ISACA 網路安全白皮書

審視威脅建模

國立臺北科技大學
副教授兼計網中心主任
魏銷志 博士
CISSP, CISA, CISM, CRISC, CDPSE

在網路風險持續升級的時代，威脅建模是企業保護關鍵資產、維護聲譽與市場地位的實用方法。本白皮書由 ISACA 發布，探討如何以結構化、主動式的方法識別、評估並緩解網路威脅。

魏銷志 副教授

✓ **專長：**

金融資訊安全、**醫療資訊安全**、**低軌衛星安全**、**資料保護**、**人工智慧安全**、資訊安全管理、**資安與個資風險管理**、車載網路安全、營運持續管理

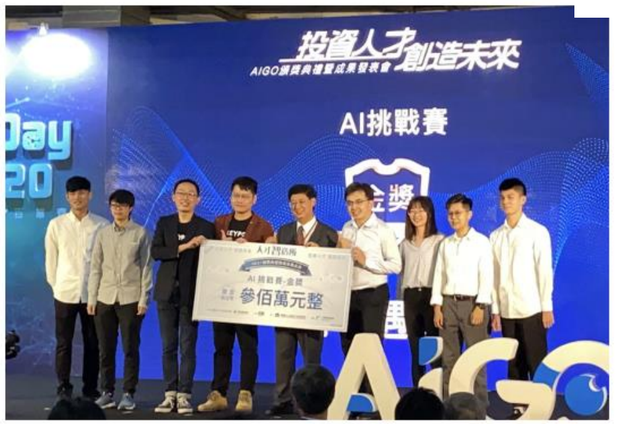
✓ **主任, 計算機與網路中心**, 國立臺北科技大學
副教授, 資訊與財金管理系/資安學位學程

- **常務理事**, 台灣數位鑑識發展協會 (ACFD)
- **監事**, 中華民國資訊安全學會(CCISA)
- **理事**, 中華民國醫療資訊學會(TIMA)
- **理事**, 臺灣亞太監理科技協會(ARTA)
- **理事**, 台灣電子健康學會(TEHA)
- **秘書長, 台灣數位鑑識發展協會 (ACFD)**
- **副秘書長, 中國民國資訊管理學會(CSIM)**
- **理事/監事, 中華民國電腦稽核協會 (CAA)**
- **理事, 全球區塊鏈策略暨應用發展協進會**

✓ **資安證照:**

- CISSP, CISA, CISM, CRISC, CDPSE, CEH, CHFI, CEI
- Lead Auditor: ISO27701, ISO27001, ISO20000, BS10012, BS25999
  ISO27018/29151, IEC 62443-2-1

(ISC)2 2017「資深資訊安全專家」



2020 AiGO挑戰賽金獎(300萬)

2022 IMA 2022傑出資訊教師

2023 資料去識別化與重新識別攻防競賽 第二名

在LEO安全GMO Cybersecurity by Ierae與電信技術中心積極合作

歡迎報考**北科大資財所碩博士、資訊安全碩博士學位學程**

目錄

01

威脅建模的價值

威脅建模是指企業以攻擊者的思考方式，
系統性評估其架構、系統與資產的過程。

威脅建模

主動預測

在漏洞被利用之前，先行識別潛在攻擊路徑

結構化分析

從對抗角度解析業務系統、資料流與營運流程

風險配置

依據風險優先級合理配置資源，做出有根據的安全決策

被動應對的代價

許多企業僅採取最低限度的防護，直到漏洞被利用、造成財務損失與聲譽損害後才著手解決。威脅演進速度遠超應變能力，被動策略已無法應對現代威脅。

主動建模的價值

威脅建模整合了**預見性、風險優先排序與可執行的控制措施**，保護客戶資料、專有技術與營運持續性，同時使安全工作與業務目標保持一致。

02 威脅建模的五個步驟

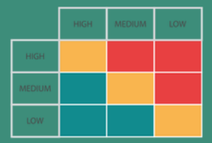
1. 確定業務目標並定義威脅建模範圍
2. 繪製商業生態系圖
3. 識別並確定威脅的優先級
4. 制定緩解策略
5. 審查、驗證與迭代

執行重點

- 確認業務目標
- 關鍵資產
- 利害關係人
- 盤點外部依賴

執行重點

- 建立流程圖
- 識別資產
- 信任邊界
- 評估外部依賴



執行重點

- 威脅分析
- 風險評估
- 優先排序

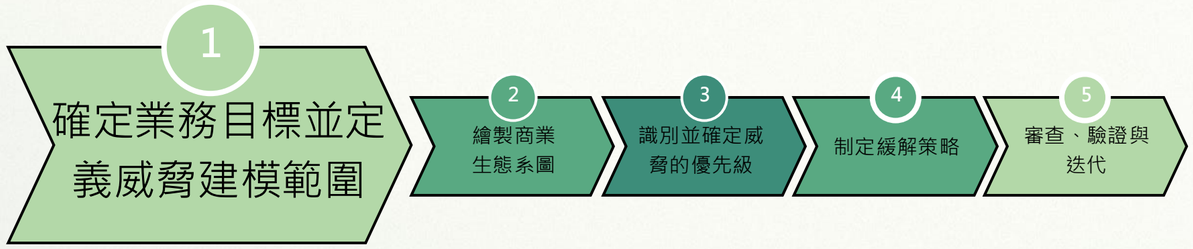
執行重點

- 設計控制措施
- 分配責任
- 規劃資源

執行重點

- 定期審查
- 模擬測試
- 更新模型
- 管理層報告

02 威脅建模的五個步驟



確定業務目標並定義威脅建模範圍

執行重點

- **確定商業目標**：如市場擴張、營運效率、客戶信任
- **界定範圍**：關鍵業務流程、資產與策略性舉措
- 與領導階層合作，確保支援公司優先事項
- 記錄範圍，包含利害關係人與外部依賴關係（供應商、第三方服務）

產出

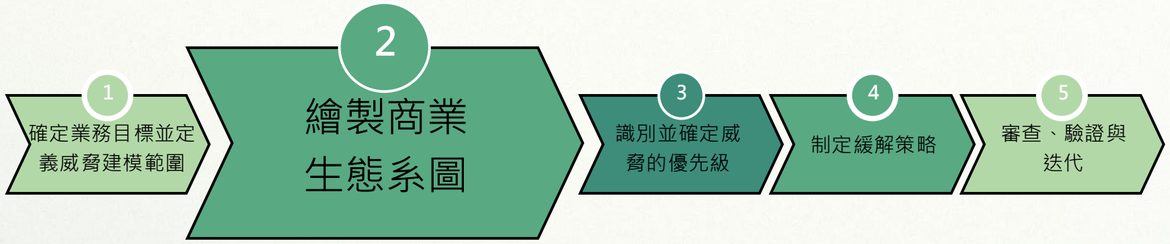
明確闡述企業正在保護什麼以及為什麼保護，並獲得領導層支持，將安全作為策略推動因素優先考慮

範例

金融機構確立了**提高獲利能力**和**確保隱私合規**的目標

金融機構將威脅建模範圍定義為：保護網路銀行平台與交易資料，免受勒索軟體與資料外洩侵害

02 威脅建模的五個步驟



繪製商業生態系圖

視覺化關鍵流程

以流程圖呈現採購、銷售等流程，標明輸入、輸出及與外部實體的互動

識別關鍵資產

標明專有資料、實體基礎設施及員工專業知識等需保護的核心資產

明確信任邊界

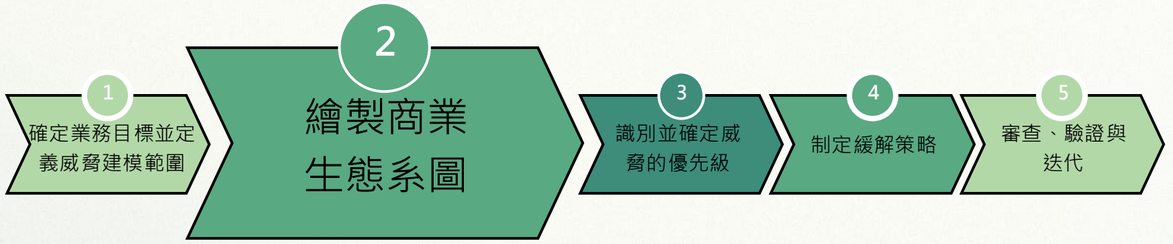
界定內部部門與外部合作夥伴之間的控制邊界，標示控制力減弱之處

評估外部依賴風險

評估雲端服務、第三方資料供應商的供應鏈風險，確定緩解優先順序

例如： 第三方資料供應商、開源模型庫（例如 Hugging Face）或雲端服務提供者（例如 AWS、Azure）

02 威脅建模的五個步驟



產出

繪製出一幅全面的商業生態系統地圖，重點介紹容易受到威脅的資產、流程和邊界

範例

金融機構為其網路銀行平台建立了人工智慧 (AI) 詐欺偵測系統架構圖

- 資料流程圖視覺化了雲端推理伺服器處理的交易資料輸入
- 基於專有資料集訓練的 AI 模型

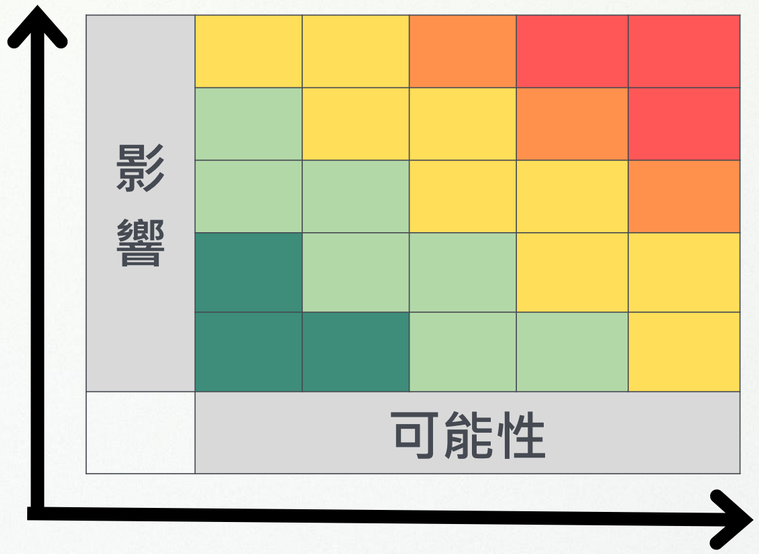
關鍵資產包括 AI 模型和推理伺服器。伺服器與第三方雲端服務供應商之間設定了信任邊界。

團隊會評估雲端服務供應商的供應鏈風險，並按季度審視架構圖，以應對新的資料來源並識別風險，例如雲端邊界的資料外洩

02 威脅建模的五個步驟

1 確定業務目標並定義威脅建模範圍 → 2 繪製商業生態系圖 → 3 識別並確定威脅的優先級 → 4 制定緩解策略 → 5 審查、驗證與迭代

識別並確定威脅的優先級



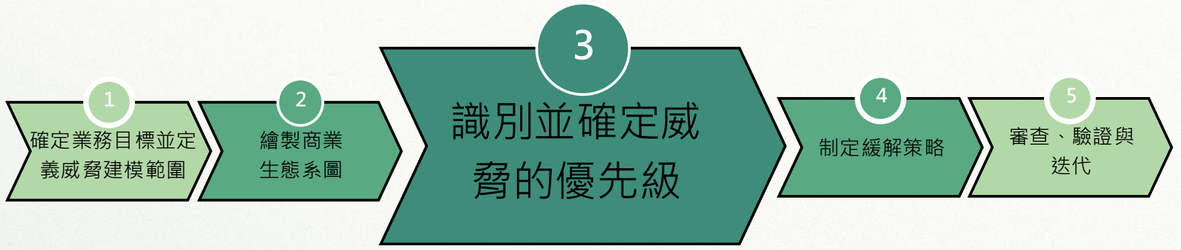
評估方法

- 與營運、財務、法務部門進行跨職能腦力激盪
- 使用 STRIDE 等成熟框架作為風險分類指引
- 以定性風險矩陣（可能性 × 影響）進行系統性評估
- 優先考慮可能破壞策略目標或造成重大財務、法律或聲譽損害的威脅

- ***STRIDE:*** *Spoofing (欺騙)、Tampering (篡改)、Repudiation (否認)、Information Disclosure (資訊洩漏)、Denial of Service (阻斷服務)、Elevation of Privilege (特權提升)*
- ***DREAD:*** *Damage (破壞性)、Reproducibility (再現性)、Exploitability (可利用性)、Affected Users (受影響用戶)、Discoverability (可發現性)*
- ***PASTA (Process for Attack Simulation and Threat Analysis)***
- ***OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)***
- ***VAST (Visual, Agile, and Simple Threat modeling)***

成果：根據影響、可能性與策略目標對威脅進行排名，並提供明確的排序理由。

02 威脅建模的五個步驟



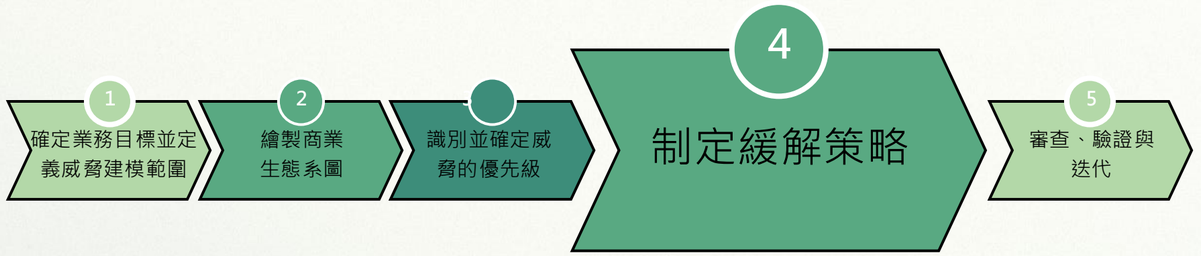
產出

根據影響(例如，經濟損失、隱私洩漏)、可能性和策略目標對威脅進行排名，並給出排名的明確理由

範例

一旦識別出企業的高優先級威脅，就會根據資料面臨的風險暴露可能性（頻繁的資料更新）和影響（財務損失、隱私洩漏）對資料進行排序。這樣就可以確定緩解策略的優先順序

02 威脅建模的五個步驟



制定緩解策略

指定風險負責人
為超出風險承受能力的威脅指派負責人，確保系統性風險管理責任落實

制定分層應對措施
針對高優先級威脅，整合加強防護、補償性控制措施及教育培訓

平衡成本與效益
優先保護關鍵資產，同時避免損害營運效率，集中資源於關鍵風險

建立風險因應策略
明確時間表、預算與責任方，將緩解措施融入企業既有流程

產出

一套切實可行的緩解方案，用於應對超出企業風險承受能力和容忍度的威脅和系統性風險。方案應明確責任歸屬，融入企業流程，並與策略目標一致

範例

- 金融機構在其詐欺偵測系統中實施資料驗證機制來**降低資料投毒風險**，但結果仍超出其隱私外洩風險承受範圍
- 部署了多雲冗餘來應對系統性雲端服務中斷

02

威脅建模的五個步驟

1 確定業務目標並定義威脅建模範圍
2 繪製商業生態系圖
3 識別並確定威脅的優先級
4 制定緩解策略
5 審查、驗證與迭代

審查、驗證與迭代

驗證威脅模型是否能夠應對新的風險或系統變更

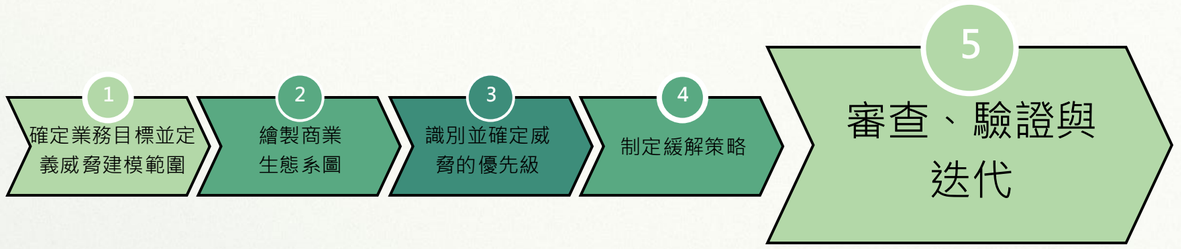
驗證模型對威脅和系統性風險的有效性

說明驗證結果、剩餘風險以及風險偏好的一致性

反映新的策略措施、市場狀況或新出現的威脅

02

威脅建模的五個步驟



產出

隨著業務發展而不斷演進的動態威脅建模流程，確保策略目標的持續保護

範例

- 某企業在 2025 年 5 月整合新的**交易資料集**後，**對其詐欺偵測系統的威脅模型進行了審查**
- 針對**模擬攻擊測試了資料驗證**，並**更新了多雲冗餘機制**以應對潛在的雲端服務中斷
- 安全工程師驗證各項控制措施並**確保合規性**，並將結果報告給管理階層

03 威脅建模的成功關鍵

利害關係人參與

明確各部門的角色與責任

培養安全意識與風險文化

將威脅建模納入企業日常流程

連結技術風險與業務目標

幫助 IT、資安與管理層建立共同決策基礎

充足資源分配

平衡安全需求與業務目標。

高階主管治理

制定安全策略與願景

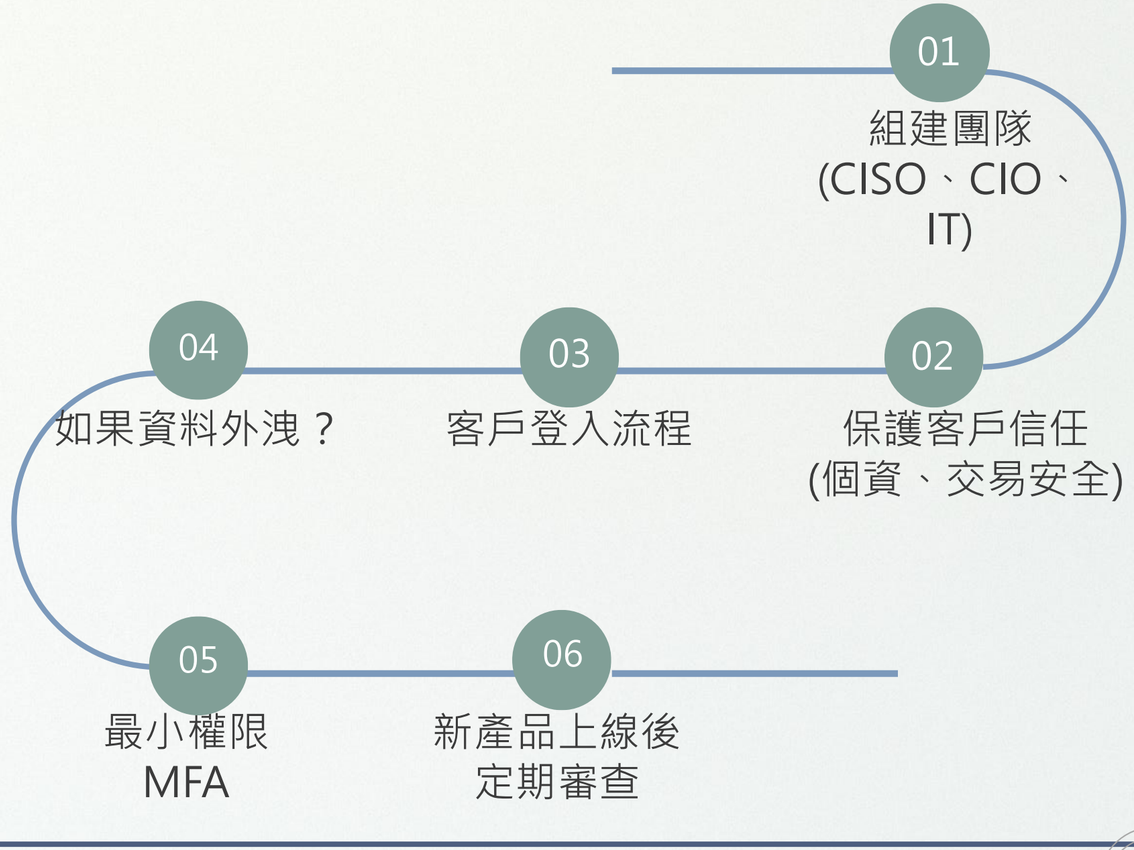
從案例中學習

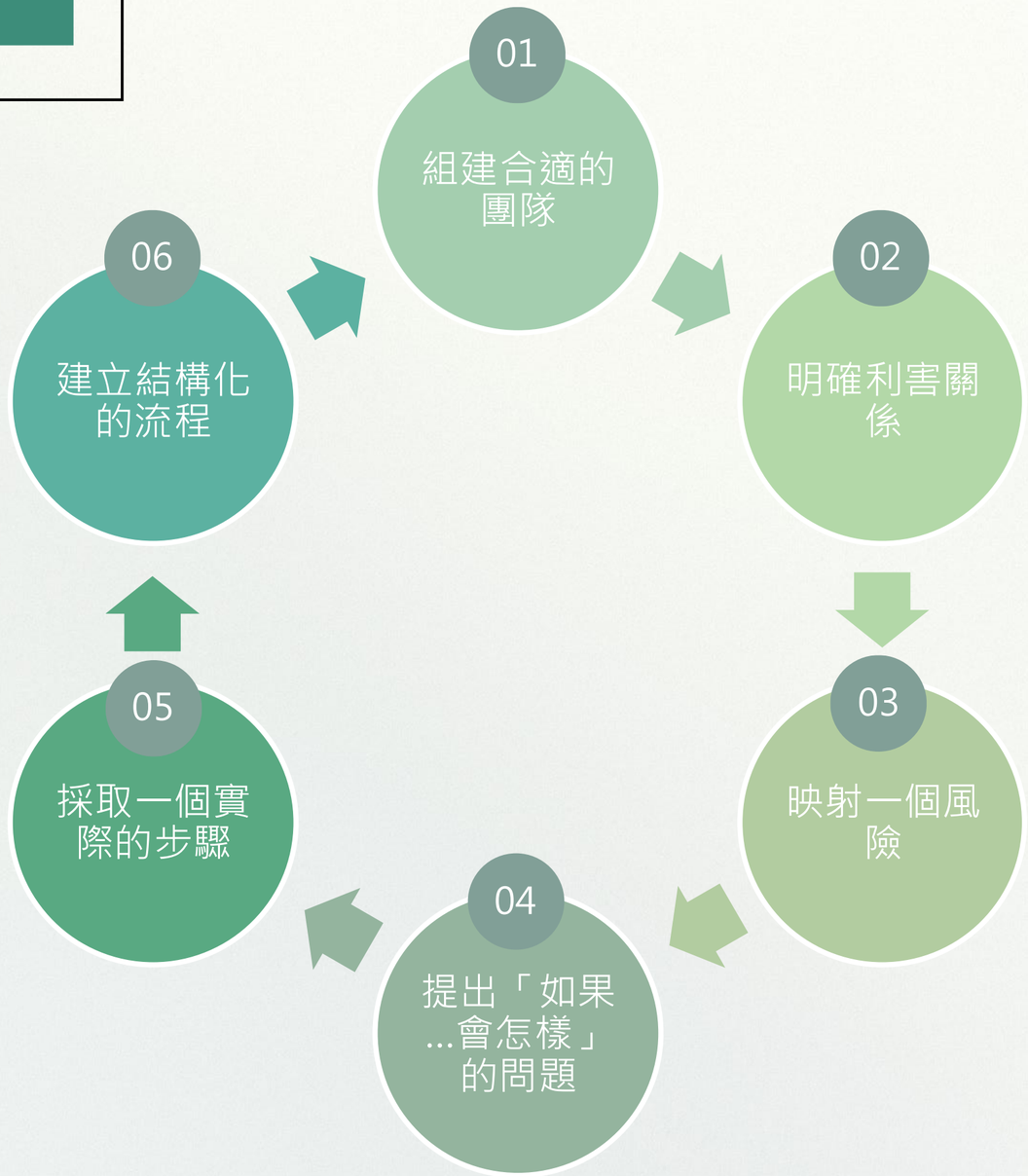
使用真實資安事件進行桌面演練

任何威脅建模練習都需要利害關係人的參與和充足的資源投入

04 讓高階主管團隊參與威脅建模

情境模擬：網路銀行客戶登入





05 CISOs 和 CIOs的三項實施策略

將風險納入 CISO 策略

- CISO 應識別主要網路威脅
- 根據業務影響排列優先順序
- 將資源集中在最嚴重的風險

CIO 安全導入新技術

- CIO 負責導入 AI、IoT、雲端等新技術
- CISO 應協助進行風險檢查

CISO 與 CIO 協同建立韌性

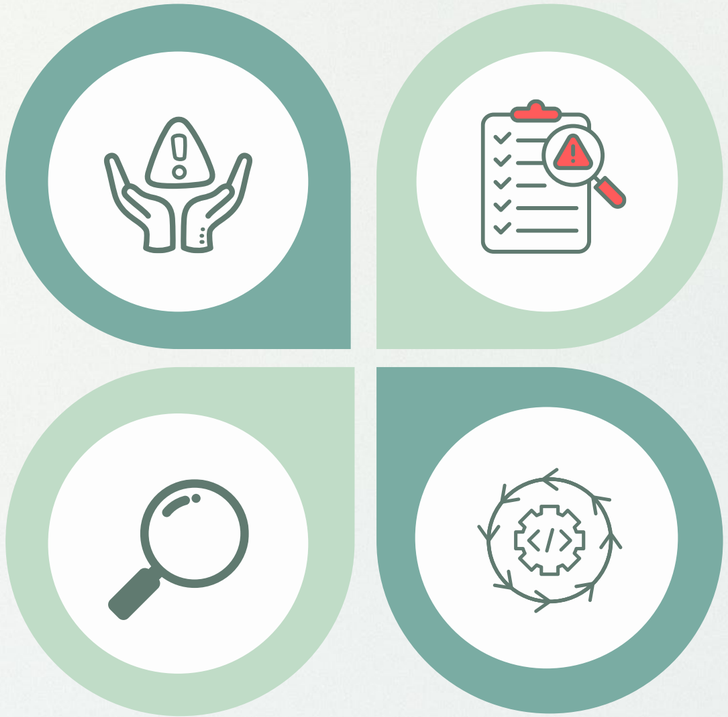
- 共同主持風險討論
- 目標是建立可操作的安全路線圖

06 威脅建模的實施

四項實施策略

01. 小處著手保持專注

- 不要一次分析所有系統
- 選擇**高風險**、**高衝擊**的系統開始



02. 聚焦真正威脅

- 不需要列出所有的漏洞
- 優先處理可能性高、影響大且可以修復的風險
- 可使用 STRIDE、PASTA、MITRE ATT&CK 等方法

03. 風險轉化為解決方案

- 透過預防、偵測、復原三層機制
- 將主要風險轉化為可執行的行動方案

有效的威脅建模不僅是識別問題，還包括制定可行的、優先排序的修復方案，從而保護業務

04. 實施持續威脅建模

- 定期（至少每月）審查威脅模型
- 於重大變更後立即更新

07 產業威脅建模

各行業的風險優先順序:

銀行	醫療保健	零售
防範詐欺	保護 PHI	購物車安全
保護 API	電子健康紀錄	付款系統
確保交易完整性	符合 HIPAA	

威脅建模不能一體適用，需依產業客製化

明確合規性要求（PCI DSS、HIPAA、SOC2）有助於根據行業定制威脅建模，並確保與 NIST 及 CIS 框架保持一致

08 結論：從被動應對到主動防禦

威脅不會等待最佳時機。忽視風險的代價遠大於應對風險

企業無需徹底改革營運模式——目標明確，而非複雜化，是成功的關鍵

1 從小處著手

選擇一個系統，召集合適人員，繪製資料流程

2 逐一解決

優先處理最關鍵的威脅

3 持續演進

威脅建模融入常規治理，與業務變更保持一致

ISACA 網路安全白皮書

THANK YOU

歡迎報考**北科大資財所碩博士、資訊安全碩博士學位學程**

白皮書下載網址