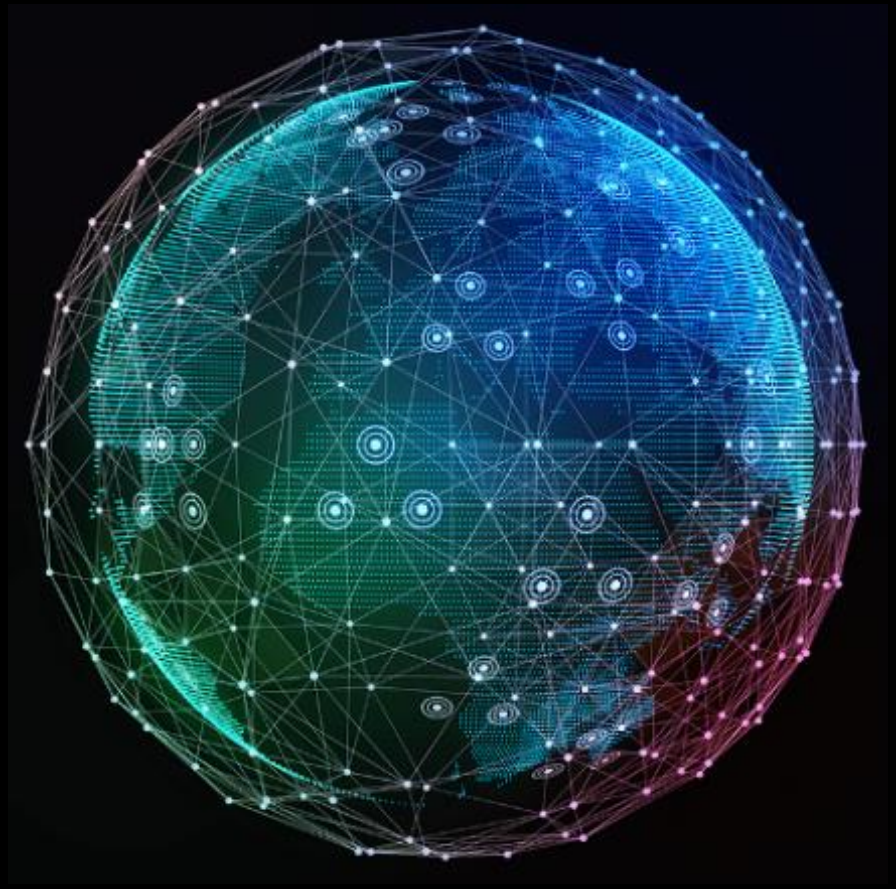
Deloitte.

勤業眾信



強化證券市場資安防禦策略

勤業眾信聯合會計師事務所 風險諮詢部門 2024/5 陳威棋

主講人

- 臺北市信義區松仁路100號20樓
- Tel : 022725- 9988 分機7807
- Fax: 4051- 6888 分機7807
- ikewchen@deloitte.com.tw

陳威棋

Ike W. Chen

資深執行副總經理

學歷：

輔仁大學資管系學士

中央大學資管系碩士

專業資格：

- 國際資訊系統資安專家(CISSP)
- 國際認證資訊安全經理人(CISM)
- 國際認證舞弊偵防師(CFE)
- 國際經濟犯罪鑑識調查員(CECFE)
- 國際網路犯罪調查員(3CI)
- 國際認證隱私保護工程師(CDPSE)
- 國際雲端安全知識認證(CCSK)
- 國際認證道德駭客(CEH)
- 國際網路安全認證師(CC)
- 國際認證電腦稽核師(CISA)
- 國際資安鑑識調查專家(CHFI)
- ISO/IEC 27001:2022 LA

陳威棋長期投入數位科技風險管理領域，擁有十多年豐富的資訊安全諮詢經驗，曾協助許多客戶進行資訊安全策略擬定並針對不同產業有豐富資安檢測經驗，包含政府單位、金融產業、高科技製造業及資訊科技產業等。

主要協助企業從公司風險治理的視角推動全面資安風險管理策略的制定，他所領導的團隊提供企業客戶有關主動式攻擊測試服務、資訊安全策略擬定、數位風險預警與防禦及資安事件危機管理等諮詢經驗。

經歷：

- 勤業眾信聯合會計師事務所　執行副總經理
- 勤業眾信資安科技與鑑識分析中心實驗室主管

參與專業組織：

- 全國認證基金會(TAF)鑑識科學技術類別技術委員會委員
- 台灣金融研訓院課程菁英講座
- 敏捷專家學會理事
- 中華民國電腦稽核協會課程講師
- 台灣舞弊防治與鑑識協會會員
- 國際高科技犯罪調查協會(HTCIA)會員
- 國際資訊系統安全核準聯盟(ISC2)會員
- 國際舞弊稽核師協會(ACFE)會員

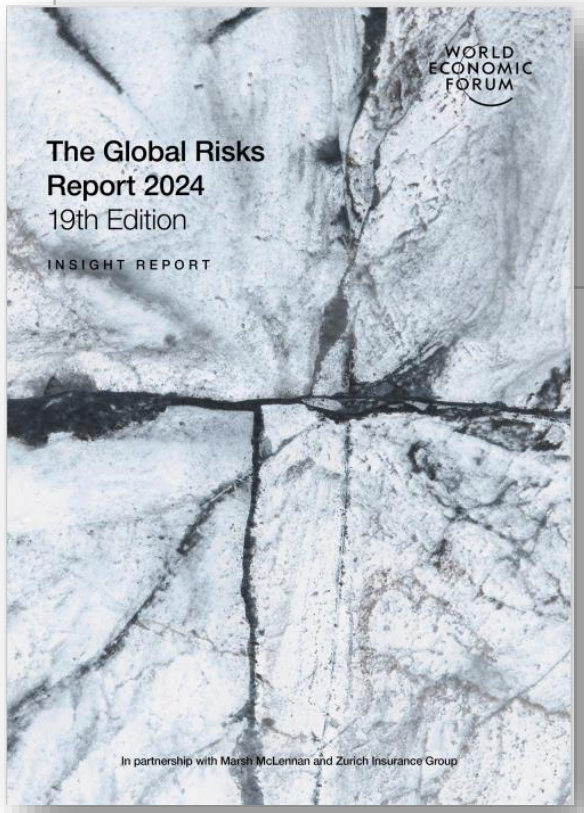
Agenda

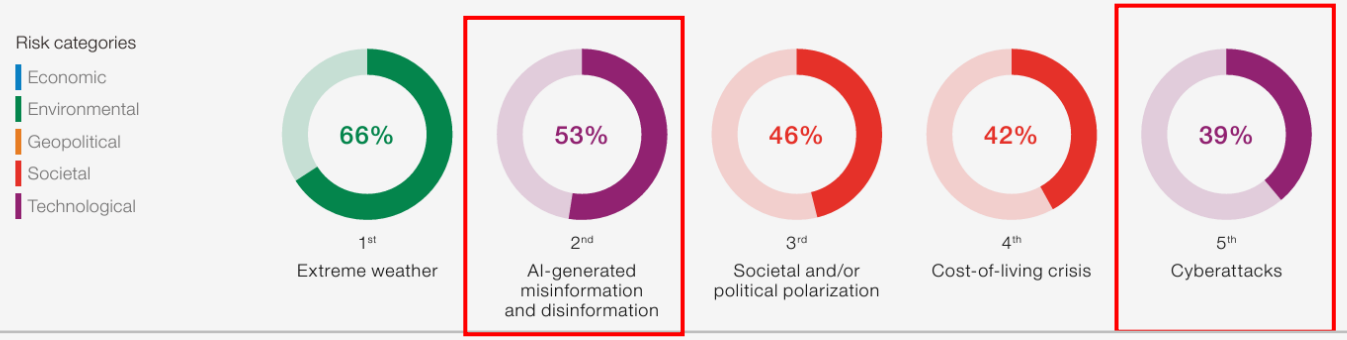
1. 全球資安整體趨勢說明
2. 以金融資安行動方案強化資安治理
3. 資安韌性強化策略
4. 問題與討論

全球資安整體趨勢說明

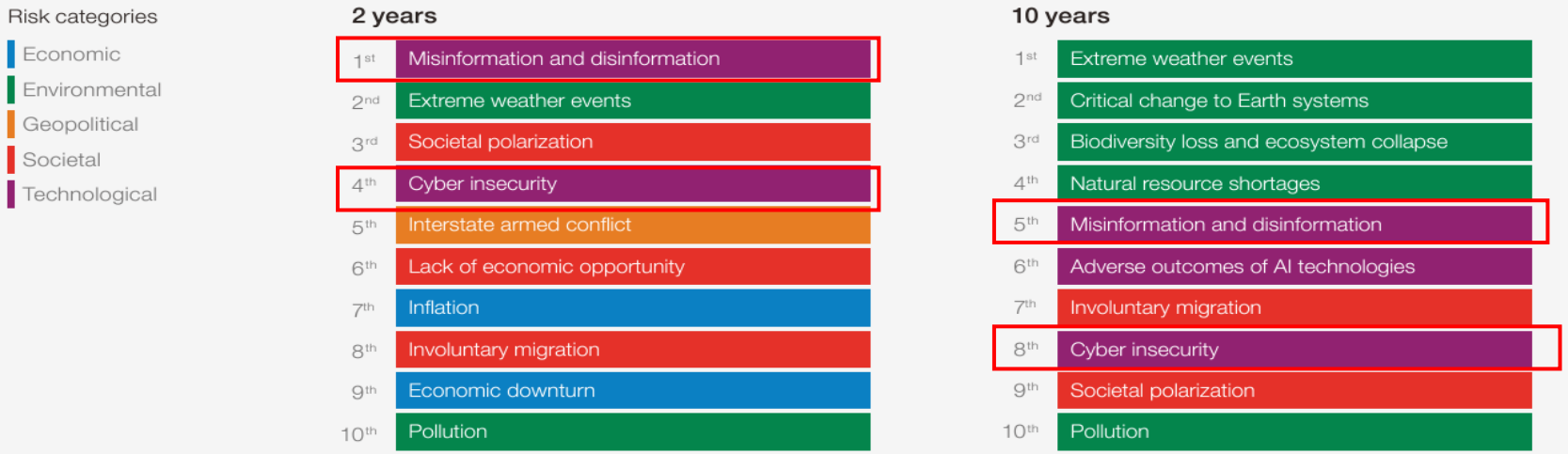
全球風險趨勢：全球經濟論壇(WEF)警示網路攻擊風險將持續對全球風險造成影響

世界經濟論壇（WEF）最新發表2024年全球風險報告，「人工智慧生成的錯誤資訊和虛假資訊」和「網路攻擊」被列 為 2024 年將對全球範圍引發重大危機的前 5 大風險。





長遠來看，「人工智慧生成的錯誤資訊和虛假資訊」和「網路攻擊」估計將持續被評估為對全球影響(嚴重)程度高的風險因子。



資料來源：World Economic Forum, The Global Risks Report 2024

Deloitte AI Institute 《生成式AI的現況：現在決定未來》
The State of Generative AI in the Enterprise : Now decides next

治理、管理人才與風險，是採用生成式AI上首要的挑戰

我們正處於由生成式AI引領重大科技轉型的早期階段，生成式AI的速度、規模及使用案例十分驚人。企業領導人正受到巨大的壓力要採取行動，期望變成業務成長的催化劑同時還要確保有適當的治理及風險緩減機制

調查橫跨了六個產業、16個國家，超過了2,800位CxO等級受訪者

79%

受訪組織表示，生成式AI將在不到三年的時間裡推動重大的組織轉型。

73%

受訪組織表示，已將生成式AI整合到產品開發及研發作業裡，並開始使用生成式AI於創新及成長的目的。

25%

組織對於應用生成式AI的治理及風險問題，具「高度」或「非常高度」的準備。

受訪者最擔心的AI治理及風險問題：

- 對治理結果缺乏信心（36%）
- 智慧財產權問題（35%）
- 濫用客戶及顧客資料（34%）
- 遵循法規之能力（33%）
- 缺乏可解釋性或透明度（31%）

人工智慧應用將重塑企業營運風險

人工智慧（AI）正變得越來越普遍，並引入了新的風險，風險面向包含公平性，透明度，信任和資訊安全及隱私。

人工智慧應用案例

- 智能客服
- 員工招聘
- 產品和服務的定價
- 信用評等決策
- 文件分析和圖像識別
- 智能理財
- 預測金融犯罪的風險

人工智慧風險

公平

- 偏見導致競爭劣勢
- 對具有共同特徵的人或群體持負面偏見

透明度

- 設計不當的 AI 而導致違規行為和聲譽損害
- 人工智慧結果無法有效明確進行解釋說明

正確性

- 錯誤的財務預測或破壞財務規劃的完整性

資訊安全及隱私

- 惡意非預期的機器決策導致對公司營運干擾
- 惡意網路入侵的風險增加
- 資料外洩

人工智慧風險帶來之影響

1

人工智慧出錯所造成聲譽之影響

人工智慧演算法所造成的不良結果，可能會引起社會大眾的強烈反彈並影響客戶忠誠度

2

圍繞人工智慧的監管要求持續提高

監管機構正在加重人工智慧應用審查之力度，並通過制定法規及自律規範來提高監管要求

3

高階管理層需要提前接觸 AI並了解風險

在組織內或透過第三方越來越多地採用人工智慧應用場景，但缺乏可視性和管理，導致未知和不明的弱點增加及風險暴露

金融業運用人工智慧(AI)之6項核心原則及對應監理理念

建立治理及問責機制 (負責任創新)

- 應對其使用之AI系統承擔相應之內外部責任(內部:指定高階主管負責AI相關監督管理並建立內部治理架構、外部:保護消費者隱私及資訊安全)。
- 應建立全面且有效的AI相關風險管理機制並定期評估及測試。
- 培養及增進人員對AI的知識、風險辨識及管理能力。

確保系統穩健性與安全性(強化資通安全)

- 金融機構在運用AI系統時，必須確保其系統之穩健性(robustness)與安全性，以避免對消費者或金融體系造成損害。
- 運用第三方業者開發或營運之AI系統提供金融服務，應對第三方業者進行適當之風險管理及監督、亦須針對第三方之責任範疇予以明定及要求針對AI相關運算規則並留存軌跡紀錄，俾利後續驗證與管理。

重視公平性及以人為本的價值觀 (公平待客及普惠金融)

- 使用AI系統之過程中，應儘可能避免演算法之偏見，所造成的不公平。
- AI系統之運用應符合以人為本及人類可控之原則。
- 生成式AI產出資訊，仍需由人員就其風險進行客觀且專業的最終判斷。

落實透明性與可解釋性(資訊揭露)

- 運用AI系統時，應確保其運作之透明性及可解釋性，理解AI如何做出決策，以確保對AI的運作之有效管理。
- 使用AI與消費者直接互動時，應適當揭露，並確保可解釋性的程度與其AI系統應用之重要性相稱。

保護隱私及客戶權益(金融消費者保護)

- 應充分尊重及保護消費者之隱私，並妥善管理及運用客戶資料，避免任何可能導致資料外洩之風險。
- 如運用AI系統向客戶提供金融服務，應尊重客戶選擇權利，並提醒客戶是否有替代方案。

促進永續發展(永續金融及關懷員工)

- 應確保其AI的運用策略與實施方式，應與永續發展原則結合，包括減少經濟、社會等不平等現象，保護自然環境，從而促進包容性成長、永續發展及社會福祉。
- AI系統運用過程中，宜對一般員工提供適當之教育及培訓，使員工能適應AI帶來之變革，尊重並保護一般受僱員工的工作權益。

企業應對策略：參酌國際相關人工智慧風險管理框架

勤業眾信根據ISO/IEC 42001、NIST AI RMF、 NIST AI RMF Playbook等框架，評估管理流程與技術層面的風險控制

國際標準化組織(ISO)

ISO/IEC 42001 Artificial intelligence Management system

規定組織範圍內建立、實施、維護和持續改進人工智慧管理制度的要求和指導。在這一標準指導下，組織能夠在滿足相關法規要求與相關協力廠商能負責任地開發或使用AI系統，並實現其目標。

美國國家標準暨技術研究院（NIST)

Artificial Intelligence Risk Management Framework (AI RMF 1.0)

NIST AI RMF該框架由美國國會指示NIST制定，目的是要提供設計、開發、部署和使用人工智慧系統的指南，降低應用人工智慧技術的風險。NIST也發布AI RMF Playbook，從中指導組織使用該框架的方法。

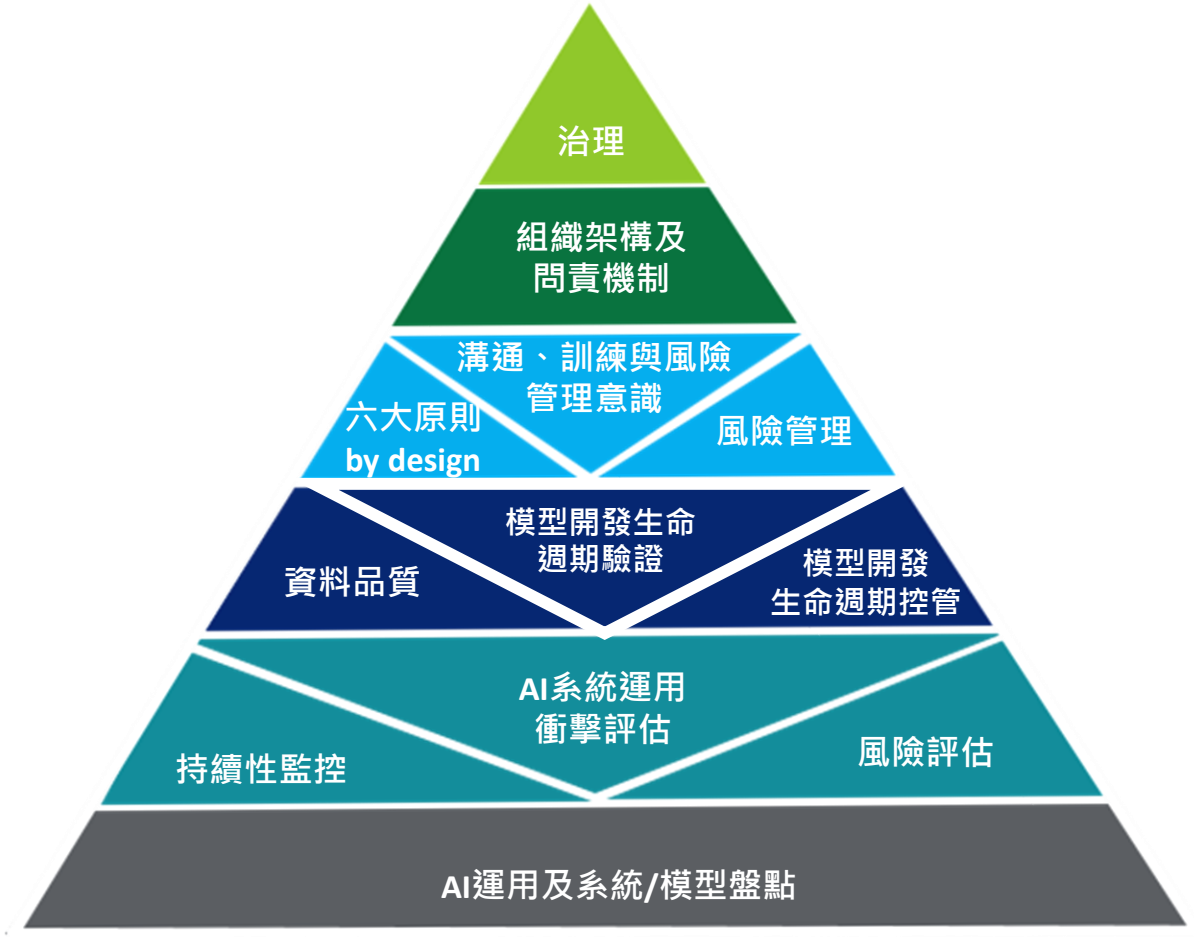
美國網路安全暨基礎架構安全署(CISA)及英國國家網路安全中心(NCSC)

Guidelines for Secure AI System Development

發表《安全AI系統開發指引》，從設計階段強化系統安全性，提供AI系統開發的必要建議，並彰顯開發AI系統，應遵循安全設計（Secure by Design）的原則，以防範可能的資安風險/

組織需有一完整從上而下的管理控制措施 - 建立人工智慧風險治理框架

依照「金融業運用人工智慧(AI)之核心原則及相關推動政策」、「金融機構運用人工智慧(AI)指引草案」、「金融機構運用人工智慧技術作業規範」，建立AI風險管理架構，包括以下關鍵要素：



第一層　治理

設立一個穩固的起始點，決定AI風險治理政策與以風險為基礎的AI管理機制。

第二層　組織架構及問責機制

要有效實施AI運用之風險管理策略，就需有紀律的組織結構。這一層包括人員的職責與如何證明合規。

第三層　組織文化與AI風險管理意識

在組織中建立AI基本概念及運作方式、高度的AI風險管理意識，確保組織的員工瞭解並遵循規則。

第四層　模型開發生命週期與資料品質

確保AI運用在組織策略框架下得到有效保護、管理和有效利用。如，盤點及風險管理機制、第三方業者監督管理、AI模型安全開發管理、資料品質、AI運用指引。

第五層　以風險為基礎的AI合規分析

將六大原則概念嵌入組織中。在構思新或更改產品或服務時，以風險評估產品及服務的遵循現況。

第六層　AI運用系統/模型盤點

AI運用及模型盤點是AI風險管理策略最基本的要素。包含有關組織的AI技術運用活動的所有必要資訊，例如對人、社會影響和風險分析。

以金融資安行動方案強化資安治理

臺灣金管會金融資安行動方案

願景

- 確保金融系統穩定安全，提供民眾安心交易環境
- 保護消費者金融資產及個人資料
- 提供多元便捷的金融服務

目標

- 建立業者重視資安的組織文化
- 提升業者資安治理能力與水準
- 確保系統持續營運與資料安全

策略

以風險為導向的資安監理、以整體為核心的資安治理、以演練為實證的資安韌性、以信任為基礎的資安聯防

推動策略、具體措施與精進措施

強化資安監理

型塑金融機構重視資安的組織文化、完備資安規範、強化資安監理職能、加強金融資安查核。

1. 擴大資安長設置
2. 定期召開資安長連繫會議
3. 建立網路身分驗證與業務風險對照
4. 強化第三方服務提供者風險評估與管理

深化資安治理

加強資安管理、強化資安監控、加強資安人才培育。

5. 推動導入國際資安管理標準
6. 推動資安監控機制及有效性評估
7. 鼓勵配置多元資安人才，提升攻防演訓量能
8. 鼓勵零信任網路部署

精實金融韌性

增進營運持續管理量能、加強資安演練、建構資料保全機制。

9. 鼓勵對外服務之營運持續演練
10. 辦理資安實兵攻防及重大事件情境演練
11. 強化資料保全機制

發揮資安聯防

資安情資分享與合作、建立金融資安事件監控與應變體系。

12. 強化資安情資關聯分析及情資分享動能
13. 規劃重大資安事件演訓，建立虛擬指揮體系
14. 提升聯防SOC協作運作效能

資安監理強化	重視經營階層資安職責、要求獨立資安職能	建立共通資安管理基準及自主評估機制	建構並實證作業風險抵禦能力	持續提升資安防護及其有效性評估

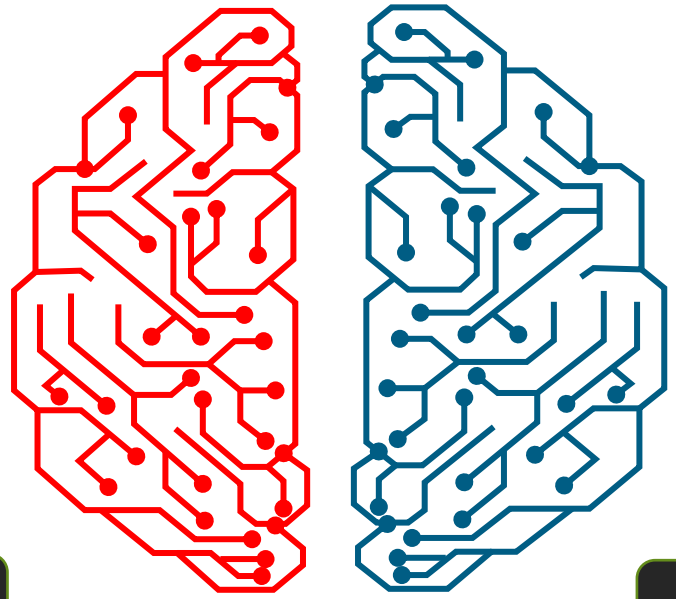
以攻擊者角度思考資安監控機制有效性

尋找攻擊目標

- 攻擊弱點
- 攻擊價值
- 攻擊機會

思考防禦措施

- 強化防禦
- 應變機制
- 監控機制



情資收集

- 以駭客角度嘗試找出弱點
- 已公開情資收集 (MITRE/ NIST/ CISA /網路資源等)

分析駭客攻擊手法

- 易受攻擊的產業
- 常使用的攻擊手法
- 明顯的攻擊目標

→ 以情資為導向設計防禦機制

知己知彼

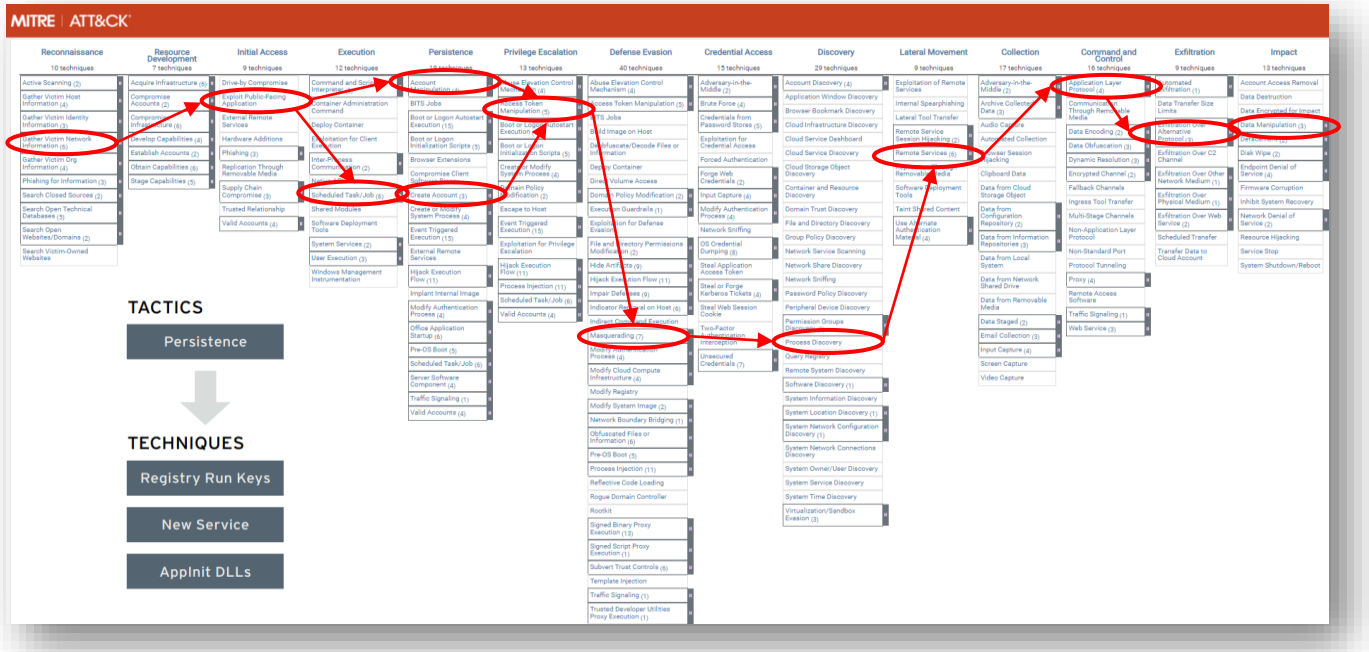
先知道敵人想做什麼，預測敵人的行動

實際演練模擬駭客攻擊，確保已有適當保護

MITRE ATT&CK 對抗戰術、技術和知識庫

MITRE ATT＆CK (Adversarial Tactics, Techniques, and Common Knowledge)

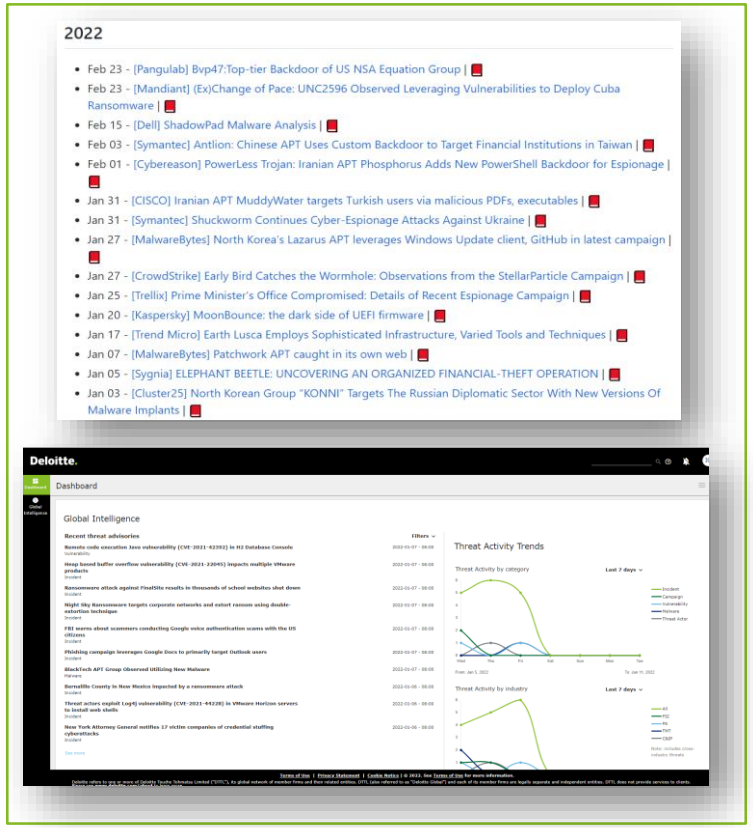
主要整理**網路攻擊行為**，反映了攻擊者生命周期的各階段變化，有助於理解已知攻擊行為與手法，並**可驗證暨資安監控及防禦機制有效性**。



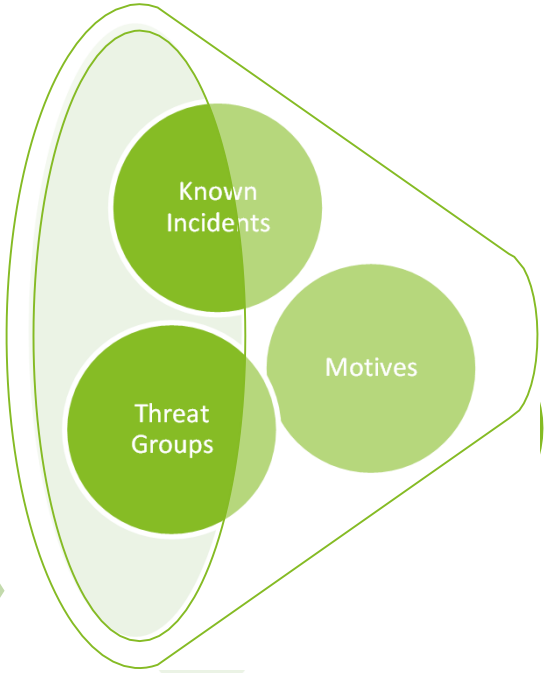
截至2023.12 月 ATT&CK v14
TACTIC 戰略 : 14
TECHNIQUE 攻擊技術 : Techniques: 201 (Sub-techniques: 424)

戰略名稱
偵查(Reconnaissance)
資源開發(Resource Development)
初期存取（Initial access）
執行（Execution）
持續性（Persistence）
權限提升（Privilege escalation）
防禦規避（Defense evasion）
憑證存取（Credential access）
探索（Discovery）
橫向移動（Lateral movement）
蒐集（Collection）
指揮與控制（Command & control）
滲出（Exfiltration）
衝擊（Impact）：

情資為導向之入侵攻擊模擬測試策略



1. 相關威脅情資蒐集

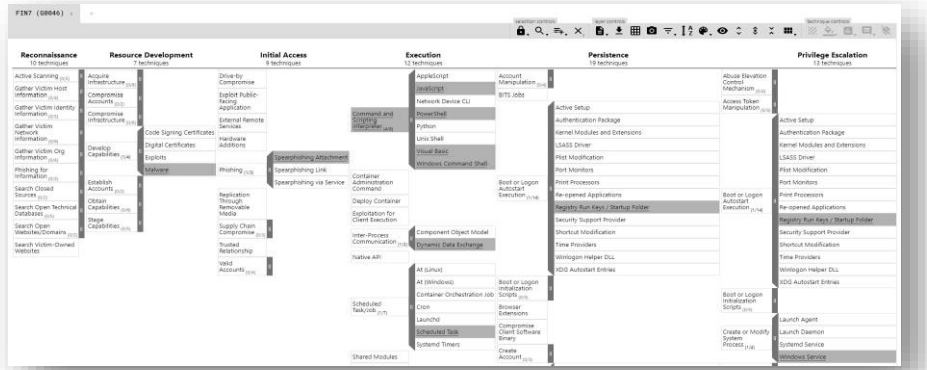


2.1 蒐集對金融產業有高度興趣的特定駭客組織

MITRE ENGENUITY | Center for Threat Informed Defense

Top ATT&CK Techniques

2.2蒐集近期TOP10 入侵攻擊手法



3. 建立Threat Profile

針對特定的駭客組織進行分析

依據F-ISAC研究，以下 APT 組織喜歡攻打金融業.....

1	**Carbanak**	該組織主要攻擊標的為銀行與金融機構，被稱為東歐銀行大盜，該組織已為30個國家/地區的數百家銀行造成了超過3億美元的損失	
2	**APT32**	越南駭客組織，2016年鎖定越南銀行業、媒體，散佈惡意程式；2018年利用CVE-2017-11882漏洞，攻擊中、韓、美、柬埔寨等國家之金融單位	
3	**APT-C-36**	南美間諜駭客組織，涉嫌入侵哥倫比亞銀行、跨國銀行金融機構ATH哥倫比亞分部	
4	**TA505**	俄羅斯駭客組織，2019年鎖定韓國金融、製造和醫療服務進行網路釣魚；2020年利用CVE-2020-1472微軟Zerologon漏洞，攻擊各國金融組織	
5	**FIN7 Group**	俄羅斯駭客組織，從 2017 年初，犯罪活動達到頂峰，成功滲透了 40 個國家和地區的 100 多家金融機構	
6	**Lazarus Group**	北韓駭客組織，2016年孟加拉中央銀行遭劫8,000萬美元、2017年波蘭的金融監管單位KNF遭入侵，進而波及波蘭多家銀行（水坑式攻擊）	
7	**APT38**	北韓駭客組織，2017年10月我國某商銀SWIFT 系統遭入侵，駭客盜轉18 億台幣之攻擊事件 ， 被認為是該組織所為	
8	**Cobalt Group**	東歐駭客組織，該組織主要攻擊標的為金融機構，主要入侵ATM 系統、信用卡處理及支付系統，2016 年 我國某銀行 ATM 盜領案， 被認為是該組織所為	
9	**Winnti Group (APT41)**	中國駭客組織，2020 年 5 月，我國中油遭駭客以勒索軟體加密勒索的資安事件，被認為是該組織所為	
10	**APT28**	俄羅斯駭客組織，主要攻擊標的為政府和金融機構，該組織於2015年從世界各地的銀行，竊取高達9億美元	

運用MITRE ATT&CK 框架之入侵攻擊測試手法選擇

彙總駭客組織用於攻擊活動中常見之技術手法

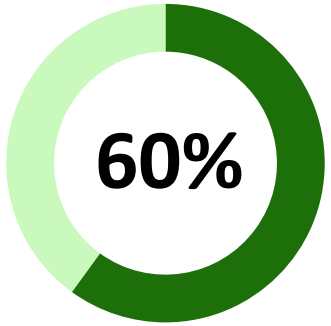
The Top Ten MITRE ATT&CK Techniques (picussecurity.com)

	PICUS	red canary	MITRE ENGENUITY. Center for Threat Informed Defense	MANDIANT
1	T1059 - Command and Scripting Interpreter	T1059:003 - Command and Scripting Interpreter: Windows Command Shell	T1059 - Command and Scripting Interprete	T1059 - Command and Scripting Interpreter
2	T1003 - OS Credential Dumping	T1059:001 - Command and Scripting Interpreter: PowerShell	T1047 - Windows Management Instrumentation	T1027 - Obfuscated Files or Information
3	T1486 - Data Encrypted for Impact	T1047 - Windows Management Instrumentation	T1053 - Scheduled Task/Job	T1071 - Application Layer Protocol
4	T1055 - Process Injection	T1027 - Obfuscated Files or Information	T1574 - Hijack Execution Flow	T1082 - System Information Discovery
5	T1082 - System Information Discovery	T1218.011 - System Binary Proxy Execution: Rundll32	T1543 - Create or Modify System Process	T1070 - Indicator Removal
6	T1021 - Remote Services	T1105 - Ingress Tool Transfer	T1562 - Impair Defenses	T1083 - File and Directory Discovery
7	T1047 - Windows Management Instrumentation	T1055 - Process Injection	T1055 - Process Injection	T1140 - Deobfuscate/Decode Files or Information
8	T1053 - Scheduled Task/Job	T1569.002 - System Services: Service Execution	T1036 - Masquerading	T1021 - Remote Services
9	T1497 - Virtualization/Sandbox Evasion	T1036.003 - Masquerading: Rename System Utilities	T1021 - Remote Services	T1105 - Ingress Tool Transfer
10	T1018 - Remote System Discovery	T1003.001 - OS Credential Dumping: LSASS Memory	T1003 - OS Credential Dumping	T1543 - Create or Modify System Process

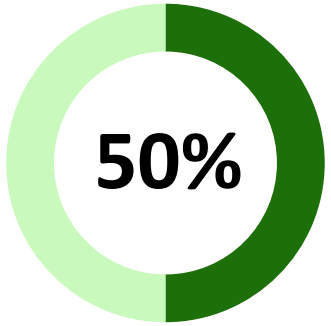
零信任 |不是靈丹妙藥

Gartner - Predicts 2023: Zero Trust Moves Past Marketing Hype Into Reality

2025

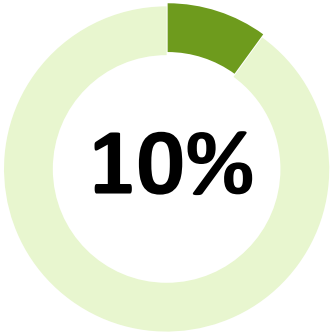


超過 60% 的組織
將採用零信任作為
安全的起點

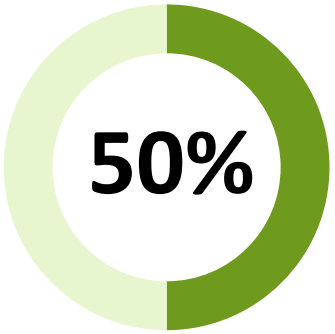


超過 50% 的的組織
未能滿足導入零信任
所帶來的效益
(為了做而做)

2026

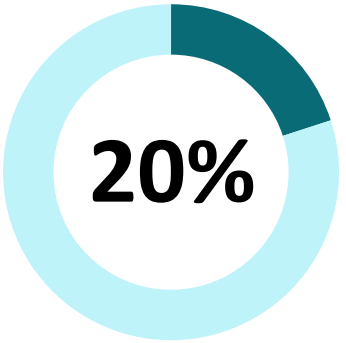


僅有10% 的大型
企業擁有全面、
成熟和可衡量的
零信任計畫



超過50%的網路
攻擊將針對零
信任未覆蓋的
領域進行攻擊

2027



有**20%**的組織將選擇
同一個供應商來滿足
他們的零信任和微切
分防護需求

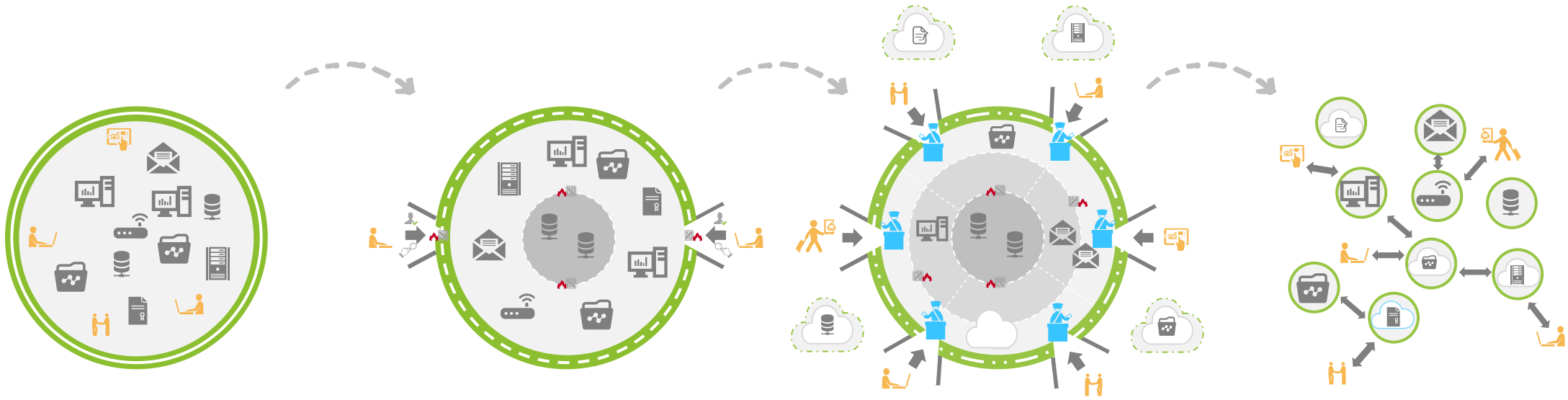
達成零信任需要整體性戰略、分階段目標及清晰治理結構

* 資料來源：https://www.gartner.com/document/4021946

網路安全防護機制的演變

網路安全的四個時代

邊界安全 » 縱深防禦 » 混合網路架構 » 零信任網路安全



邊界安全	縱深防禦	混合網路架構	零信任網路安全
受邊界防護和實體安全控制保護的數位資產	通過多層防禦措施進行控制。防禦著重在南北向(自網際網路通過周邊防禦系統到核心設施)	支援混合架構環境（例如雲/SaaS），對資安監控可視化依賴增加。著重在東西向保護(內部裝置之間的網路通訊)	已刪除網路防禦邊界 。為每次存取交易建立信任並不斷重新進行驗證

零信任導入常見面臨挑戰

零信任不僅僅是單一技術的議題； 而是需要一個完整導入策略及整體方法

CxO Support

管理階層和利害相關方對零信任概念的理解有限，亦不知能為企業帶來什麼樣的效益，無法得到有效的支持

No Strategy

許多組織未能推動零信任，因為沒有建立支持零信任架構所需的流程和治理框架

Crown jewel data

組織不知道他們的”最有價值”資訊儲存在哪裡，以便設計更有效的存取控管機制

Asset Inventory

缺乏全面的數位資產和應用程式清單，對攻擊面及防護邊界掌握也不足夠

Only Zero Trust products

誤以為存在零信任的產品，另未有明確的導入戰略

勤業眾信觀點：參酌零信任導入最佳實務與標準

依據政府導入建議、DoD、CISA等框架，評估管理流程與技術層面的零信任安全控制，衡量組織網路安全性。

國家資通安全研究院 (NICS)

零信任網路架構參考NIST零信任架構，以資源門戶部署方式(Resource Portal-Based Deployment)為基礎，逐步導入決策引擎之**身分鑑別、設備鑑別及信任推斷3大核心**機制

Department of Defense (DoD)

- **ZTA 7大支柱：**以使用者、設備、應用程式與工作負載、資料、網路、自動化與協調、可視性及分析7大支柱作為零信任導入基礎
- **成熟度 3 階段：**依7支柱管理成熟度，分為目標(Target)、目標與進階(Target & Advanced)與進階(Advanced) 3階段

Cybersecurity and Infrastructure Security Agency (CISA)

- **ZTA 5大支柱：**以身分、設備、網路、應用程式與工作負載、資料5大支柱作為零信任導入基礎，自動化與協調、可視性及分析已經涵蓋於各支柱中
- **成熟度 3 階段：**依5支柱管理成熟度，分為傳統(Traditional)、進階(Advanced)與優化(Optimal) 3階段

Next Steps | How to start this journey

根據我們的經驗，零信任旅程最佳方式是定義整體策略和架構，然後用案例分析和概念證明開始

建議通過持續不斷改善方法代替革命方法

Main outputs

- **ZT Workshop**
  - 增加ZT 知識 - 為什麼、和如何執行
  - 從外到內查看內外部組織在 ZT 上所做的事情
- **建立基準**
  - 成立 ZT Taskforce或PMO
  - ZT 成熟度自我評估
  - 評估現況和威脅態勢
- **制定戰略、願景和架構**
  - ZT 願景、目標成果和指導原則
  - ZT 架構制定
  - 定義不同階段所採用的戰略/路徑圖
- **案例定義和 PoC 評估**
  - 定義範圍
  - 供應商選擇框架
  - 概念驗證評估框架
  - ZT案例設計
- **建置**
  - 擬定計劃和時間表
  - ZT詳細架構
  - ZT 政策和標準定義
  - 啟動試點
  - 執行建置

資安韌性強化策略

資安事件發生時應對策略

重大資安事件可能為企業帶來的損害

資料外洩：客戶資料、內部敏感資料
連帶影響客戶/供應商
影響企業競爭力

財物損失
賠償/訴訟
設備重新開發
耽誤營運進度

系統重建成本：事件調查、系統清理、系統重建
聘請外部專家追查事件根因
委請原廠清理系統中的惡意檔案
調整系統架構、設備規則

商譽
登上新聞版面、客戶失去信心

資訊公開措施 – 證交所及櫃買中心對有價證券上市公司重大訊息之查證暨公開處理程序

如上市(櫃)公司發生資通安全事件，符合上述情事者，應比照重大訊息做即時發布與通報。

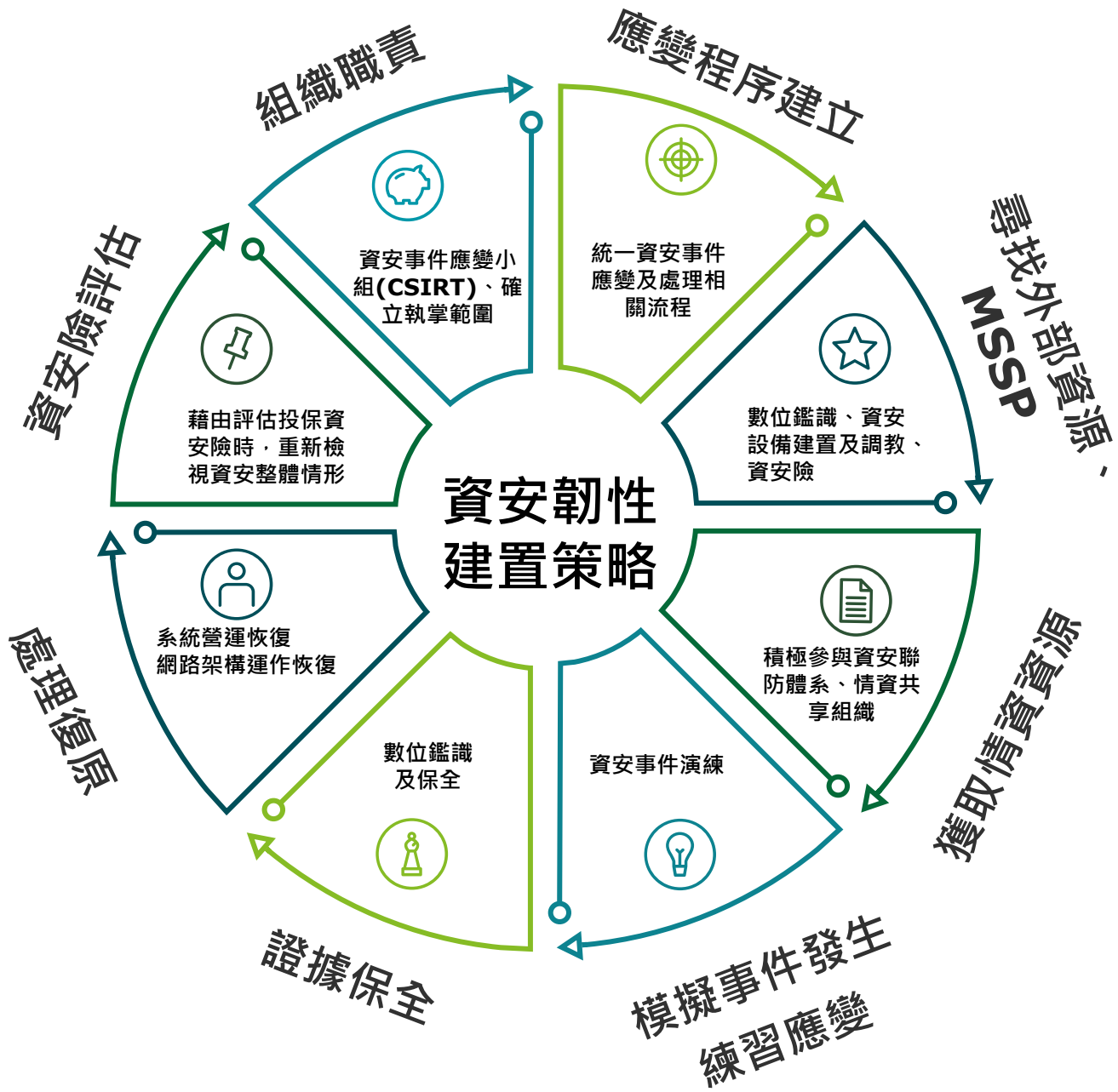
資安韌性展現
為資安事件預先做好準備

“每個人都認為自己有一個完美計劃.....
直到他們被擊倒。"

“ Everyone has a plan… …‘till they get punched in the mouth.”

Mike Tyson

資安韌性建置策略



最重要任務 : 建立資安事件應變團隊

■ 企業可參考事件應變組織架構，安排團隊中的職位階層、各職務對應之業務及管理責任

Sample

管理階層

管理階層

CSIRT指揮官

執行階層

危機管理組

危機處理

情資監控組

定期監控

系統復原組

技術支援

法務/PR/HR...

後續支援

事件調查小組

第一線處理人員

需求彙整/溝通組

專案管控

緊急應變

於第一時間內進駐，制定適當的應變策略，確保於第一時間內進行最適當的威脅控制。

資安調查

針對進行根因調查，分析公司電腦系統以查明是否發生洩漏機密或網路攻擊、發生的原因。

危機處理

於攻擊或災害發生後，協助客戶進行對外危機處理，包含對外說明及聲譽挽回等項目。

數位鑑識

清楚明瞭法律要求的數位證據蒐證流程，以確保其證據能力，以對於企業內部IT設備及數位媒體瞭瞭若指掌，協助辨識蒐證範圍。

資安事件演練所帶來之效益

檢視組織對於程序之熟悉度

- 有效確認各單位熟悉資安事件發生時，各階段處理流程
- 協助各單位深入了解執行各自職掌之時間點，縮短工作項目對接時間

確認分組分工清楚明確

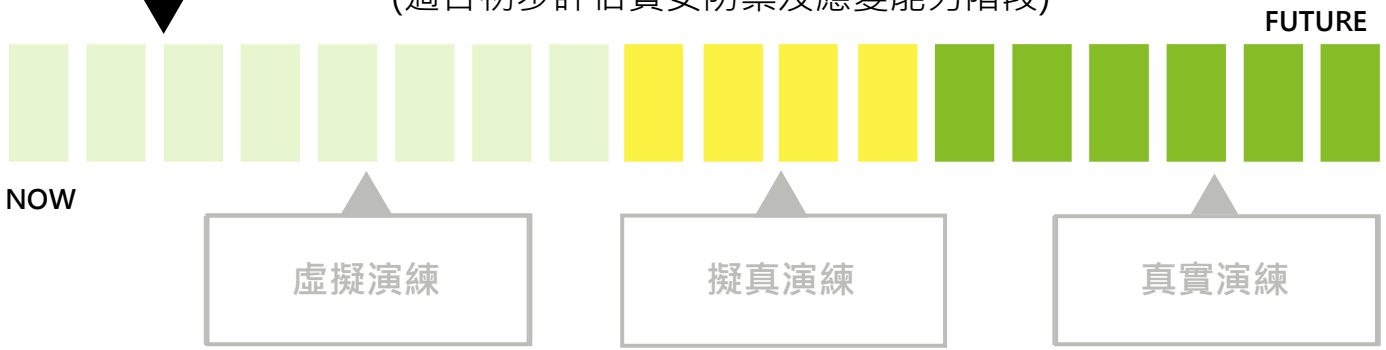
- 有利於專注在各自職掌項目，可在應變過程中有效進行相關工作，並依據自身專業能力與經驗提供有效建議
- 確認各分組執掌切分明確，避免資源重複投入或權責混淆

累積資安敏銳度

- 透過複合式情境，模擬實際資安事件情節，提高演練複雜度
- 有效協助參與演練單位根據自身經驗及專業，思考應對決策與判斷.

桌面演練

依事先假定的演練情境進行互動式討論和思考臨場決策的過程，協助各單位掌握演練情境中之角色職責。(適合初步評估資安防禦及應變能力階段)



強化評估人員於資安事件發生時之決策意識

協助人員強化觀察與資安預警敏銳度

協助人員深入了解駭客思維與攻擊脈絡

全面啟動企業資安韌性

01 CSIRT成熟度自我評估

- 組織面向
- 工具面向
- 人員面向
- 程序面向

短期目標

02 成立資安事件應變小組

- 資安事件處理指揮中心及CSIRT團隊
- 資安事件通報及溝通平台機制
- 確認分工與橫向溝通的效率

03 演練！演練! 演練 !!

- 演練情境及方式確認
- 執行資安事件應變攻防演練
- 執行數位鑑識演練

中期目標

04 及早掌握威脅情資

- 及早掌握各類型有用之威脅情資
- 威脅情資正確性判斷
- 威脅情資分享及運用

05 資安事件協作自動化

- 設計不同情境資安事件處理流程自動化腳本
- 流程標準及自動化設計

長期目標

意見交流

Deloitte.

勤業眾信