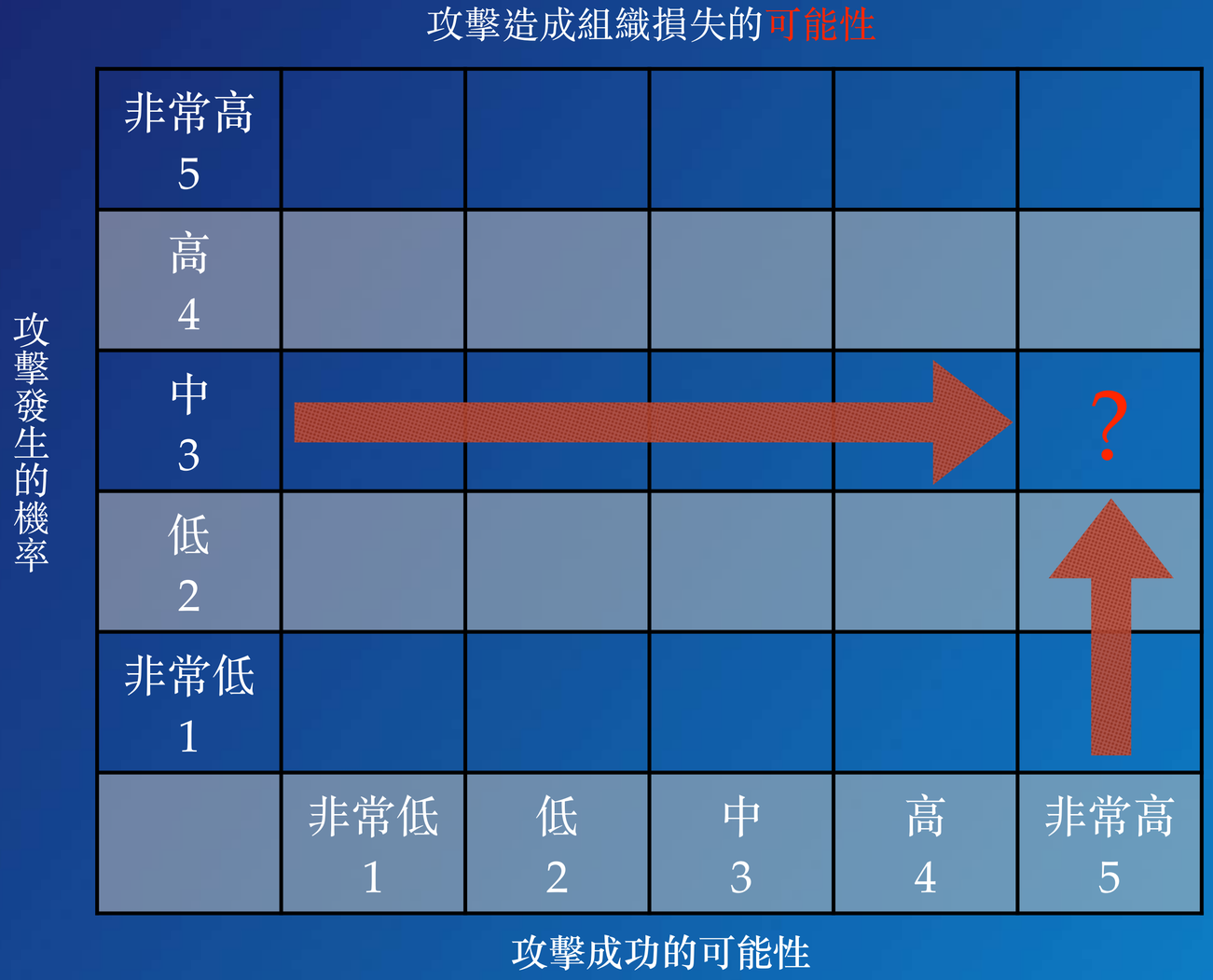
A. 建置不可變動備份系統（Immutable Backup）- 降低勒索軟體影響及損失

B. 執行持續性滲透測試 -- 避免罰款

C. 強化高權限帳號控管與操作軌跡審查 -- 通過稽核

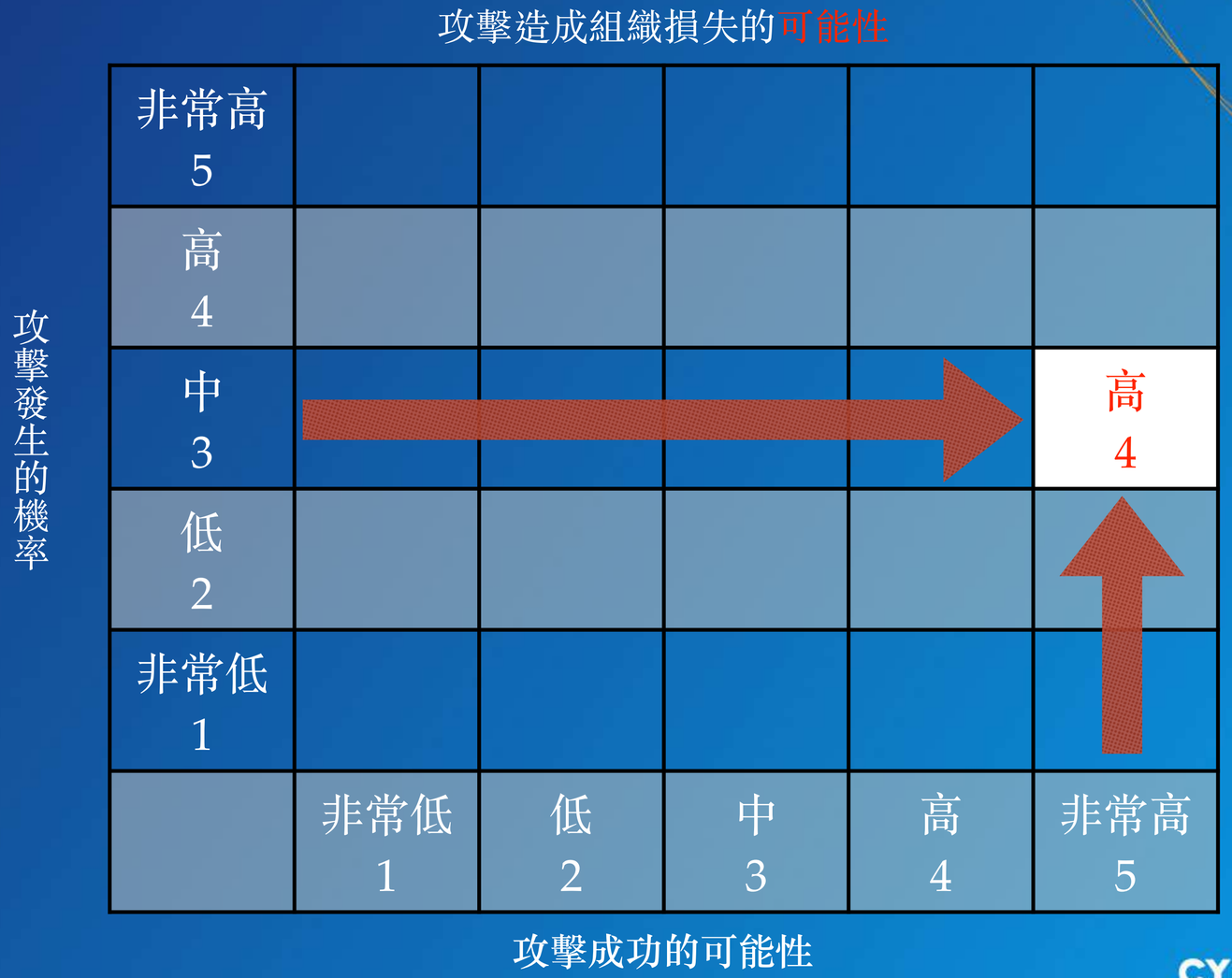
傳統風險矩陣(Heat Map)的限制

傳統風險矩陣(Heat Map)的限制 (續)

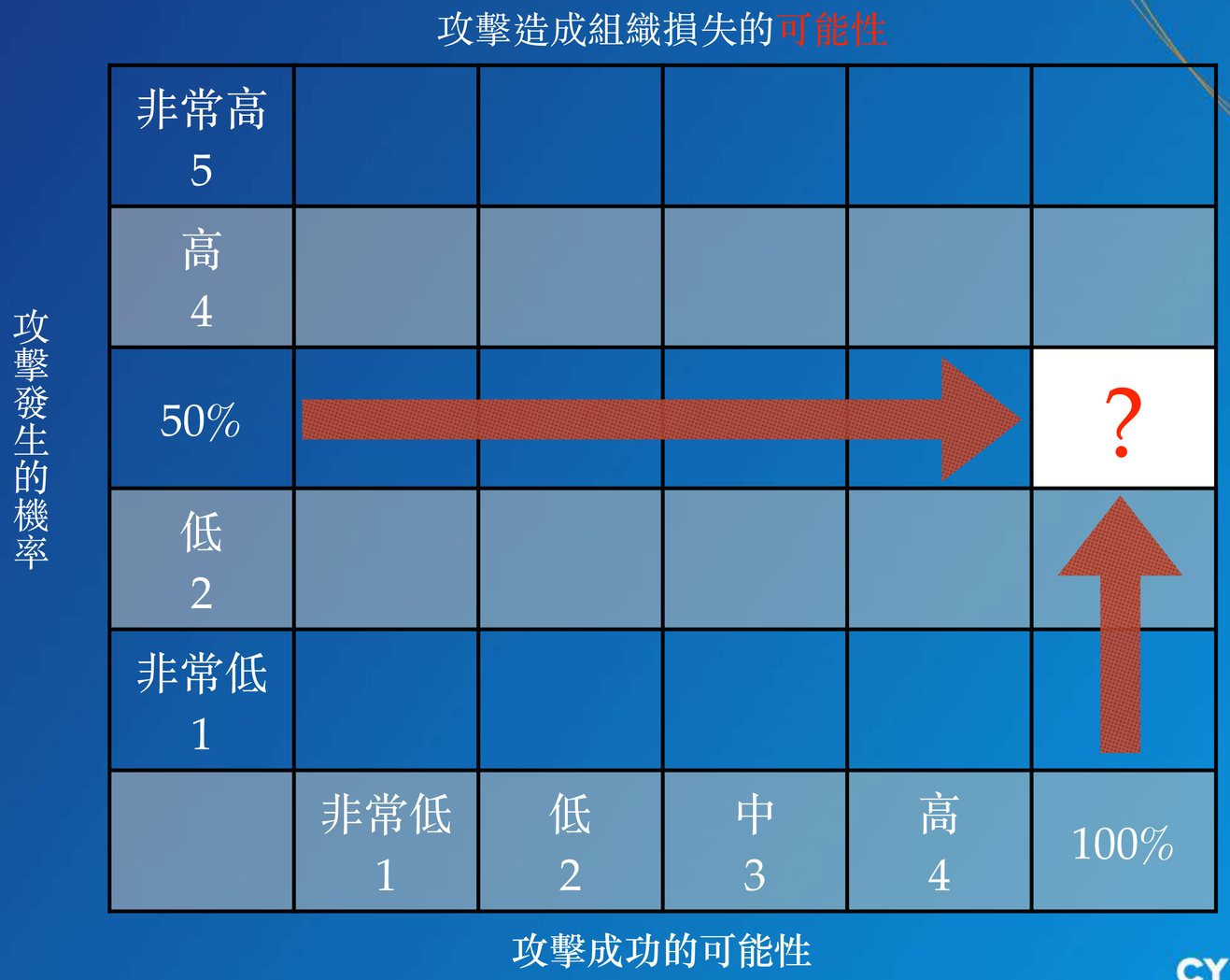


如果攻擊發生的機率為中(3)，而
攻擊成功的可能性為非常高(5)，
攻擊造成組織損失的可能性為何?

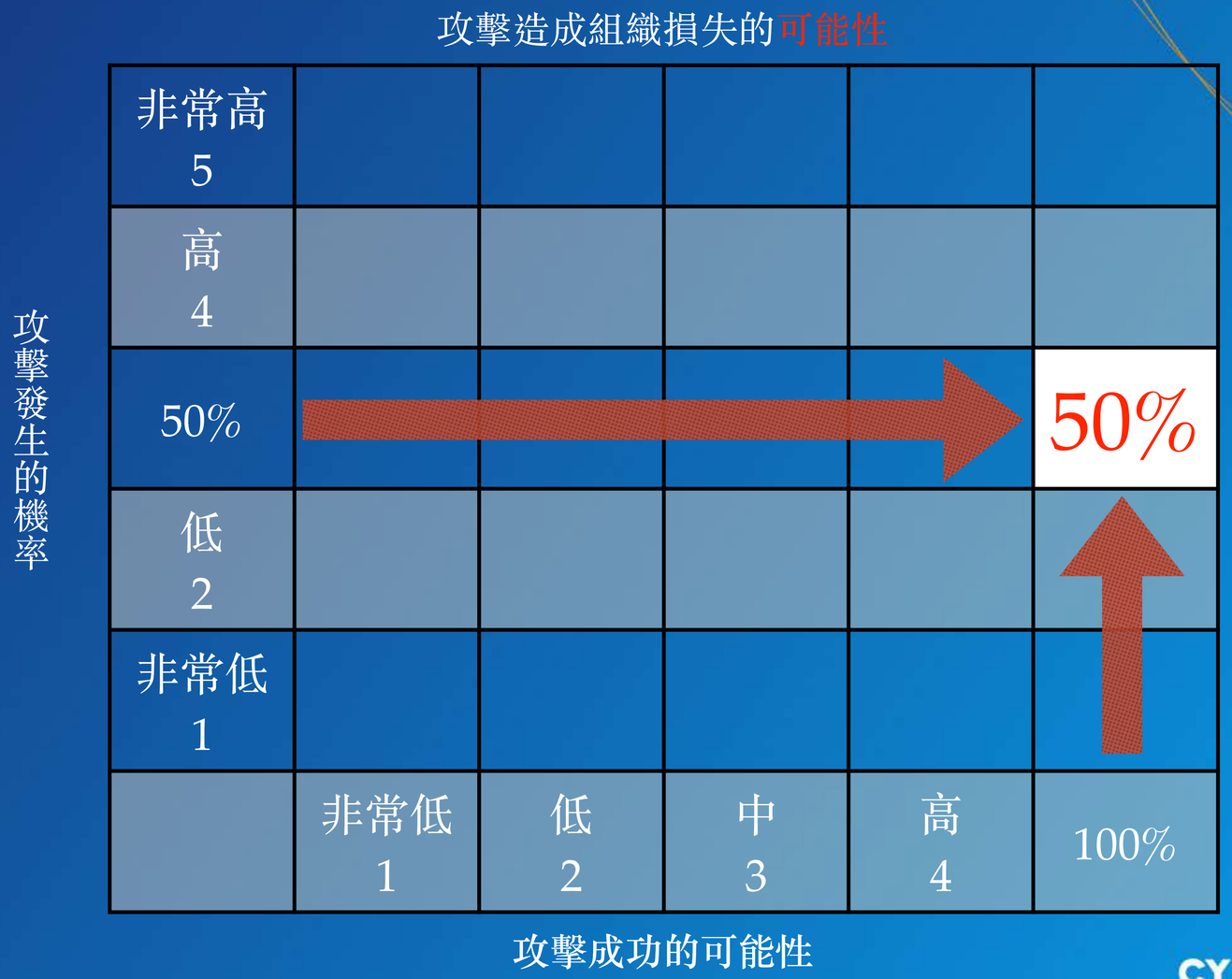
傳統風險矩陣(Heat Map)的限制 (續)



傳統風險矩陣(Heat Map)的限制 (續)



傳統風險矩陣(Heat Map)的限制 (續)



攻擊造成組織損失的可能性
不可能高於攻擊發生的機率

傳統風險矩陣(Heat Map)的限制 (續)

攻擊造成組織損失的可能性

非常高 5	低 2	中 3	高 4	非常高 5	非常高 5
高 4	低 2	中 3	中 3	高 4	非常高 5
中 3	低 2	低 2	中 3	中 3	高 4
低 2	非常低 1	低 2	低 2	中 3	中 3
非常低 1	非常低 1	低 2	低 2	低 2	低 2
	非常低 1	低 2	中 3	高 4	非常高 5

攻擊發生的機率

攻擊成功的可能性

傳統風險矩陣(Heat Map)的限制 (續)

			Impact				
			Negligible	Minor	Moderate	Critical	Catastrophic
			<$10K	$10K to <$100K	$100K to <$1 Million	$1 Million to <$10 Million	≥$10 Million
Likelihood	Frequent	99%+	Medium	Medium	High	High	High
	Likely	>50%–99%	Medium	Medium	Medium	High	High
	Occasional	>25%–50%	Low	Medium	Medium	Medium	High
	Seldom	>1%–25%	Low	Low	Medium	Medium	Medium
	Improbable	≤1%	Low	Low	Low	Medium	Medium

Risk A: Likelihood is 2%, impact is $10 million → 2% * $10 million = **$200,000**

Risk B: likelihood is 20%, impact $100 million → 20% * $100 million = **$20 million**

Reference: Douglas Hubbard, Richard Seiersen, "How to measure Anything in Cyber Security Risk"

傳統風險矩陣(Heat Map)的限制 (續)

			Impact				
			Negligible	Minor	Moderate	Critical	Catastrophic
			<$10K	$10K to <$100K	$100K to <$1 Million	$1 Million to <$10 Million	≥$10 Million
Likelihood	Frequent	99%+	Medium	Medium	High	High	High
	Likely	>50%–99%	Medium	Medium	Medium	High	High
	Occasional	>25%–50%	Low	Medium	Medium	Medium	High
	Seldom	>1%–25%	Low	Low	Medium	Medium	Medium
	Improbable	≤1%	Low	Low	Low	Medium	Medium

Risk A: Likelihood is 50%, impact is $9 million → 50% * $9 million = $4.5 million

Risk B: likelihood is 60%, impact $2 million → 60% * $2 million = $1.2 million

Reference: Douglas Hubbard, Richard Seiersen, "How to measure Anything in Cyber Security Risk"

風險能降多少？
CISO開始流汗的時刻

通報？不通報？會議先吵三回合！

為什麼主管機關不列出「重大」定義或條件

避免一體適用的規定

主管機關不希望制定一個通用的「重大」標準，以避免不同企業在應用時面臨不合適的情況link

企業特性差異

每個企業的產業類別、資本規模和運營模式不同，導致「重大」的定義和影響程度也會隨之變化link

例如，對於一家資本額200萬的公司而言，50萬的損失可能會對該公司造成相當大的影響；然而，對於資本額上千萬的公司來說，50萬的損失可能影響微乎其微。(irent租車2023年資料外洩案裁罰金額為例)。所以主管機關期待企業自己思考並判斷風險事件對企業本身營運是否有「重大」影響。

靈活性要求

各企業應根據自身情況進行風險評估，決定風險事件是否對其運營構成「重大」影響link

強調個別風險評估

主管機關鼓勵企業自行判斷並進行風險管理，而不是依賴統一的標準來評估「重大」風險link

協助我們思考是否「重大」的條件

立法精神

主管機關的立法目的是為了保障投資者的權益，確保他們能夠獲得充分且透明的信息，以便做出明智的投資決策。因此，判斷某一事件是否「重大」，首先要考慮該事件是否會影響投資者對企業未來的展望和行為link

影響投資者決策的資訊

需要識別和分析哪些訊息會影響投資者的評估，這些訊息可能包括財務報表中的數據變動、公司治理的重大變化、法律訴訟、環境和社會風險等。所有這些因素都可能影響投資者對公司的長期信心和投資行為link

重大性判斷的核心考量

其中一個核心考量點是事件對公司財務狀況的影響。任何可能對公司財務產生顯著負面影響的事件，都應被認為具有「重大性」。這解釋了為什麼美國企業越來越重視並使用定量風險評鑑，因為這有助於客觀評估潛在風險對財務的影響link

錯，我可以認；風險，能不能說清楚？

失去脈絡的稽核缺失，只會讓人失控

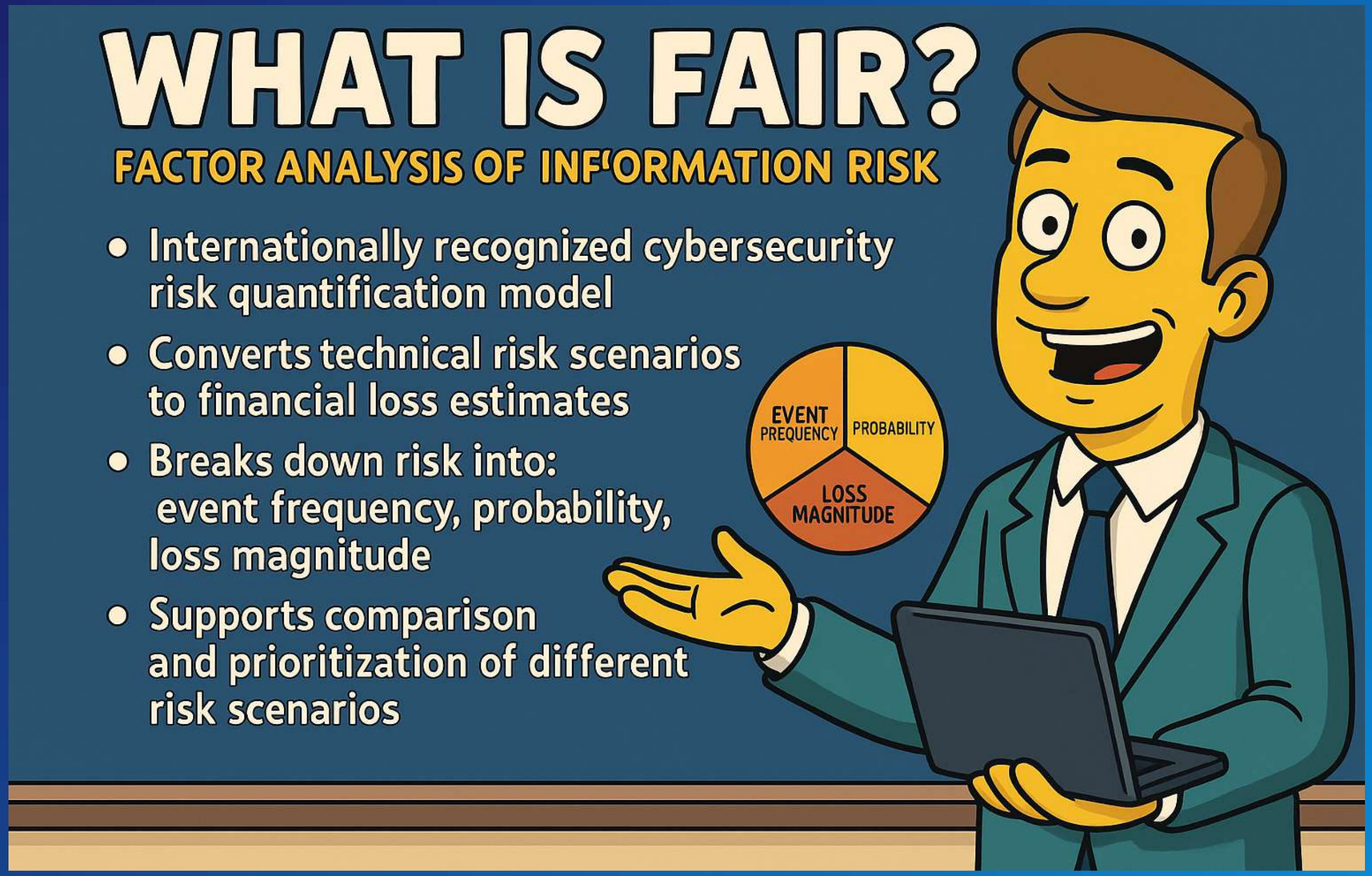
當主觀感受凌駕於事實，風險就變成情緒炸彈

當代 CISO 所背負的 5 大壓力

恐懼行銷的決策陷阱

廠商與 CISO 常以恐懼驅動決策，卻缺乏精準數據支持。

什麼是FAIR CRQ模型



- 國際公認的資安風險量化模型
- 將風險情境轉換成財務損失預估
- 將風險拆解為：事件頻率、可能性、損失規模
- 支援不同風險情境間的比較與排序

FAIR 與傳統風險分析方法比較 —「從熱度圖(Heatmap)到財務數據」

挑戰	傳統方法	FAIR CRQ
主觀性	高	低 (數據導向)
決策支援力	弱	強 (可計算ROI與損失)
合規	ISO 27001	SEC / DORA
優先順序	顏色導向	財務風險導向

困在壓力裡的 CISO，需要一套能說服決策者的方法

FAIR CRQ 如何CISO幫助你完成這些挑戰？

CISO挑戰(痛點)	影響	FAIR解決方案
財務部門挑戰	難以理解資通安全投資的必要性缺乏明確的投資回報率(ROI)	可量化年損失金額(ALE)
溝通障礙	技術與業務單位語言的差異 風險解釋的複雜性	統一風險語言 提升透明度
不一致性	傳統風險評估方法的主觀性 各說各話讓比較失去意義	標準化風險評估框架 量化風險讓比較有意義
資源分配效率低下	有限的資源 資源分配缺乏科學依據	風險排序有依據，聚焦於高風險項目
難以判斷是否達重大偶發通報門檻	違反法規，面臨鉅額罰款或法律責任 喪失投資人與董事會信任	可計算資通事件事件是否對其運營構成「重大」影響
持續演變的(資通)威脅	新型態攻擊不斷出現 威脅環境複雜多變	動態風險管理 強化防禦策略

FAIR定量風險分析模型

風險
由特定的情境而來 $

預估的未來損失的可能頻率和規模

損失事件頻率
Loss Event Frequency, LEF #

在一定時間範圍內，威脅對資產造成傷害的可能頻率。

損失規模
Loss Magnitude, LM $

由損失事件導致的損失可能的規模。(使用六種損失形式分析)

威脅事件頻率
Threat Event Frequency, TEF #

在一定時間範圍內，威脅對資產造成傷害的可能頻率。

接觸頻率
Contact Frequency, CF #

在一定時間範圍內，威脅對資產造成傷害的可能頻率。

行動機率
Probability of Action, POA %

在一定時間範圍內，威脅來源與資產接觸的可能頻率。有三種類型，分別是定期、隨機和蓄意的。

漏洞/弱點
Vulnerability, VUL %

威脅事件成為損失事件的概率，也被稱為敏感性(Susceptibility)

威脅能力
Threat Capability, TC %

在一定時間範圍內，威脅來源與資產接觸的可能頻率。有三種類型，分別是定期、隨機和有意的。

防禦強度
Resistance Strength, RS %

防禦強度指的是相關控制措施用來防禦作業上的弱点或漏洞的能力。

主要損失
Primary Loss, PL $

主要損失是由損失事件本身直接引起的，或者由於主要利害關係人對事件的反應而產生的。常見的主要損失形式包括：生產力損失、更換成本和應對措施。

次要損失
Secondary Loss, SL $

次要損失是由於次要利害相關人（外部方）對損失事件的反應而引起的，進一步對主要利益相關者造成損失。

次要損失事件頻率
Secondary Loss Event Frequency, SLEF %

在一定時間範圍內，預估次要損失影響資產的可能頻率百分比。(又稱: 次要風險)

次要損失規模
Secondary Loss Magnitude, SLM $

代表因應次要利害相關人行動可能引起的預期損失。

六種損失的型態

生產力損失
由於運營無法交付產品或服務而導致的損失

- 網路交易平臺無法提供服務
- 員工無法登入系統進行日常作業
- POS機無法正常運作

風險處理(回應)成本損失
涉及處理(回應）風險事件的成本相關的損失

- 員工因為風險事件，需要加班的成本也需要納入考量
- 數位鑑識
- 通知受影響者
- 安全培訓和意識提升

更換成本損失
組織因需更換資產而產生的損失

- 更換受感染的硬件
- 軟體更新或升級
- 恢復和重建系統

競爭優勢損失
因智慧產權或其他關鍵競爭差異因素被損害而導致的損失

- 專利技術外洩 / 產品設計被竊取 / 企業機密泄露

罰款和裁判損失
因民事、刑事或合同爭議而對組織處以的罰款或判決

聲譽損失
因外部利害相關者認為組織價值降低和/或其責任增加而導致的損失

- 股價下跌 / 客戶流失 / 市占率下降
- 合作夥伴關係破裂

當你導入 FAIR，會發生什麼？

- 國際公認的資安風險量化模型
- 高層、非科技/資通背景利害關係人、及財務單位更容易理解與支持資安決策。
- 合規與稽核準備效率大幅提升。

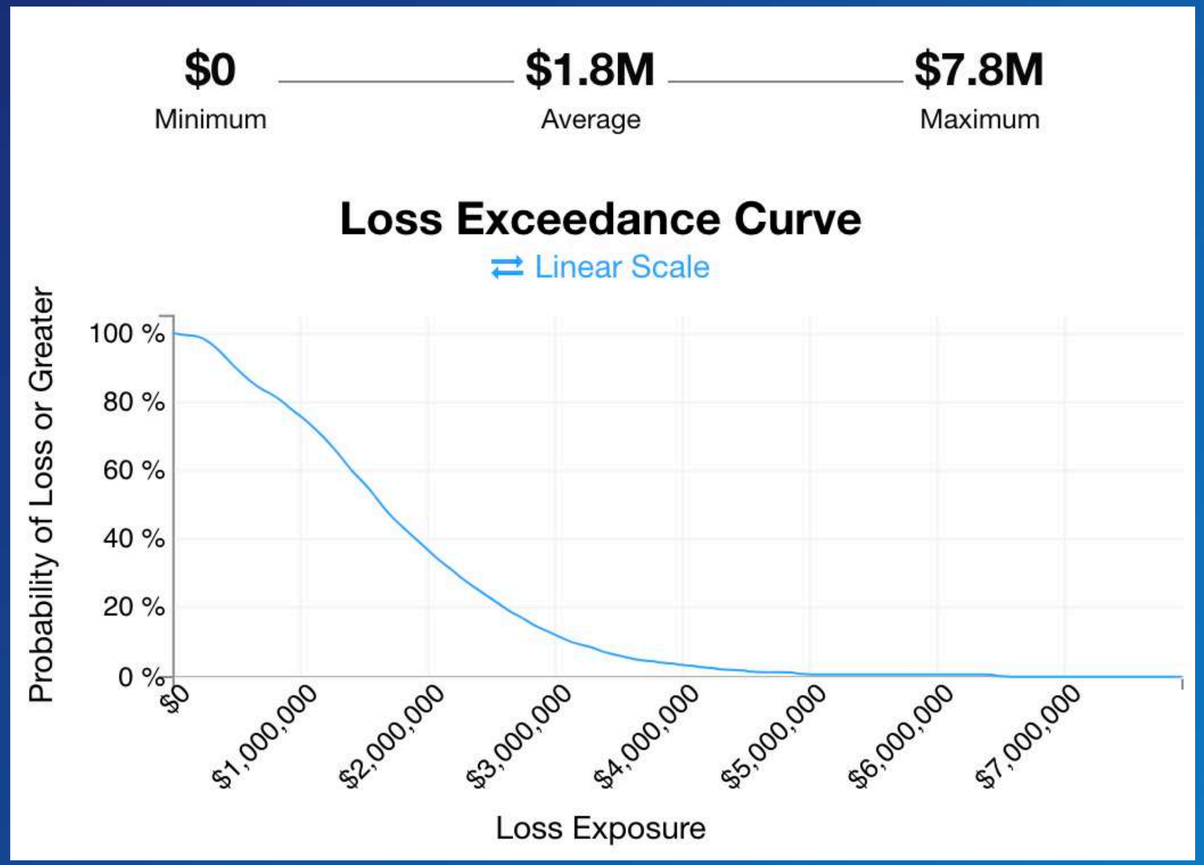
風險量化分析報告範例

- 根據我們目前獲得的資訊和我們風險專家的估計，每年預測會發生61.49個損失事件，每個事件的平均損失為120萬。
- Based on the information currently available to us and the estimates of our subject matter experts, 61.49 loss events are forecasted per year with an Average Per Event Loss of 1.2 M
- 風險改善控制成本為120萬
- 目前針對此類損失的資安風險保額為5千萬

資安風險納入經營決策考量
— 金融資安行動方案2.0

補充案例 是否需要投資資安工具

(投資前後比較) Annualized Loss Expectancy (ALE)年度損失期望值分析



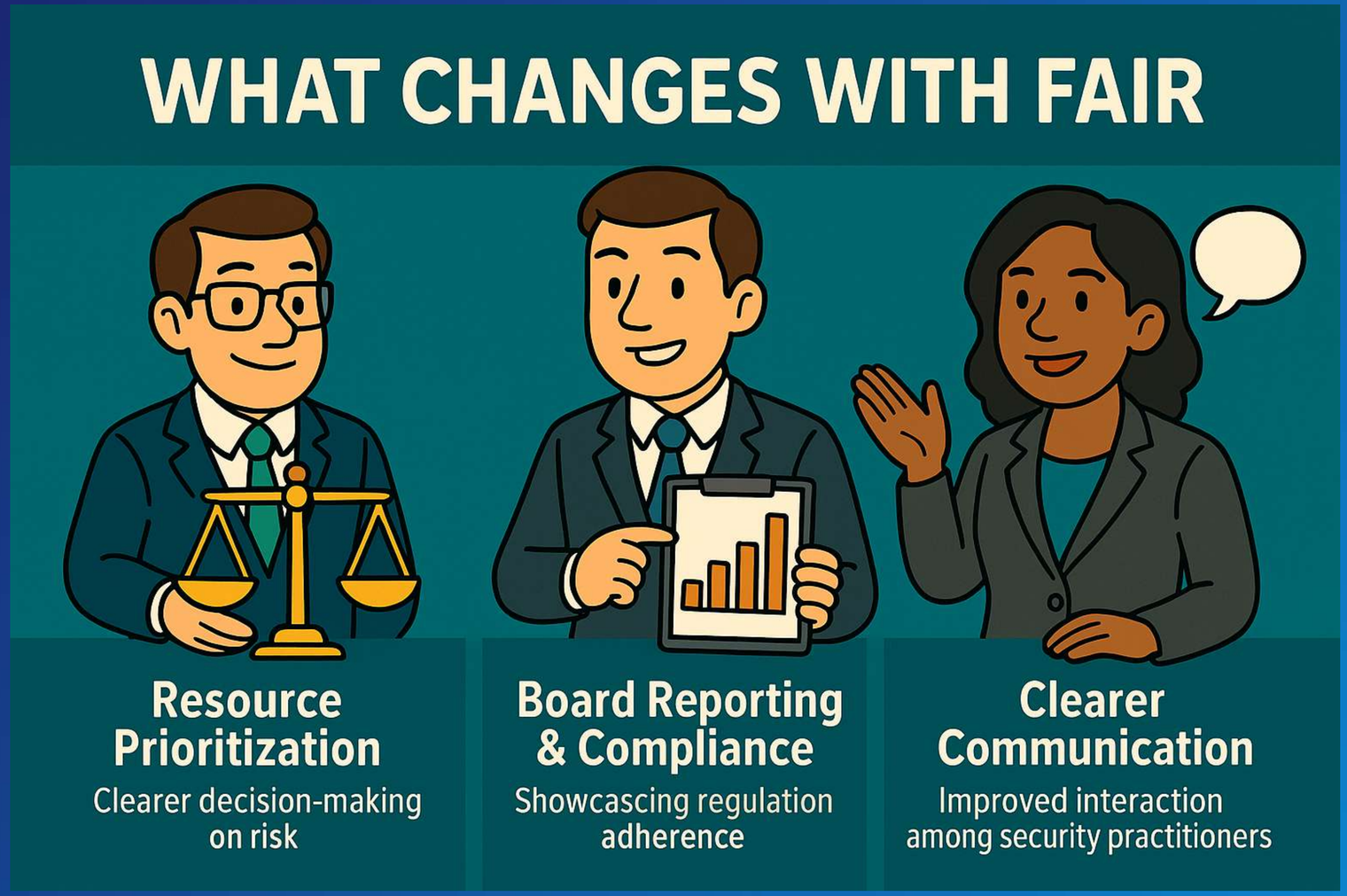
投資前

投資後

CISO 不必孤軍奮戰

- FAIR CRQ 並非取代 CISO 經驗，而是放大其價值。
- 是時候從「合規導向」轉向「決策導向」。
- 讓資安風險變得可衡量、可管理、有意義。

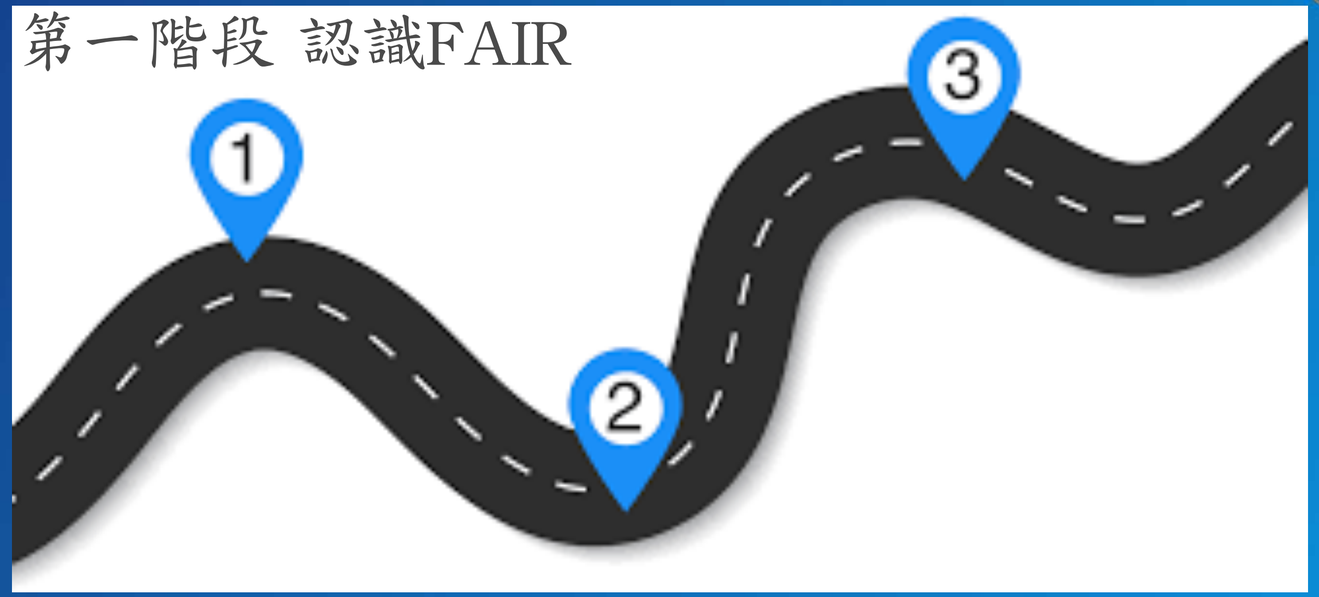
當你導入 FAIR，實際改變會是什麼



- 讓數據取代恐懼，驅動精準決策
- 從無序到聚焦，高效配置資源
- 從繁亂到清晰，有效呈報風險
- 跨越技術藩籬，團結利害關係人

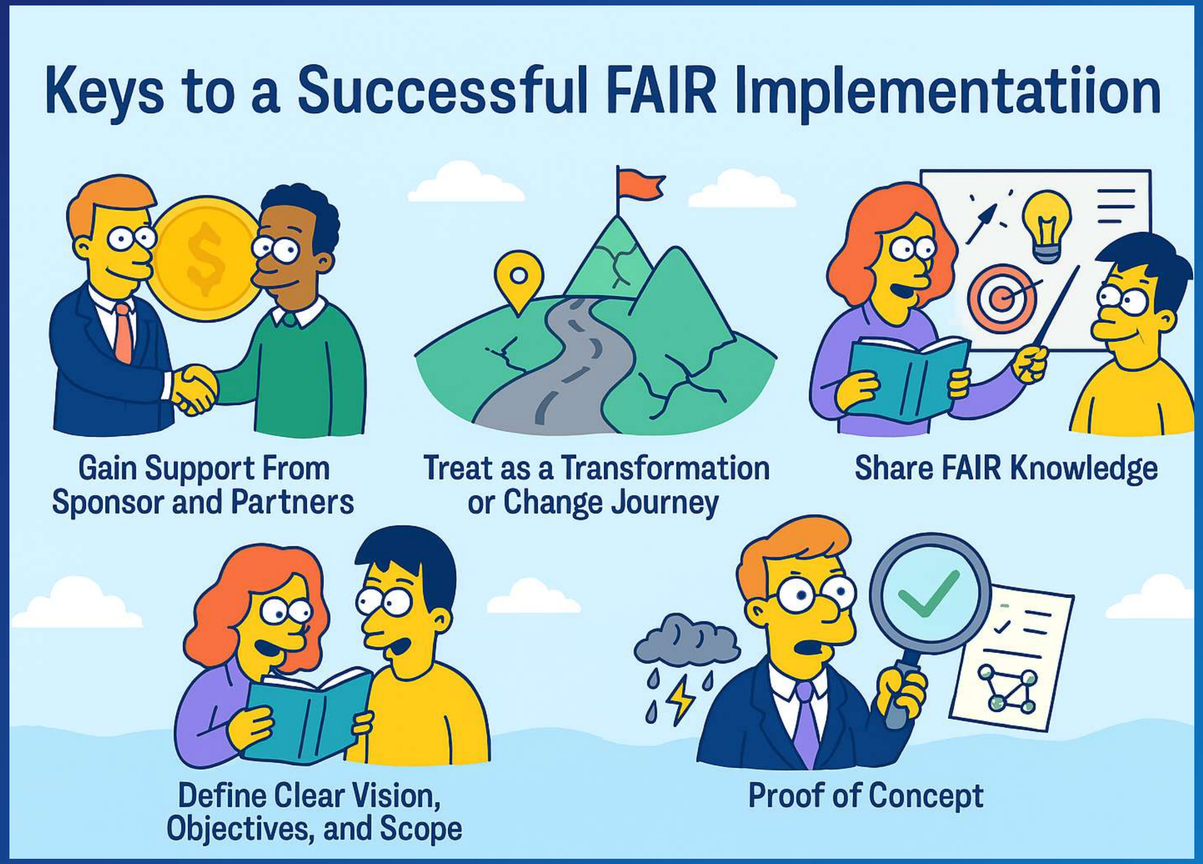
啟動FAIR 之旅的藍圖

第三階段 實施FAIR



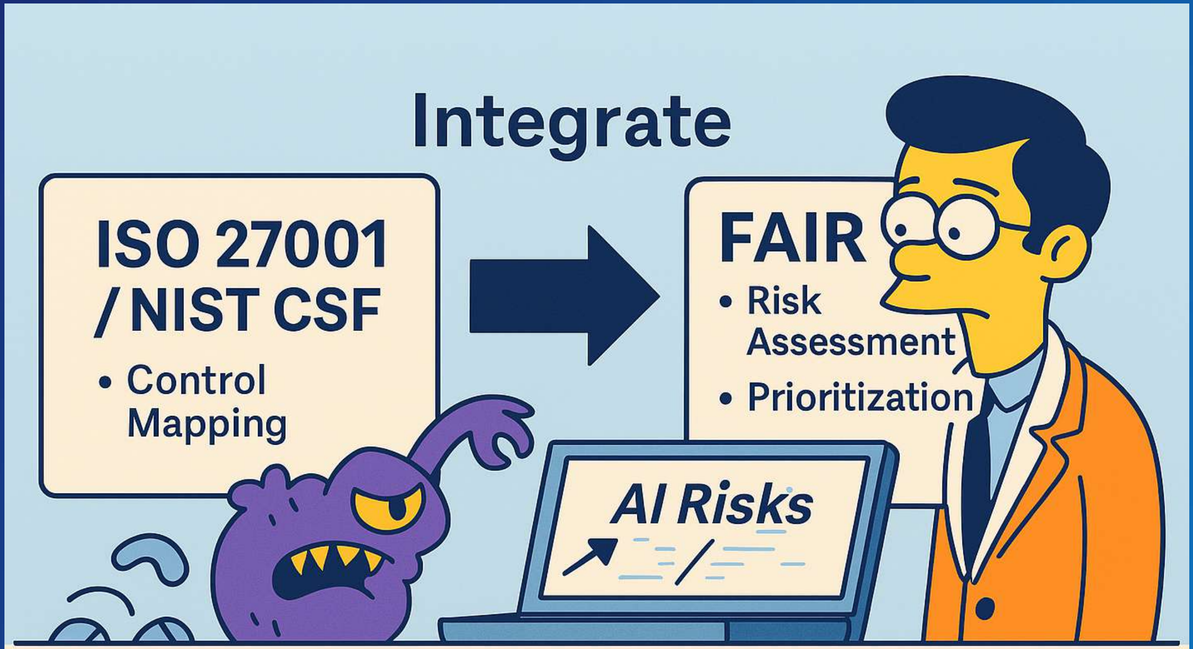
第二階段 整合FAIR

第一階段 認識FAIR CRQ



- 導入FAIR的成功關鍵要素獲得專案發起人(Sponsor)與專案夥伴們(Partners)的支持
- 將專案視為一場轉型(Transformation)或變革(Change)之旅
- 分享FAIR方法論及知識
- 定義清晰的願景、目標與範疇
- 可行性驗證 (Proof of Concept)

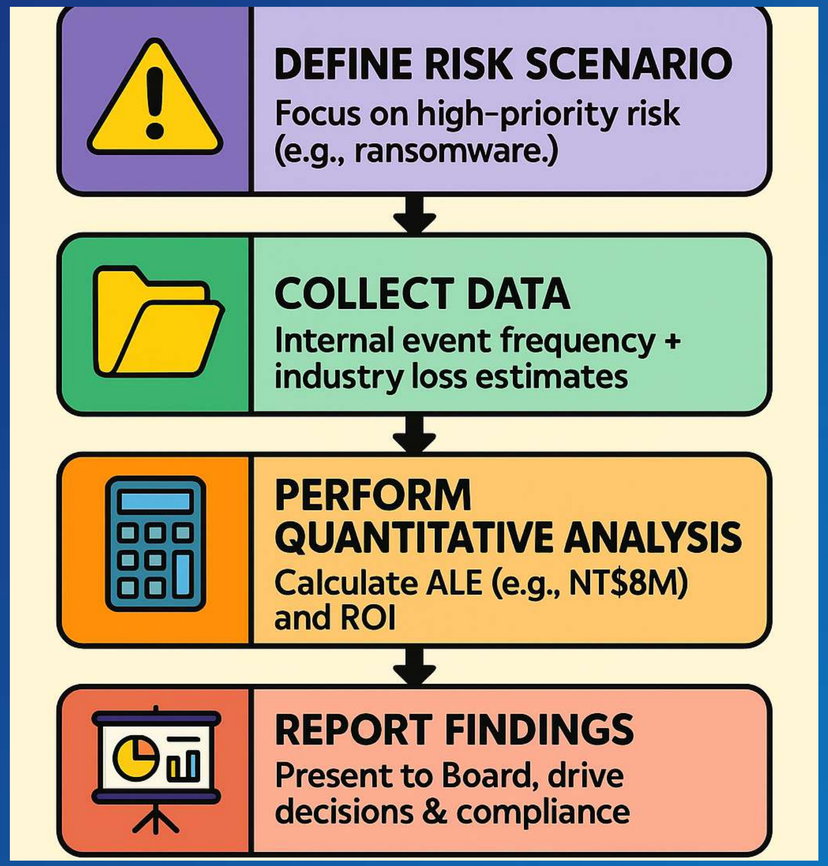
第二階段 與現有框架整合



在不改變既有資安治理架構的基礎上，將 FAIR 方法論嵌入 ISO 27001、NIST CSF 等主流程中，強化其在風險量化、優先排序與資源配置上的執行力。

FAIR 不僅補足傳統風險評估主觀與模糊的問題，也讓資安團隊能更有效地與業務與高層對話，形成策略驅動的風險治理文化。

第三階段 實施FAIR



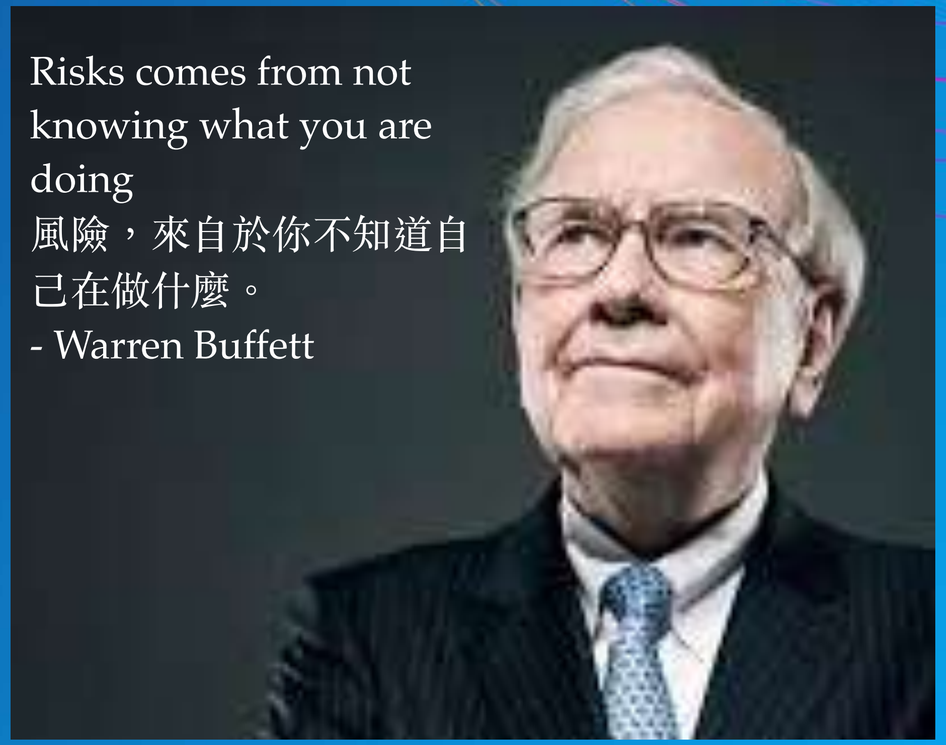
定義風險情境: 聚焦高優先風險（如勒索軟體）

收集數據: 內部事件頻率+行業損失估計

進行量化分析: 計算ALE（如800萬台幣）與ROI

報告成果: 呈報董事會，驅動決策與合規

下一步，由你啟動
讓數據取代恐懼、讓 FAIR 引領決策



下一步，由你啟動(續)

加入FAIR社群

加入台灣FAIR社群

加入FAIR台灣

FAIR 總會

加入FAIR總會

學習FAIR相關知識

FAIR教材

FAIR官方教材

官方資源

FAIR官方資源

近期相關教育訓練 (英語)

線上研討會（1)

線上研討會(2)

線上研討會(3)

相關資源 (續)

FAIR CRQ 顧問服務與CRQ工具

- C-Risk (歐洲/美國)
- Ostrich (美國)
- Kovrr (以色列)
- 歐洲KPMG

FAIR CRQ 教育訓練機構

- FAIR總部實體課程 (於美國舉行, 英文授課)
- C-Risk線上與實體課程 (線上課程為英文授課，預計於2025年提供中文字幕)
- 台灣企業風險治理暨量化分析協會 (目前全球第一及唯一中文實體課程提供單位)

台灣企業風險治理暨量化分析協會活動與教育訓練

- 亞洲區資通風險計量分析線上研討會(英文活動)
  - Cyber Risk in Context: A Data-Driven Approach to Risk Management 24 Apr 2025 (link)
  - Modeling and Measuring Cyber Risk: A Data-Driven Approach to Risk Management 15 May 2025 (link)
  - Optimizing Cyber Insurance: A Data-Driven Approach to Risk Management: 12 Jun 2025 (link)
- 內控三道防線與建構Tech/Cyber Risk Governance框架及專責單位教育訓練

台灣企業風險治理暨量化分析協會姊妹協會

- FAIR 歐洲分會 (FAIR European Chapter)