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

FINSEC FORUM

FINSEC FORUM

前瞻金融資安長的省思與蛻變：先相信才會看見

TEAM CYBERSECURITY

高大宇 教授/博士

永豐商業銀行 副總經理
政治大學資安碩 兼任教授
台灣資安主管聯盟 副會長

高大宇/DAYU KAO

- 堅持：30年產(金融資安副總)官(科技警官)學(大學教授)
- 惜福：滿懷感恩，熱情享受
- 典範：避免瞎選 - 聽說、跟風、不知所以然
- 傳承：觀察知識、技術、能力及態度，選用育晉留人

台灣資安主管聯盟 副會長

政治大學資安碩兼任教授

1. 持續成長

- 警大資管系畢業(官)
- 資訊主管
- 網路犯罪偵查員
- 資安碩士
- 三線一星資訊主管
- 資安博士
- 資安助理/副/教授(學)
- 資安主管(產)

2. 珍惜機會

- 識才：千里馬常有，須伯樂賞識
- 治理：上馬打天下，下馬治天下
- 時機：有德配位，責任承擔聲望
- 警覺：自動偵測，主動分級防禦
- 溯源：透明可視，韌性無限賽局
- 借鏡：識別復原，持續曝險管理
- 團隊：兄弟爬山，互相支援練兵

3. 專業技能

職能品牌

- 金融資安治理
- 通資科技法律
- 訴訟舉證蒞庭
- 電腦稽核調查
- 數位鑑識分析

證照/研究

- 資安證照：CEH 、CHFI、ISO 27001、NSPA認證
- 金融證照：銀行內部控制與內部稽核、金融市場常識與職業道德、金融科技力知識、防制洗錢與打擊資恐專業人員等。
- 美澳短期訪問/研究，論文近200篇，參與或主持國際會議

治理策略

- 組織治理：預想被駭，721 學習，適當挑戰
- 風險管理：化資安幻覺成實際幫助CSF/CDM
- 法規遵循：三道防線，協調合作，KISS原則

大綱

1.美國監管與全球治理

2.先相信才會看見

3.前瞻資安長的省思與蛻變

4.結語

1.美國監管與全球治理

(1)地下帝國：網路、金融、半導體
(2)美國如何武器化世界經濟

美國監管Vs.全球治理

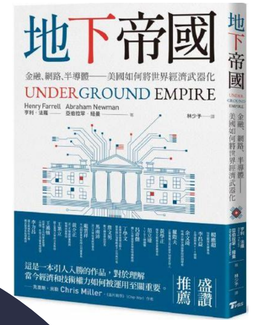
面臨問題(Problem)

- 在**美中2大**帝國**霸權競爭**下，全球(台積電)**半導體供應鏈渴望自由的理想雖美好，**
- 卻**面臨強權監管關鍵脆弱點的殘酷現實**。

思索對策(Strategies)

- **台灣**經濟**要有雁群合作的團隊運作，退居第三**(緩解**帝國霸權**的持續追殺，屈身忍辱尋求恐怖平衡)，
- **輔以識時務的防兼併合縱政策**(有共同凝聚力和重要目標)，
- **方能保有專業研發，穩居專業霸權產業地位，永續韌性地長久經營**。

地下帝國：網路、金融、半導體
—美國將世界經濟武器化，抗中、俄、伊朗、北韓



1955-2007

- 1955五眼聯盟**通訊**監聽
- 1980Intel一條龍式
- 1990台積電代工
- 1999-2003中國**網軍**入侵
- 2007稜鏡計畫**網路**監聽

2010-2015

- 2010美以Stuxnet、ARM等矽智財SIP
- 2012SWIFT逐伊朗
- 2015北韓APT38駭入SWIFT

2016-2017

- 2016俄駭第一銀行ATM
- 2017北韓Wannacry
- 2017SWIFT逐出北韓

2018-2022

- 2018-2021中國華為**通訊**孟晚舟緩起訴(匯豐銀行)
- 2020以**飛馬**間諜軟體
- 2022SWIFT逐出俄

2024-2025

- **關稅競爭**：台積電美國設廠
- 非紅供應鏈，美國製造，貿易失衡
- 數位美元**穩定幣**、中國數位人民幣跨境結算系統(**即時分散式帳本**)
- 美通緝、起訴12名中國人；中公布3~4名台匿名者64**網軍**；台通緝1名中駭客Crazyhunter**勒索**攻擊；台海纜斷裂(**通訊**或電力傳輸)

(1)地下帝國：網路、金融、半導體

地域	美國	中國	台灣
資訊網路	**(1)索取機密** **(2)竊取機密：監聽或破解** **1955**年五眼聯盟通訊監聽、1999-2003中國**網軍**入侵、**2007**年稜鏡計畫**網路**監聽、2010年美以Stuxnet蠕蟲、2015年北韓APT38駭入SWIFT、2017年北韓Wannacry、2020年以飛馬間諜軟體 **(3)(傳票)依法要求**：數據解密、取得密鑰、隱藏後門	(1)**2016年**中國APT27「駭客僱傭」生態系統 (2)2018-2021年中國華為通訊孟晚舟緩起訴(匯豐銀行) (3)2025年，美國起訴APT27 12名中國人；中國公布3~4名台匿名者64網軍；台灣通緝1名crazy hunter中國駭客。	(1)**2017年**中國控台網路攻擊滲透活動 (2)**APT**駭客看財報，**找**金融（供應商）、（核）電力、（海纜）通訊等**數位寶藏練兵場**，如2025年精誠勒贖
金融資金	(1)布雷頓森林體系1.0的「雙掛鉤」制度：美元清算系統(二戰後)、SWIFT全球支付系統，逐出伊朗(**2012**、2018年)、北韓(2017年)、俄羅斯(2022年) (2)布雷頓森林體系2.0「去美元化」前哨戰數位美元穩定幣(**2025**年)	(1)**2025**年中國人民銀行宣布數位人民幣跨境結算系統(即時分散式帳本) (2)中國數位絲路的虛實戰略佈局(掌控人民活動)：覆蓋200個國家數位支付網路	(1)數位轉型，跨境金融須持續提供好、快、自由且具信譽的產品服務。 (2)面對金融監理與反恐合規成本增加的全球不確定經濟風險(市場波動、地緣政治及通膨壓力)
晶片關稅	1980Intel一條龍式、2010美ARM矽智財SIP奪回經濟主權(**非紅供應鏈**)，製造業回流(去風險戰略，**美國製造**)，解決**貿易失衡**(最先進半導體製造的地理集中)	**中國衝擊**(China Shock)：**低階國際供應鏈**帶來靈活性，如iPhone	1990**台積電**代工 **高階半導體供應鏈**：台灣擁有完整的中、下游半導體產業聚落及專業分工

(2)美國如何武器化世界經濟：讓美國再次偉大(MAGA)

地域	美國	中國	台灣
聯盟	五眼聯盟Five Eyes：英美加紐澳	金磚國家BRICS：巴俄印中南非10國	12邦交國：生於憂患，死於安樂
態度	**親美尋求安全**	**疑慮中國憂患**	**穩妥布局全球**
差異	**地下帝國**金融網路 (1)完全掌握：金融實力、管控技術 (2)強硬治理：粗暴威脅、震攝脅迫 (3)理想美好：權力越大、責任越重	**專制帝國**矛盾處理 (1)努力狂奔：危機浮現、選擇脫鉤 (2)粉飾太平：掩蓋麻煩、謀取利益 (3)現實殘酷：擴張建設、軍備競賽	**專業霸權**妥協和解 (1)攜手合作：協調管控、避免對抗 (2)謹慎掌握：恐怖平衡、度過危機 (3)老三哲學：合作和解、別逼盟友

網路
監聽入侵

→

金融
裁罰管控

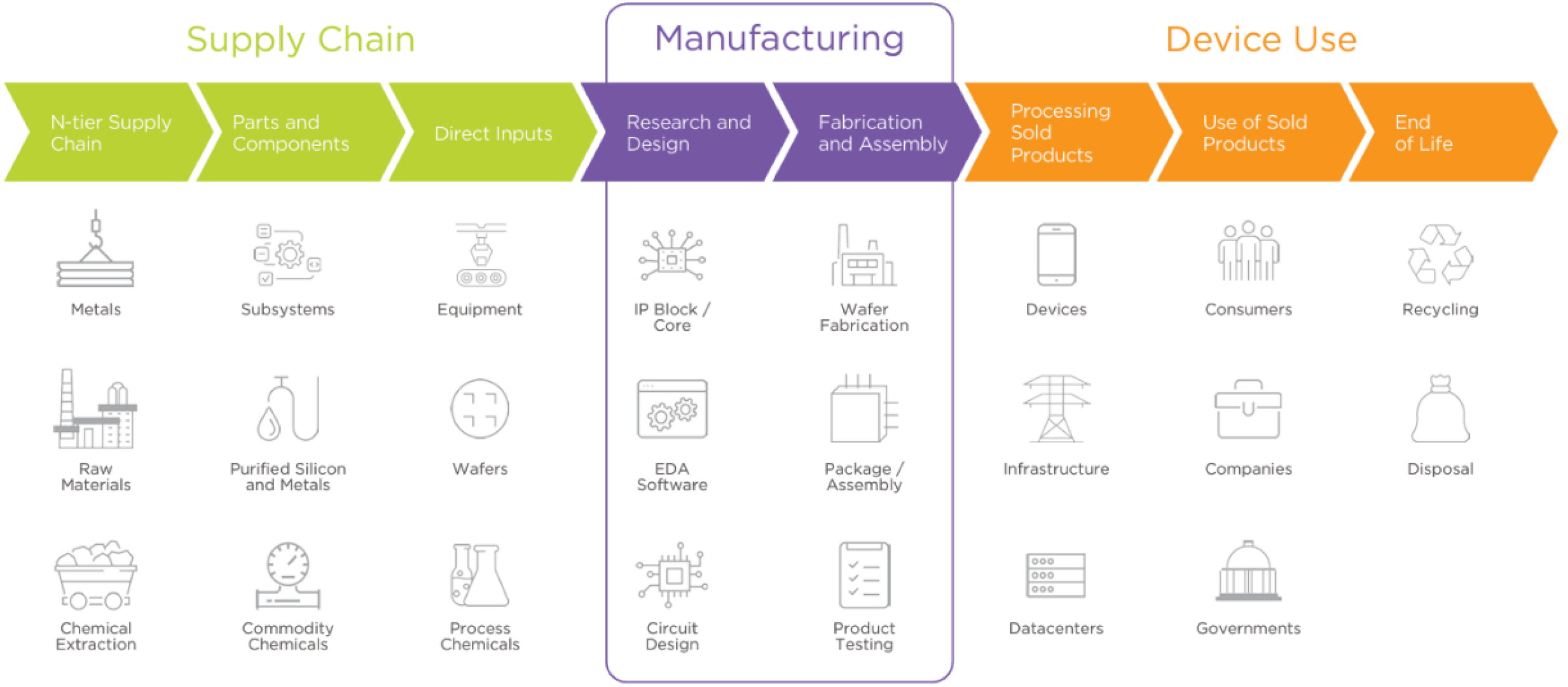
→

半導體
美國製造

→

關稅對等
美國優先

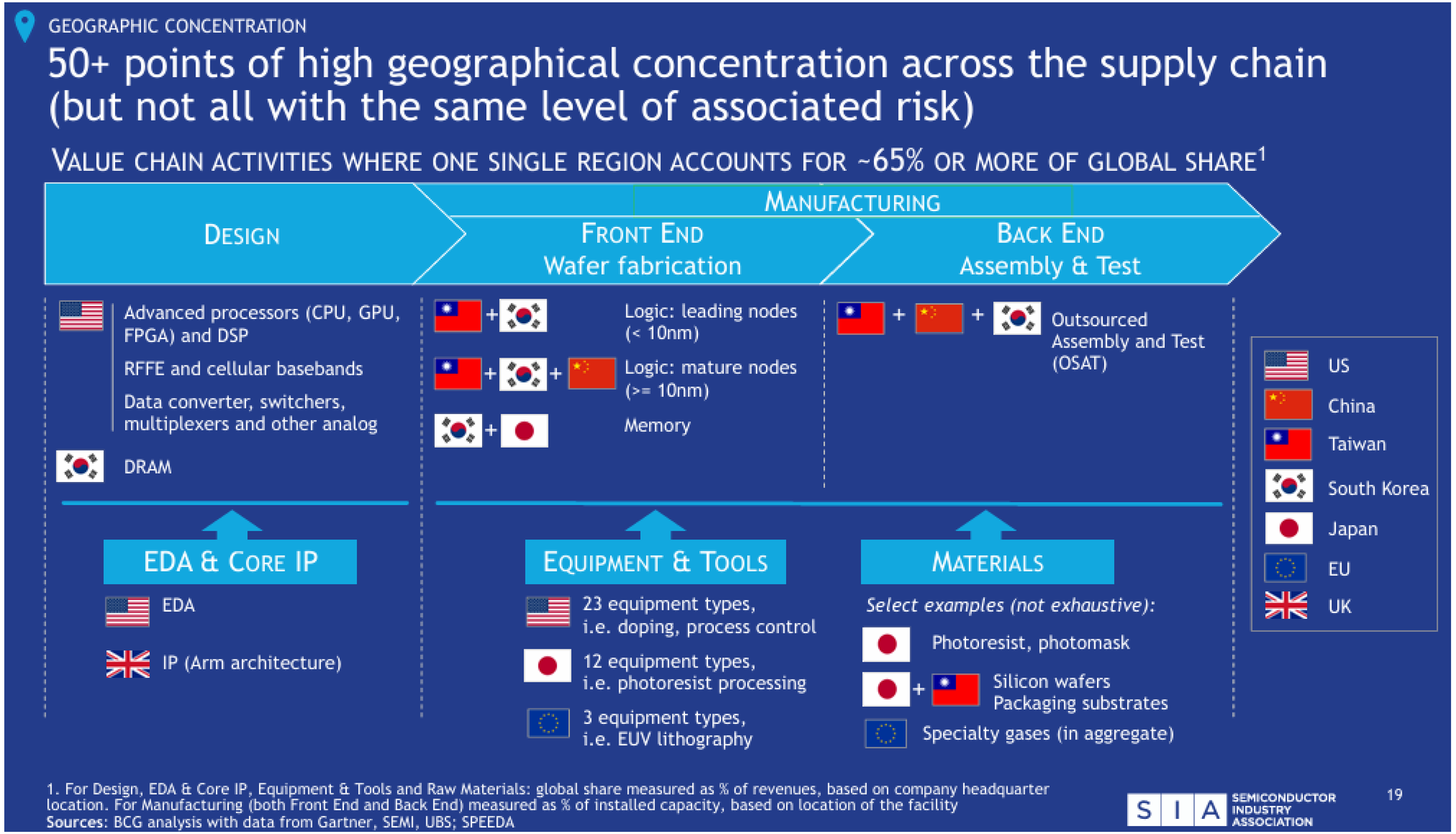
緊密聯繫：半導體價值鏈活動



Source: BCG analysis

https://discover.semi.org/rs/320-QBB-055/images/Transparency-Ambition-and-Collaboration-BCG-SEMI-SCC-20230919.pdf

地緣政治風險：高度地理集中的半導體供應鏈關係



https://tac.bis.doc.gov/index.php/documents/public-presentations/484-sia-semiconductor-supply-chain-briefing-deck-vsent-sia-branded-6-8-21/file

老三哲學：保有研發，穩居霸權

1.全球關稅衝突現況

(1)霸權競爭：川普2.0政策走向、地緣政治風險及(G)AI科技發展
(2)衰退關鍵：強權監管全球網路及管控金融SWIFT系統，半導體成美國經濟關鍵脆弱點
(3)關稅衝突：2025年美國單挑全世界，神仙打架(大國反制，小國協商)，小鬼遭殃(出場越帥，死得越快)

2.定調企業目標策略

(1)政商分離的老三哲學：緩解帝國霸權的持續追殺，若無法主導談判地位(我知道我比你好，但我永遠不會告訴你)，退居老三(我知道我是最好，但我永遠說我是老三)。
(2)雁群合作的聯盟合縱：有共同凝聚力和重要目標，能思考艱難決定，模糊說服，達成和解。
(3)永續韌性地長久經營：能勇敢向前，如樹活一張皮(樹皮能防寒防暑防病蟲害)，人活一口氣(幹最累的活，拿最低的薪)

3.半導體供應鏈的資安治理作為

(1)主動的**營業秘密**及個資保護：避免洩密、秘密分享攤責、偽裝保護究責。
(2)被動的善用**三道防線**管控：理性選擇下，常識帶來見識，見識帶來膽識。
(3)積極的**內部**人員**調查**釐清異常事件：有效查核究責人員(ABC黃金原則)、完整備份釐清盲點(紀錄4要件)

定調企業目標策略：職場社交的5桶金

1.累積**知識**槓桿

自我修煉**知識**，靠實力讓人尊重，增**技能**優勢助職涯發展

2.善用職場**人脈**

真誠信任感謝，助別**人**解決問題，**資源**交換產生情緒價值。

3.擴展**資源**名聲

持續連結關係，緩解過剩**資源**人士的煩惱，深入優化**名聲**。

半導體供應鏈的資安治理作為

保有研發，穩居專業霸權產業地位

1.主動的營業秘密及個資保護

- **避免洩密**(簽署入職聲明書、明示浮水印提醒)
- **秘密分享攤責**(前瞻研發、智慧財產、程式開發、資料分級)
- **偽裝保護究責**(隱藏存取身分、設備、資料源、公司商標等，以利侵權訴訟舉證)。

3.積極的內部調查釐清異常

ABC黃金**3原則**：

- 不預設立場(**A**ssume Nothing)
- 不輕易相信(**B**elieve Nothing)
- 審慎檢查跡證(**C**hallenge and Check Everything)

2.被動的善用三道防線管控

- 常識帶來見識，見識帶來膽識。
- 採CDM網路防禦矩陣、ZTA零信任架構及DLP遺失保護(Web、Mail、USB)
- 關注**資安防禦人員、程序、技術及治理**，不美化數據，掩飾真相、才能防範(彙整情資、相互參照、循跡追查)。

- 有效查核究責**人員**：能究責相關主管(經理人)及人員，注意數位犯罪調查的ABC黃金**3原則**
- 完整**備份**釐清盲點：能完備稽核紀錄的**IP位址、時間戳記、數位行為及系統訊息**(成或敗) **4要件**
- 專業電腦稽核**調查**專業：掌握**信賴**性(Reliability)、**相關**性(Relevance)及**充分**性(Sufficiency) **3關鍵**

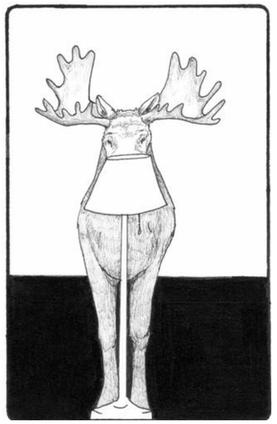
2.先相信才會看見

(1)資安長轉型
(2)資安長的未來關鍵能力

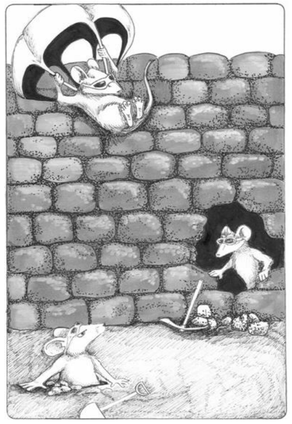
(1)資安長轉型：安全須適合無數使用者和情況

適合使用情況

默默無聞
不安全



突破防火牆



鎖並不一定意味沒風險

誤認安全

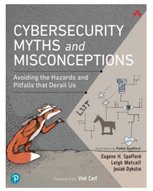
透過默默無聞(誤認他人不知)實現安全，就像相信永遠不會找到燈後面的駝鹿一樣！

不留後門

供應商的後門(秘密)，內部人士都知道(可能出售)。

強化防護

能被發現的弱密碼(秘密)，肯定會導致不安全。



避免視野狹窄/眼光短淺(資訊安全)

1. 認清真相(AS-IS)

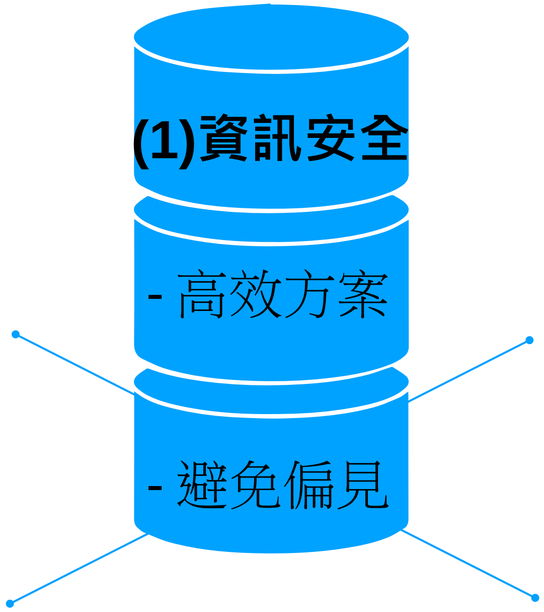
(1)無快速方法：外洩原因很多

-密碼猜測等攻擊
-**防禦誤擋**或**偵測誤判**
-資安政策不足、缺乏多因素驗證、允許過多密碼嘗試、配置錯誤或員工培訓不足

(2) 無靈丹妙藥

- **不應僅尋找**工作問題的**簡單解方**
- 故事**還沒結束**。

2.差異分析(Gap Analysis)



(2)努力尋找解決方案

- **無單一工具或解決方案**，來完成資訊安全、緩解安全挑戰或提供完美結果。

3. 展望未來(TO-BE)

(1)資安事件成因調查

-不斷增加：違規行為和訴訟
-資安事件：檢查成本和原因

(2)找出簡單解釋的背後原因

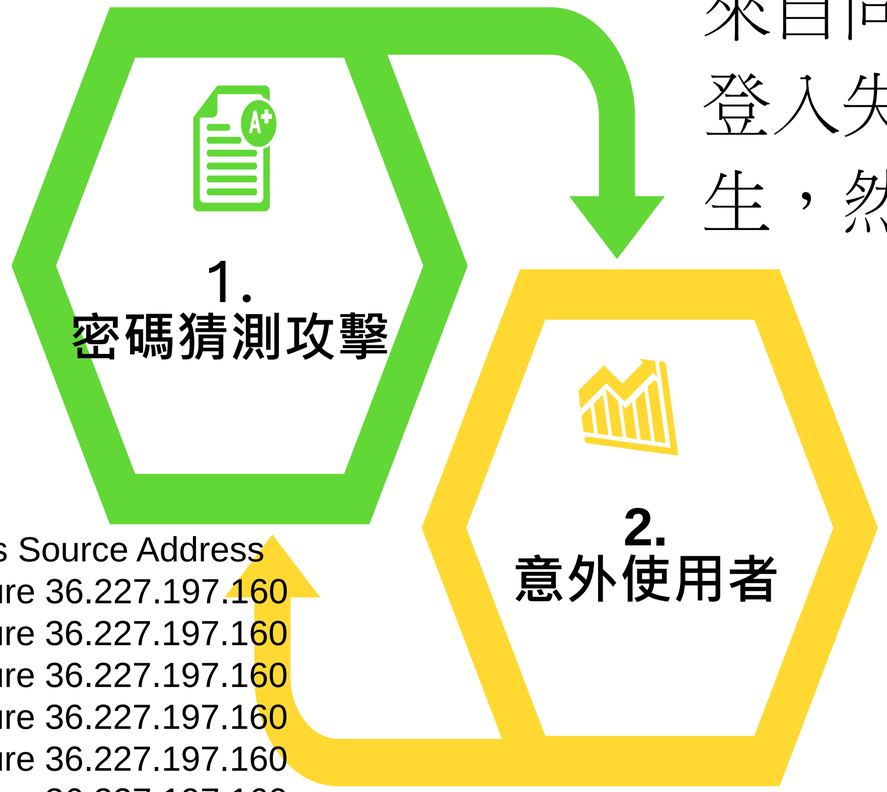
- 認知後果：解釋事件的因果關係和個別立場
-專業領域：不完整/隱含的解釋，常引人注目且難以辨別的

深入解釋知識：攻擊/隨意、程式/人為的行為判斷

前後相關性暗示因果關係

伺服器觸發警報，SIEM

日誌顯示發生什麼事？



1. 密碼猜測攻擊

來自同一來源的多次登入失敗很快就會發生，然後登入成功。

2. 意外使用者

可能是一位沮喪的使用者不小心打開了大寫鎖定鍵。

顯示相關性的日誌範例

Date	User	Host	Login Status	Source Address
31/10/2024, 10:37:30 AM	dayukao	mail	Failure	36.227.197.160
31/10/2024, 10:37:31 AM	dayukao	mail	Failure	36.227.197.160
31/10/2024, 10:37:32 AM	dayukao	mail	Failure	36.227.197.160
31/10/2024, 10:37:33 AM	dayukao	mail	Failure	36.227.197.160
31/10/2024, 10:37:34 AM	dayukao	mail	Failure	36.227.197.160
31/10/2024, 10:37:35 AM	dayukao	mail	Failure	36.227.197.160
31/10/2024, 10:37:36 AM	dayukao	mail	Failure	36.227.197.160
31/10/2024, 10:37:37 AM	dayukao	mail	Failure	36.227.197.160
31/10/2024, 10:37:38 AM	dayukao	mail	Success	36.227.197.160

(2)資安長的未來關鍵能力

認清現況(AS-IS)

治理者

監視和調整程序和控制以持續提高安全性。

技術專家

指導安全技術和標準的部署和管理。

職場軟實力 (Gap Analysis)

溝通
對於困難的對話

相信
關懷、正直、可靠和能力

解決問題
為了企業的利益而做事

策略
停下來，向前看

展望未來(TO-BE)

顧問

幫助企業主和管理團隊了解網路安全風險，以便他們做出明智的決策。

策略家

將安全性與業務策略結合起來，以確定安全投資如何為組織帶來價值。

(Source: https://www2.deloitte.com/content/dam/insights/us/articles/ciso-next-generation-strategic-security-organization/DR19_TheNewCISO.pdf)

資安長的治理知識：職責角色與工作重點

通盤了解公司營運

(1)通盤了解公司營運
(2)技術合作：資安/訊長密切合作

企業治理 (Governance)

數位資料保護措施

(1)了解人性
(2)持續維運 (BCP/BCM)：
A.危機處理
B.事前規劃和演練
C.召集各部門參與

風險為本 (Risk-based)

新法規規範與罰則

(1)了解國際法規
(2)注意新的規範 (刑事處罰或行政繳罰鍰)

合規為本 (Compliance-based)

善用AI升級資安

(1)優質防禦團隊 (People)
(2)節省苦力時間 (Process)
(3)快速辨識威脅 (Technology)

策略規畫 (Strategies)

資安長的必要技能：識別資安儀錶板之可視性和控制力錯覺

認清現況

1.認清真相AS-IS

- **值得投入努力**：靠**防禦慾望**不能完全阻止駭客，需付出值得投入的有效努力。
- **可能輸給駭客**：即使有**安全機制**和政策，仍可能輸駭客。
- **不能保證成功**：**蜜罐**可分散駭客注意力至低威脅**環境**，但不保證成功。

2.視覺化路徑

網路資安狀態彩色圖表

- **看起來很棒**：漂亮可愛且令人**印象深刻**
- **幻想很誘人**：很誘人的**可視**性和**控制**力幻想。
- **要決策細節**：**具**提供做出正確決策完整細節的**可解釋性**

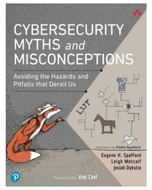
展望未來

3.FUD差異

- **怕預測錯誤**：恐**錯認可控**或預測，如相信可擲骰子獲特定數字。
- **不確定為真**：圖表可能**無法代表**系統發生的實情。
- **疑海市蜃樓**：疑**隱藏實情**在漂亮表象後面。

4.發掘真相TO-BE

- **複雜多變**：視覺化常過於**簡化**實際有價值的**複雜性**。
- **隱藏真相**：**難理解**被隱藏的東西
- **無法想像**：駭客有目的、目標和動機，**無法**完全**控制**其行動。



凡事存疑、總是驗證：人前尊重、人後提醒

3.前瞻資安長的省思與蛻變

(1)資安轉型再成長的關鍵路徑

(2)您若盛開，蝴蝶自來

(1)資安轉型再成長的關鍵路徑

看見成長機會
認清現狀(As-Is)

- **識才**：千里馬常有，須**伯樂**賞識
- **時機**：有德配位，責任**承擔**聲望
- **警覺**：自動偵測，主動**分級**防禦
- **溯源**：透明可視，韌性無限**賽局**
- **借鏡**：識別復原，**持續**曝險管理
- **團隊**：兄弟爬山，互相**支援**練兵

相信治理策略
期望目標(To-Be)

- **組織治理**：預想被駭，**基礎實作**，**團隊合作**， 721 學習，適當挑戰
- **風險管理**：**攻防場域**，**刺激願景**，CSF/CDM化資安幻覺成實際幫助
- **法規遵循**：三道防線，**互利視野**，協調合作，KISS原則，內部控制

核心理念

- 持續不變內涵與**價值觀**
- 符合期待的信念與**使命**

硬實力基礎

- 專業技術可獲工作**聘僱**
- 適當**挑戰活用**專業知識

不進則退
以終為始

願景驅動

- **刺激進步**的**潛能**力量
- **願景圖像**的**轉念**達成

軟實力進化

- **情商**適當表達**超越感動**
- 個人特質可獲**更高成就**

(1)資安轉型再成長的關鍵路徑：現況與未來

認清現況(AS-IS)

明顯資安風險

- **關心最終結果**：**不總與**明顯的**電腦**本身風險**有關**。
- **風險接受程度**：培訓費用昂貴且**無法完全消除**風險。
- **商業決策結果**：不同投資成本，獲得不同的**保護等級**。

別怪設計師

- **試圖完成任務**：調查根因，**尋求解決**。
- **程式存在漏洞**：問題，怪罪/責備某人?
- **指責未解問題**：指責也許感覺好一點，但**很可能是錯的**。
- **找根因防類案**：可能犯錯。適當方法是採取措施防止再次發生。

別怪資淺者

- **歸咎他人病態**： 喉嚨要窒息。
- **不可避免受害**：**防止傷害，**主管**公開指責**實習生選擇**弱密碼**。既沒幫助，也不合適
- **好的指導監督**：為什麼實習生在做出這樣的決定時，沒有得到更好的指導和監督？

展望未來(TO-BE)

超越熊威脅

- **停下來穿跑鞋**：Q.會遇另一隻熊?
- **慢速的受害者**：Q. 如熊注意力集中在第一個人
- **只需比他人好**：Q.希望同事死來拯救自己?
- **大量的熊威脅**：Q.防禦能力夠嗎?

風險可控

- **適合情境**：安全不好用，安全性必須適合無數的使用者和情況。
- **科技應用**：停泊在港口的船是安全的，但不是造船目的。
- **風險控制**：鎖並不一定意味沒有風險。

未雨綢繆

- **準備成功**：事先不準備，容易失敗
- **不會後悔**：將所學活用於實際工作
- **有備無患**：凡事豫則立，不豫則廢

(2)您若盛開，蝴蝶自來：您重要的事他人也重要

- **活著的理由**：是否還會遇見他
  - 最重要的**時間**：**掌握現在**
  - 最重要的**人**：**身邊的眼前人**
  - 最重要的**事**：**幫助**眼前人
- **很多「選擇」**：判斷**正確**、有**效率**、**值得**嗎？
- **一起「活著」**：帶來**溫暖與美好**
- **美麗「緣分」**：**主動伸出援手，帶來正面**影響**價值**

轉念後的自己(伯樂)

環顧四週

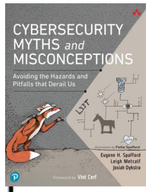
- **關心資安**：大多數環境，資安團隊外的人常不太關心資訊安全
- **資源支持**：高階領導有金錢和其他資源的支持？
- **輕重緩急**：不該期望所有人的優先事項均相符。
- **聘請專業**：聘請資安人員來協助資訊安全。

見樹要見林

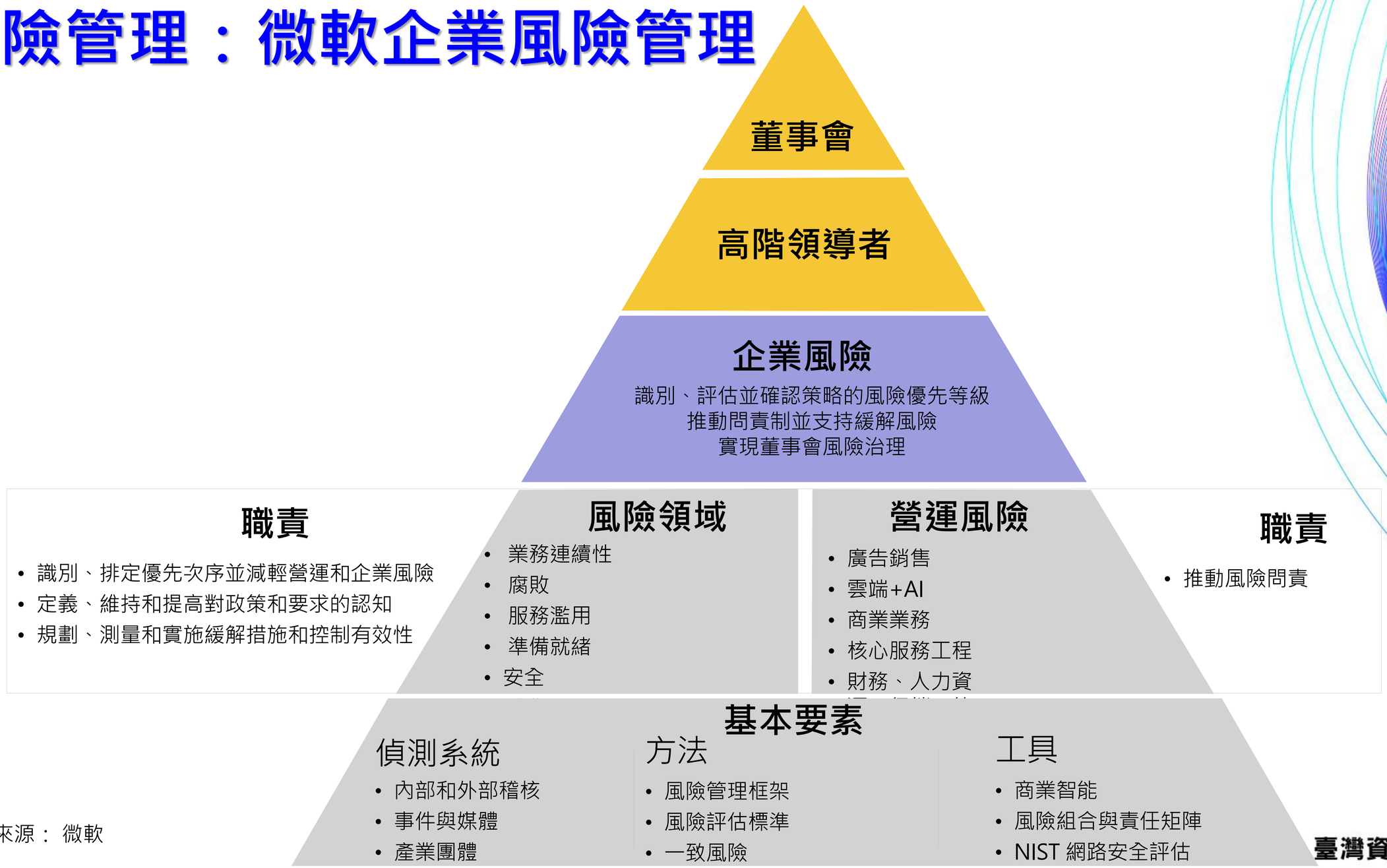
- **主要目標**：對CEO，資安常非主要目標，非前10名
- **網路衛生行為**：即使了解資安，有時表現危險行為
- **專業獎勵**：因保護獨創性獲得個人獎勵。
- **見樹不見林**：越專業職業，關注興趣越狹窄和具體。
- **擴張邊界**：廣泛擴展專業時，看到更大視野圖像並考慮更多觀點

考慮背景的關鍵想法

- **了解背景**：規劃和執行策略時，了解歷史、資源、目標、風險、合規等。
- **正視問題**：**弱點修補**可能會導致**批評**而不是**讚揚**！如，安裝需重新啟動的修補程式可能會干擾行銷活動。
- **剖析迷思**：在一種情況正確的東西，在另一情況下可能是無稽之談
- **尋求澄清**：存在無法知道的情有可原情境，會導致CEO持有不同優先事項



風險管理：微軟企業風險管理



資料來源： 微軟

4.結語

CrowdStrike初步事件檢討

影響 Falcon 感測器和 Windows 作業系統的內容配置更新，越界讀取記憶體(CWE-125)，導致藍屏死機(BSOD)

概述

透過軟體定期更新升級，**收集新**威脅的遙測**資料**(telemetry)、改進威脅或漏洞偵測模式，以保護新威脅。

發生何事：事件概述

2024年7月19日 04:09至 05:27 UTC，更新感測器快速回應內容(**RPC**; Rapid Response Content)，**收集新**遙測**資料**，發到7.11(含)以上版本Windows(未連線主機不受影響)

發生原因：事件原因

驗證檢查期間**未發現**的**RPC**缺陷造成崩潰。感測器載入內容時，越界讀取記憶體(**CWE-125**)，讀取未授權資訊，導致Windows藍屏死機(**BSOD**; Blue Screen of Death)。

防止再次發生：**供應商**

(1)強化**軟體測試**程序：缺乏充分的質量檢查

- 改進**RPC**測試：使用內容更新和回溯、錯誤注入等
- 額外驗證檢查：內容驗證器(Content Validator)

(2)強化**韌性**和**復原**力

- 加強錯誤處理機制：妥善管理有問題的錯誤內容

(3)**第三方驗證**：程式碼審查及(開發到部署)品質審查

防止再次發生：**客戶**

(1)舉證影響：民/刑事？舉證責任？求償損失？
(2)應變協商：合約規定？費用減免？Uber Eats禮物卡？
(3)精緻階段部署(staggered deployment)

- **階段排程選擇**：金絲雀(canary)先行，再分階段。
- **加強效能監控**：在階段內容部署期間，加強對感測器和系統效能的監控，以及時發現和緩解問題。

https://www.crowdstrike.com/wp-content/uploads/2024/07/CrowdStrike-PIR-Executive-Summary.pdf
https://www.engadget.com/the-morning-after-blue-screen-of-death-outage-affected-around-85-million-devices-112012903.html

網路勒贖事件檢討：依附系統生存(LoL)就地取材攻擊

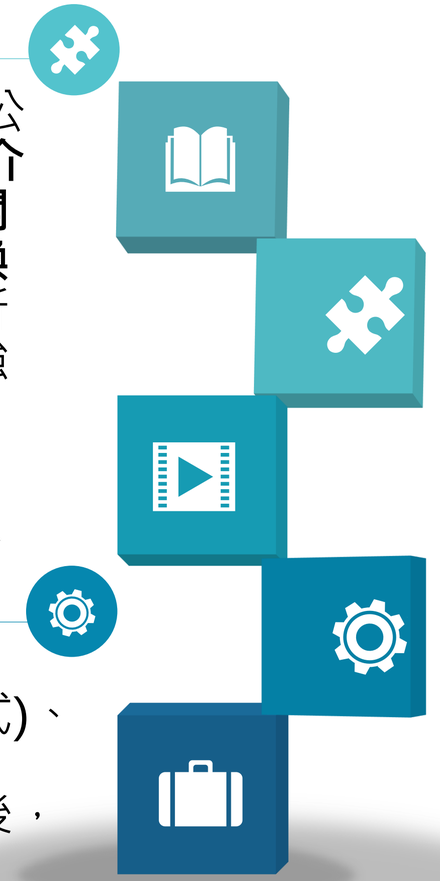
主旨	本公司網路資安事件說明				
符合條款	第	26	款	事實發生日	114/03/31
說明	1.事實發生日:114/03/31 2.發生緣由:匿名網路勒贖信件 3.處理過程:本公司接獲匿名網路勒贖信件後，已向法務部調查局報案，並立即啟動資安應變機制，配合法務部調查局及本公司內、外部資安技術專家清查受影響的系統。 4.預計可能損失或影響:尚在清查中，目前對本公司營運尚無重大影響。 5.可能獲得保險理賠之金額:不適用 6.改善情形及未來因應措施:本公司全力配合法務部調查局偵辦本案件，配合法務部調查局及本公司內、外部資安公司技術專家追查事件及釐清原因，全面性檢視系統安全，並加強系統的監控與防護，以提升及強化資安保護及資訊安全。 7.其他應敘明事項:無				

2.盤點影響

盤點公司(含各子公司)的供應商**網路介接**、**代管系統**、**開發維護**及**資料交換**等維運狀況，剖析風險等級，並加強監控資安告警。

4.偵測異常

偵測異常IOC 情資(中繼站與惡意程式)、**清查連線**(外對內、內對外及交叉對)後，**封鎖**可疑**高風險**連線(如海外VPN)。



1.事件了解：警調資安聯防

了解APT入侵文件外洩**情資**(未安裝EDR、未有資料加密)及可能影響**範圍及程度**(AD、VPN、Exchange、OA及核心系統等系統特權帳號)。

3.加強管控：24小時

(1)安心使用：積極從網路、網站、端點、程式、資料等**多層次防禦**
(2)資安無虞：遇異常攻擊流量，均經**資安戰情室**的**逐日交叉比對**紀錄，於**質(行為特徵)量(大量攻擊)分析**後，適時調教阻擋機制。

5.提高警覺：轉達與宣導

(1)系統**異常**(如時間、金額與內容)，比對及**複核**真偽。
(2)避免點選**社交工程**釣魚信件或惡意附件
(3)提醒留意開發**程式碼**的安全性。
(4)落實**零信任**措施。

適當挑戰：把握機會、向上發展、符合期待、超越感動

應對原則：阻擋管控威脅、偵測管理風險、例外申請責任

Risk Management

裡子
Problem

風險管控、**主動**偵測
幫公司**賺錢或省錢**？
公司利益、開源節流

Compliance

解決問題
Solution

遵法不觸法/被告
公司省麻煩、解決問題？
幫**老闆**省心、營運順利

不怕辛苦
怕未解決

幫**老闆**做面子？
提升**專業正面**形象
股價/生意**跟著**水漲船高

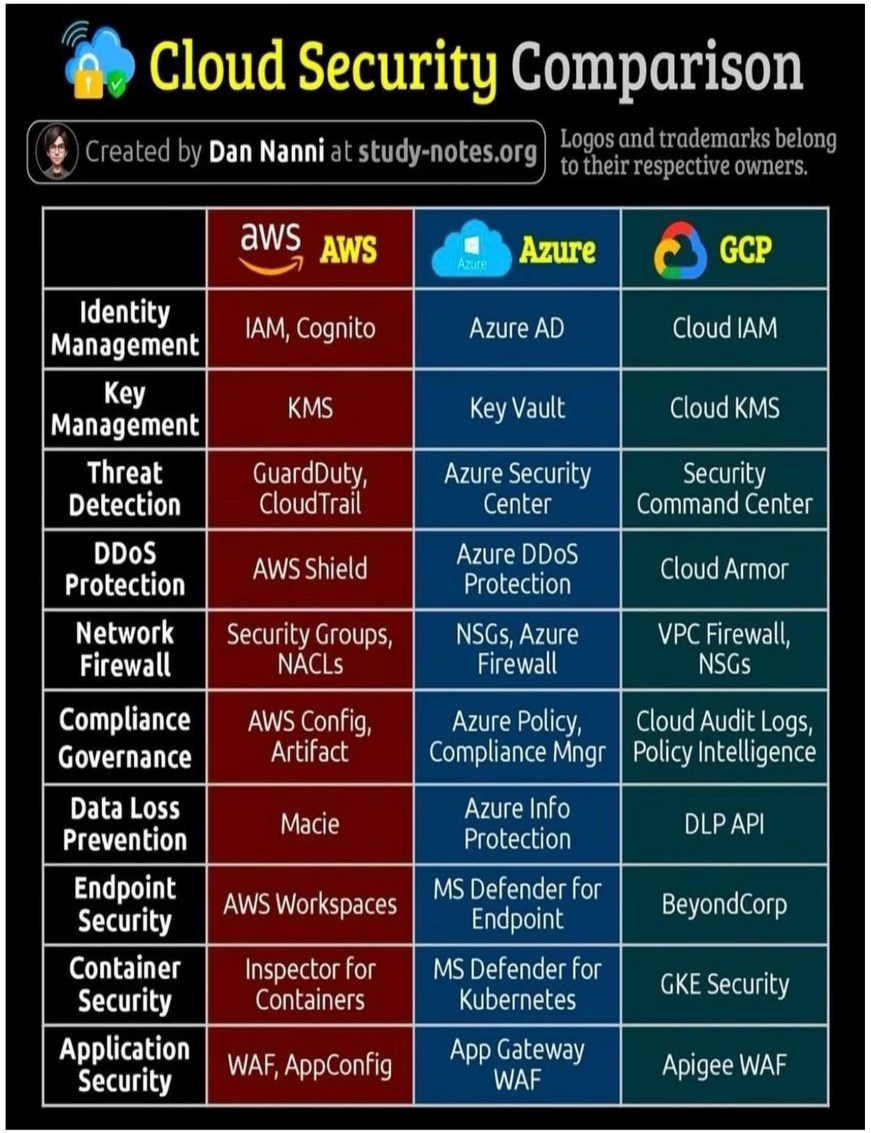
面子
Market

治理：**善用**每人**特性**
公司**經營核心**？
不得不存在部門？

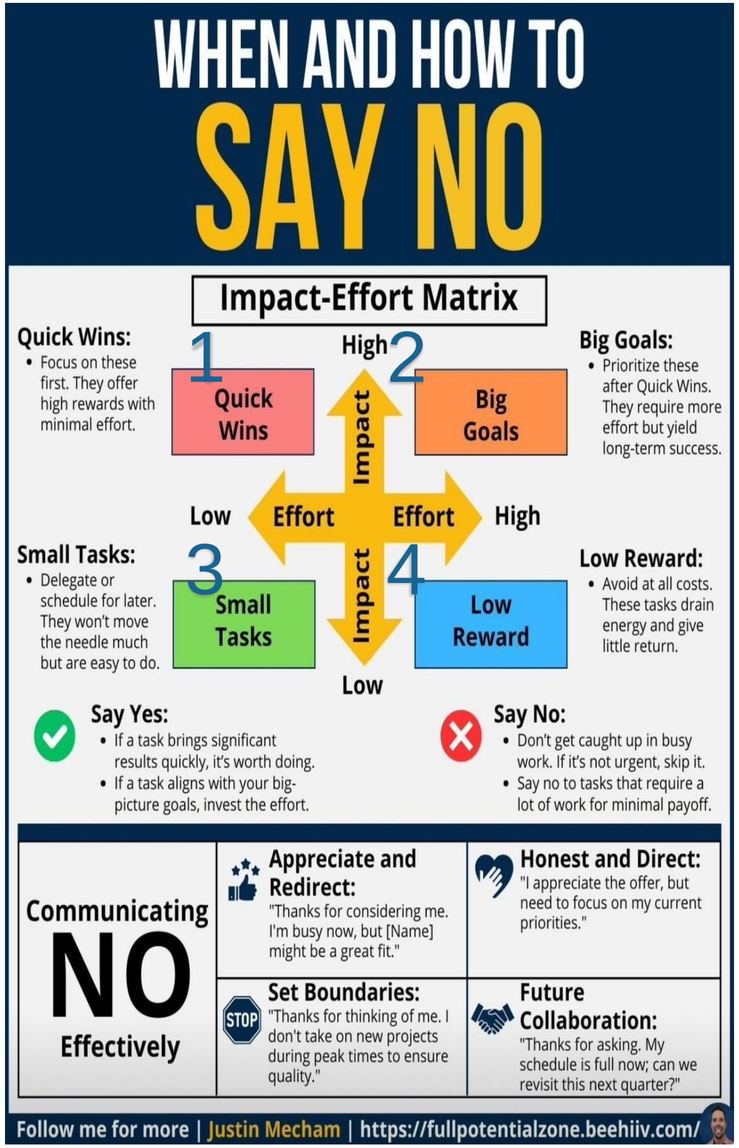
部門角色
Mission

Governance

下一步維運(現實殘酷)：攻不破、打不穿(理想美好)



	AWS	Azure	GCP
Identity Management	IAM, Cognito	Azure AD	Cloud IAM
Key Management	KMS	Key Vault	Cloud KMS
Threat Detection	GuardDuty, CloudTrail	Azure Security Center	Security Command Center
DDoS Protection	AWS Shield	Azure DDoS Protection	Cloud Armor
Network Firewall	Security Groups, NACLs	NSGs, Azure Firewall	VPC Firewall, NSGs
Compliance Governance	AWS Config, Artifact	Azure Policy, Compliance Mngr	Cloud Audit Logs, Policy Intelligence
Data Loss Prevention	Macie	Azure Info Protection	DLP API
Endpoint Security	AWS Workspaces	MS Defender for Endpoint	BeyondCorp
Container Security	Inspector for Containers	MS Defender for Kubernetes	GKE Security
Application Security	WAF, AppConfig	App Gateway WAF	Apigee WAF



https://www.linkedin.com/feed/

Thanks!

Do you have any questions?

高大宇 教授/博士
dayukao@gmail.com

TEAM
CYBERSECURITY

1. 退居第三民不與官鬥：
審時度勢，實現永續經營產業
2. 團隊建立的雁群合作：
一個人走得快；一群人走得遠
3. 同盟管理的領導策略：
聯合次要對手，對抗主要對手