「數位轉型　資安共行」

數位轉型下的資安風險管理

主講人

國立雲林科技大學

張宏昌

講師介紹

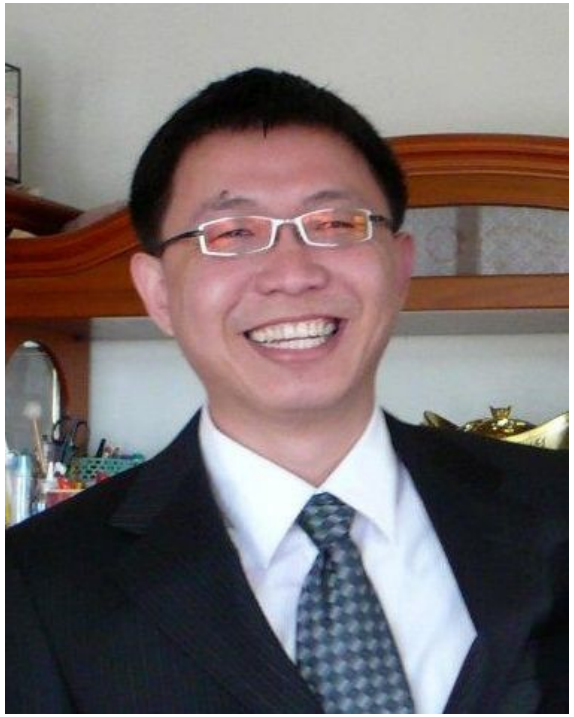
姓名: 張宏昌

現任:

雲林科技大學 資工系 助理教授
雲安全(資安) 創辦人
創璿科技(人工智慧) 技術顧問

經歷:

中央研究院 資創中心 專案研究員
福懋科技 研發中心主管



雲安全-國立雲林科技大學衍生新創公司

專注研發 / 守護資安

Content

01

數位轉型的機會與挑戰

「數位轉型　資安共行」

新戰場的入場券：數位轉型

微軟CEO曾說COVID-19讓企業數位轉型加速五年以上，但是數位轉型絕對不只是改變辦公模式和雲端應用而已，對於企業主來說有更深層的意義：數位化攻擊將成為重挫商業的最有利武器之一。

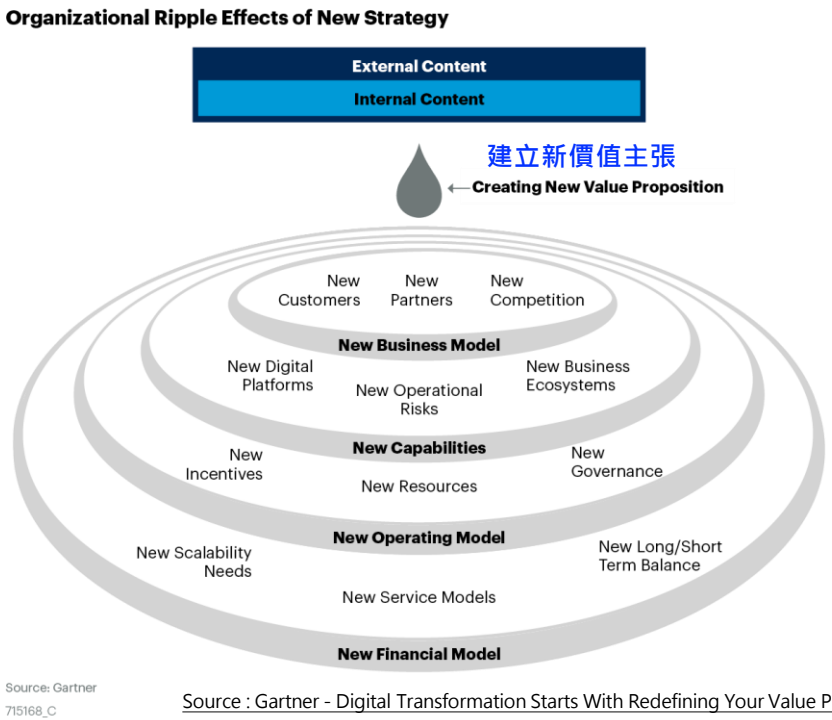
後疫情時代，企業更著眼於提高生產力、降低成本，以強化競爭優勢及可持續性，因此資訊環境的升級成為取得新戰場的入場券。自由系統根據在資訊產業的服務經驗，以及疫情期間協助數百間導入數位升級的解決方案，歸納出數位升級可以為企業帶來的競爭優勢：

數位轉型是企業強化競爭力的關鍵戰略

四大關鍵策略

耕耘客戶、激力員工、運作優化、產品轉型

Source : IDC Worldwide Semiannual Digital Transformation Spending Guide.



Source : Gartner - Digital Transformation Starts With Redefining Your Value Proposition

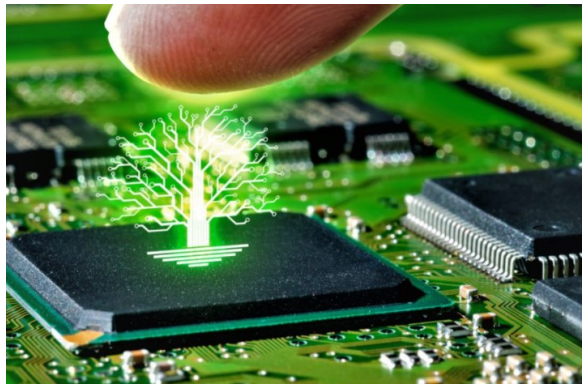
大量利用資通訊技術(ICT)與聯網技術，涵蓋客戶、營運、產品

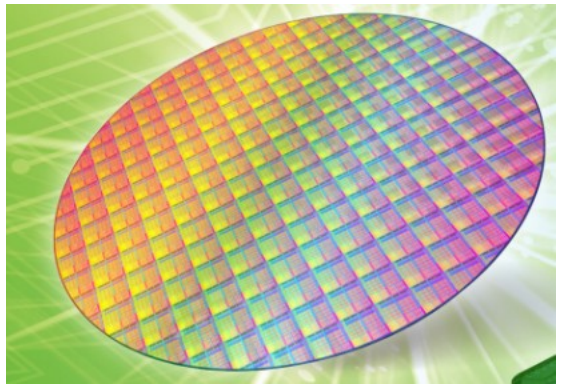
數位轉型下的資安思維

- 新興技術的使用與資訊安全的相對應
- 進階威脅攻擊持續發酵
- 已知問題但仍未做好準備

首當其衝的六大產業

面臨後疫情時代的台灣企業，不同產業都擁有各自的限制，使得企業在下優化資訊環境的決策窒礙難行，綜合數位升級及資訊安全佈署的必須性及急迫性，自由系統執行長俞伯翰表示，電子零組件業、資訊科技業、半導體產業、製造工業、軟體服務和生技業等產業為需要優先考量的產業。





四大指標檢視疫後資安新挑戰

「2020年在疫情影響下，加速企業數位轉型的進程，企業將可能面臨雲端風險升高與逐漸增長的複合式目標攻擊。」 - 趨勢科技台灣區暨香港區總經理洪偉淦

指標一、落實遠距辦公安全防護機制

指標二、由上而下「零信任」擴大資安防守範圍

指標三、建立監控體系轉被動處理為主動追蹤

指標四、慎選合適的資安服務供應商

各種行業數位轉型的機會與資安挑戰

金融4.0

- **行動支付**
  - ✓Tokenization強化安全
- **機器人理財**
  - •大數據&人工智慧決策
- **電子貨幣**
  - ✓區塊鏈防止偽冒

- 2016.07一銀ATM受駭
- 2017.02券商遭DDoS攻擊勒索比特幣
- 2017.06 ATM與烏克蘭央行感染NotPetya勒索軟體
- 2017.10遠銀SWIFT受駭

金融資安威脅

工業4.0

- **智慧工廠(全自動生產)**
  - ✓物聯網控制、調度設備
  - ✓大數據&人工智慧制定決策

- 2014.12德國鋼鐵廠受駭導致高爐損毀
- 2017.04美國AW North Carolina工廠遭惡意程式入侵停擺，駭客威脅關閉產線勒索贖金

工業資安威脅

物流4.0

- **智慧物流**
  - ✓物聯網自動配貨(物流中心)
  - ✓物聯網自動配送(無人機)
  - ✓大數據&人工智慧制定決策

- 2016.10 趨勢研究人員展示如何以Software Define Radio (SDR)脅持無人機
- 2017.06 貨運業者Fedex及Maersk感染NotPetya勒索軟體，致業務停擺損失上億美元

物流資安威脅

零售4.0

- **網路商店/行動購物**
  - ✓大數據、AI分析預測需求
- **無人商店**
  - ✓物聯網感測所購商品
  - ✓行動支付加速結帳流程

- 2013-2014 Target與Home Depot PoS受駭，致信用卡資訊外洩
- 2017.03 MajikPOS感染PoS，竊取信用卡資料
- 2017.08 ERPScan研究人員發現SAP與Oracle PoS存在漏洞可更改商品價格

零售資安威脅

各種行業數位轉型的機會與資安挑戰

•行動支付

✓Tokenization強化安全

•機器人理財

•大數據&人工智慧決策

•電子貨幣

✓區塊鏈防止偽冒

金融4.0

- •DDoS攻擊中斷服務
- •APT攻擊入侵企業
- •勒索軟體威脅重要資料
- •網站、服務存在弱點
- •ATM受駭

金融資安威脅

•智慧工廠(全自動生產)

✓物聯網控制、調度設備

✓大數據&人工智慧制定決策

工業4.0

- •物聯網裝置受駭
- •基礎設施遭受威脅
- •勒索軟體威脅重要資料導致業務停擺

工業資安威脅

•智慧物流

✓物聯網自動配貨(物流中心)

✓物聯網自動配送(無人機)

✓大數據&人工智慧制定決策

物流4.0

- •物聯網裝置受駭
- •勒索軟體威脅重要資料導致業務停擺

物流資安威脅

•網路商店/行動購物

✓大數據、AI分析預測需求

•無人商店

✓物聯網感測所購商品

✓行動支付加速結帳流程

零售4.0

- •網站、服務存在弱點
- •POS機受駭
- •物聯網裝置受駭

零售資安威脅

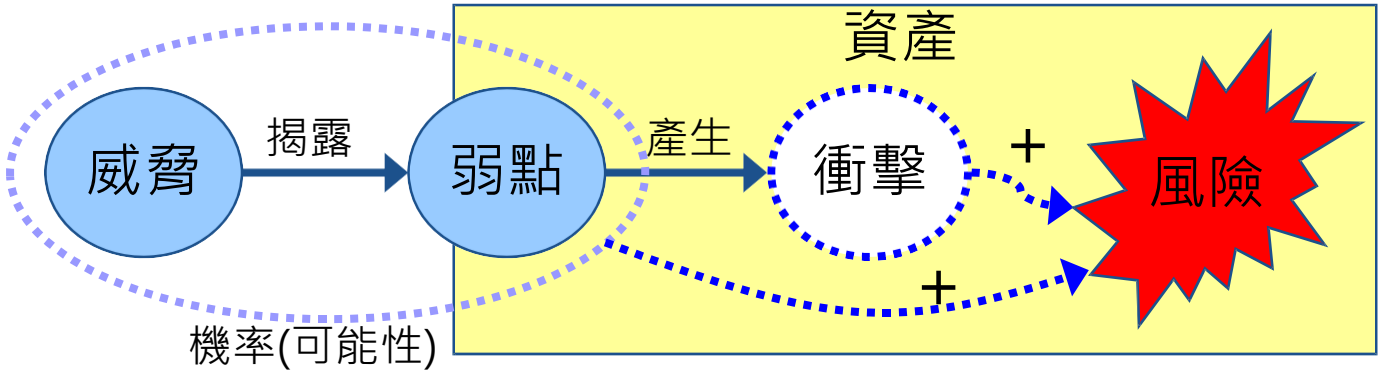
02

資安風險隨之而來

「數位轉型　資安共行」

風險的定義

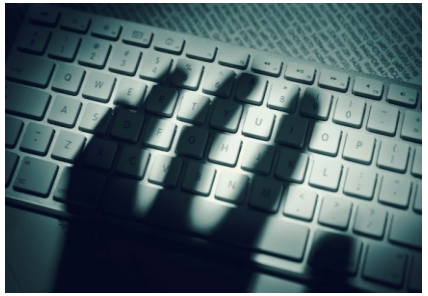
- 所謂「風險」是指「威脅」利用其相對應「脆弱性」直接或間接造成組織一個或一群「資訊資產」受到「衝擊(Impact)」的「可能性」



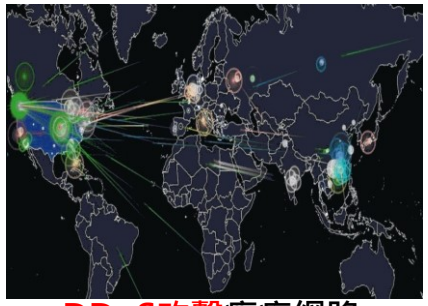
- 風險透過「衝擊」與其「可能性」兩個因素的結合來定義其影響程度或損害程度
- 風險管理的目標

  在最低的防護成本投入下獲得最優化的安全性(最優化非最強固，而是最合適)

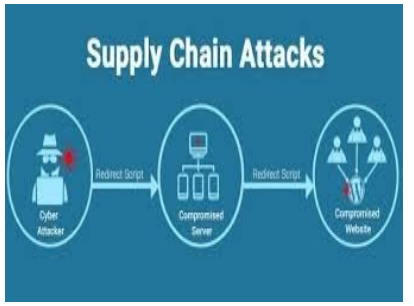
台灣面對大量的網路威脅



組織型駭客以APT攻擊竊取機密資料



DDoS攻擊癱瘓網路運作



駭客透過供應鏈攻擊進行滲透

漏洞攻擊仍是駭客的入侵捷徑

OT環境資安威脅日增且落地

IoT物聯網裝置受駭頻傳

組織型駭客以APT攻擊竊取機密資料

2018/3司法院及所屬機關遭APT攻擊事件：
受感染的電腦數目為243台，其中90%是XP系統，10%為windows2003，受入侵的法院總數是29個法院

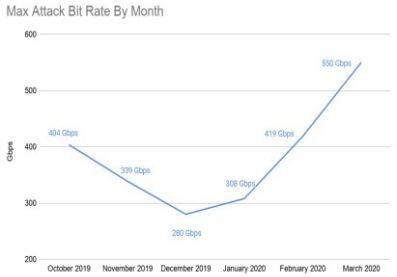
2019/6銓敘部個資外洩餘24餘萬筆

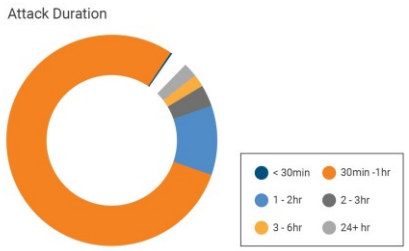
APT：Advanced Persistent Threat

國內DDoS最大攻擊流量上升至487Gbps

全球 DDoS攻擊趨勢(2020Q1)：

- 2020 DDoS攻擊**頻率持續上升**，近期最大攻擊流量達**550Gbps (2020/03)**
- 主要攻擊類型**SYN & ACK** 攻擊 (72%) ，其次為CLDAP 攻擊(5.3%)
- 遭受DDoS攻擊的國家，前三名為**中國**、美國和香港
- 全球殭屍網路分布，以**美國**居第一 (39.93%)、其次荷蘭(10.07%)及德國 (9.55%)
- 殭屍網路病毒目標從終端**IoT設備**和**嵌入式設備**朝向**企業級物聯網裝置(NAS、Router等)**
- 三月下半月的DDoS攻擊次數比上半月多出55%，三月開始，94%的流量均有高達**300Gbps**到**400Gbps**

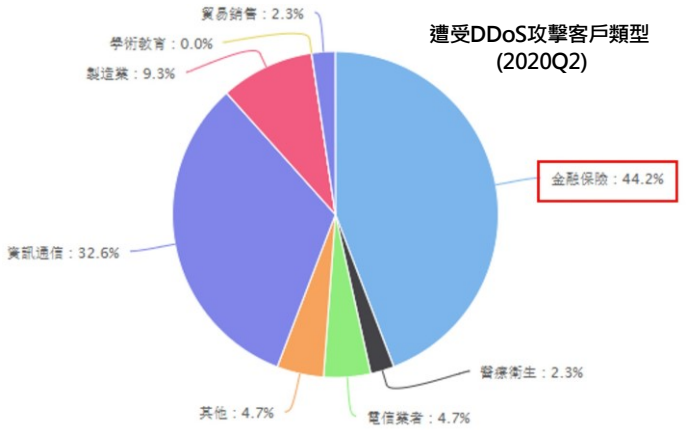


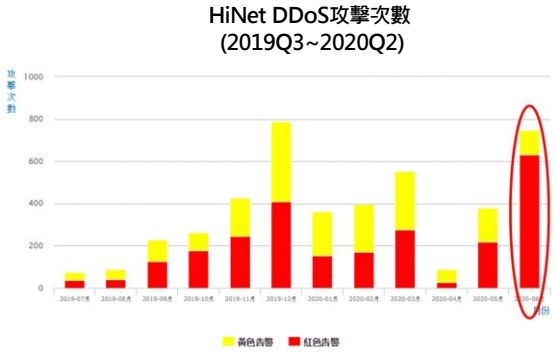


來源: Cloudflare Network-Layer DDoS Attack Trends for Q1 2020

CHT Security SOC 觀察(2020 H1)：

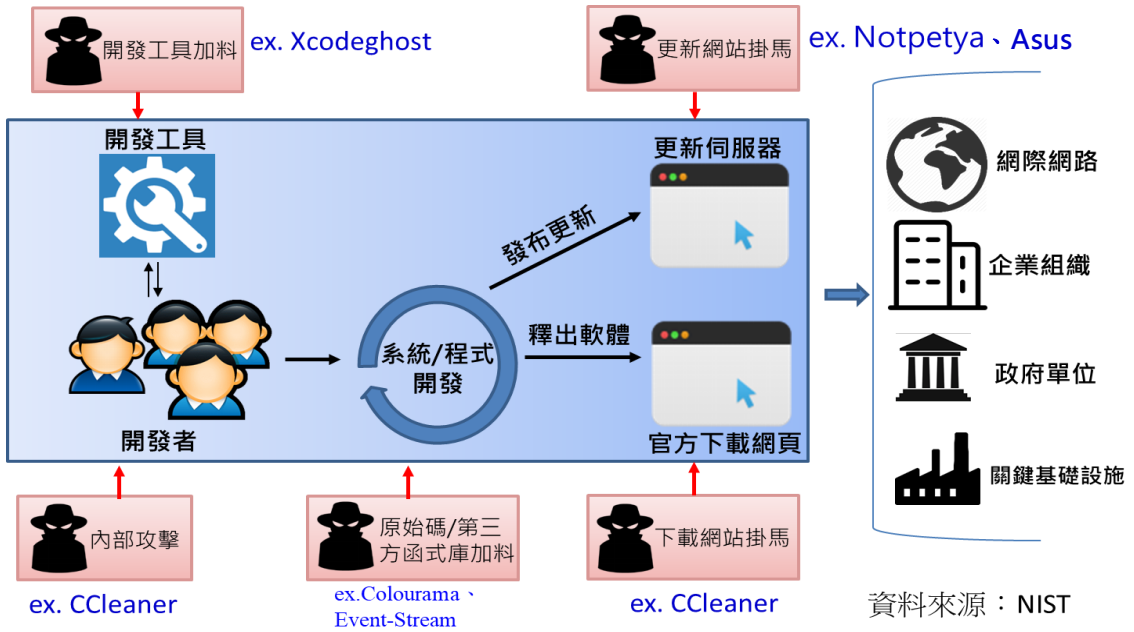
- 國內2019 Q2 **平均每天發生約420次**攻擊，6月份每天攻擊次數高達749次
- 2020年**1月最大攻擊量達487Gbps** ，**UDP Flooding**為大宗
- 遭攻擊對象偏重**金融保險業(44.2%)、資訊通信(32.6%)** ，其次為製造業、電信業、醫療衛生等
- 未來趨勢為**混合式**的反射放大攻擊，**IoT 設備**易於入侵且不易發現，成DDoS攻擊來源主力，建議對外服務系統及網站均須**建立DDoS防護機制**
- 最長攻擊時間460分鐘 (2020/01)、平均攻擊時間<30分鐘





利用供應鏈攻擊進行無差別感染、目標式攻擊

- **攻擊手法**
  - 開發工具加料
  - 更新/下載網站被掛馬
  - 原始碼/第三方函式庫遭加料
  - 內部受駭
- **案例：**
  - 2019/3華碩電腦更新機制及雲端儲存遭駭，藉以滲透進入國內諸多政府與民間企業



企業的資安風險 – 彼的威脅、己的漏洞

威脅說明(Threat)	漏洞說明(Vulnerability)
個人或團體(駭客、網軍、競業、惡意員工、頑童...)因金錢、政治理念、商業機密、犯罪心態等目的，蓄意或不小心的作為，導致企業的損害或危險	企業自己的**網路有管理缺口、系統有漏洞、應用程式寫得不安全或留了後門，甚至是員工缺乏警覺性，導致企業曝險(浮現可被攻擊的介面)**

Risk = Threat x Vulnerability x Impact

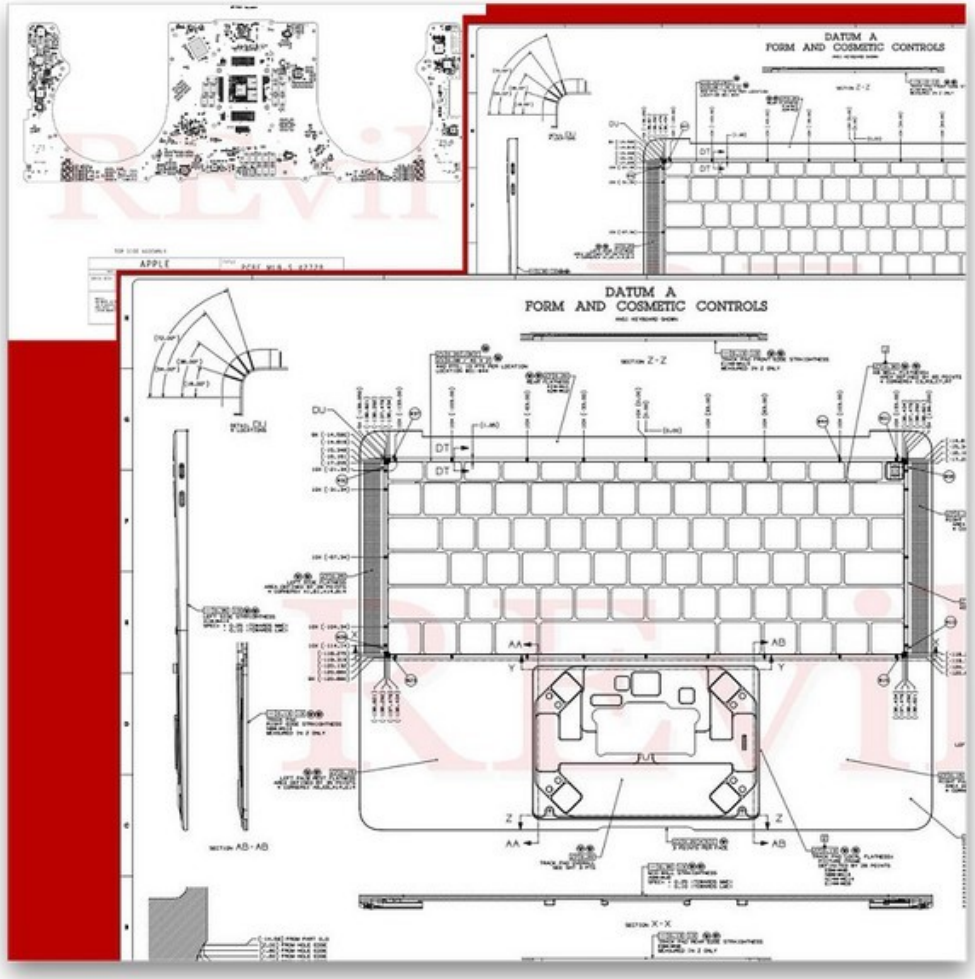
資安風險 = 內外威脅 x 自身弱點 x 影響衝擊

如果威脅是不可控的，企業的重心就應該回到自身的「弱點管理」，以降低風險

台積電3天痛失26億元的教訓！如何不重演機台中毒慘劇，從半導體一哥變身資安要角？

台積電晶圓廠房

駭客轉型企業化-中小企業亟須政府奧援

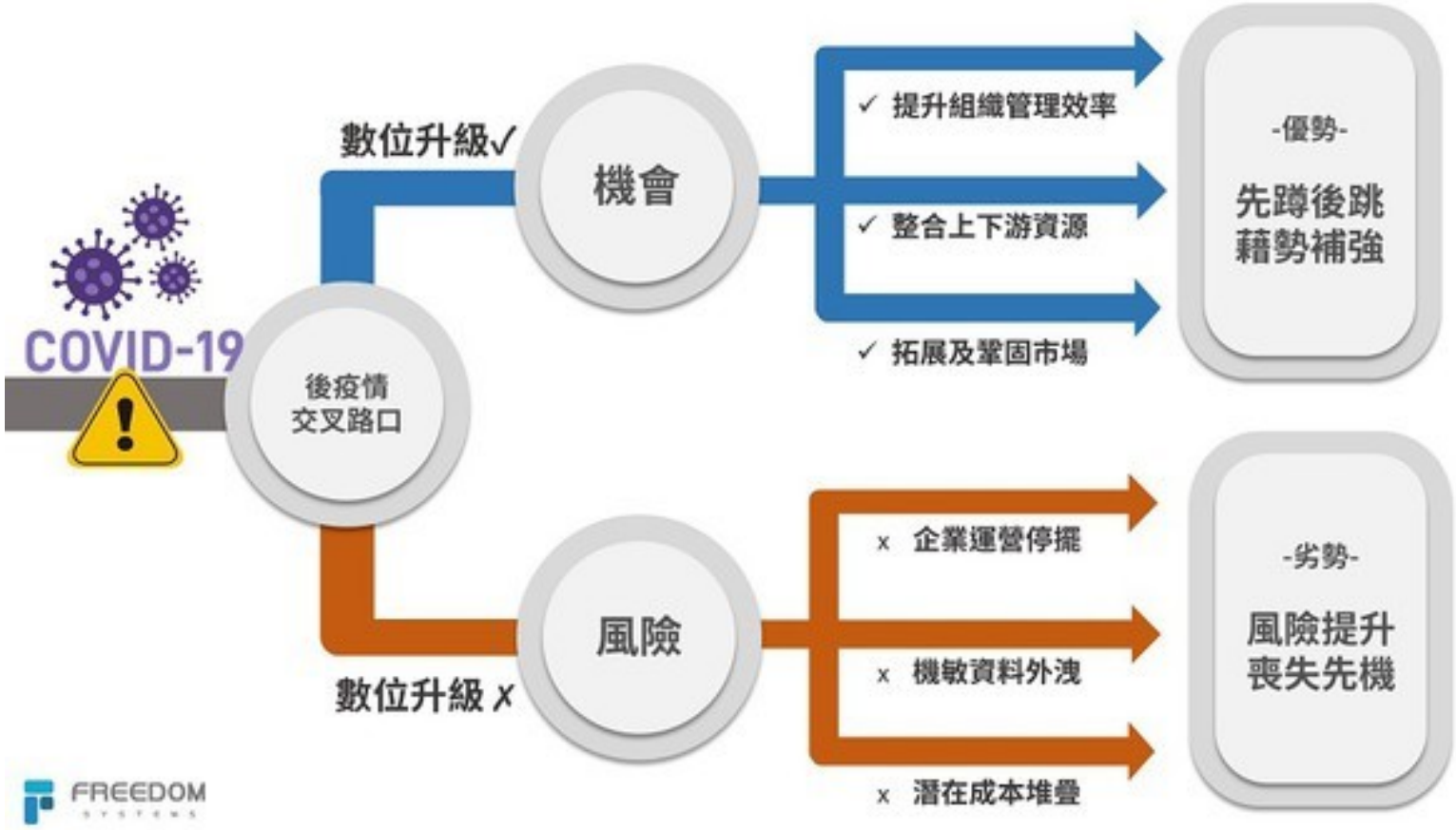


近年來駭客組織逐漸企業化和分工細密，
除了開發出更快加密及竊取資料的軟體，
還為此發布新聞稿，提供下線所需工具包，
事成後從贖金中支付一定比率給組織。
（source：static.wixstatic.com）

產官法人齊力-落實「資安即國安」策略

經濟部工業局針對「工控安全」主題展示工業控制模擬系統，並結合資安攻擊情境模擬廠區的運作流程及網路、測試環境，發展台灣自主工控情境腳本及培訓工控資安專業人才

聰明評估+策略放遠+趁勢補強



03

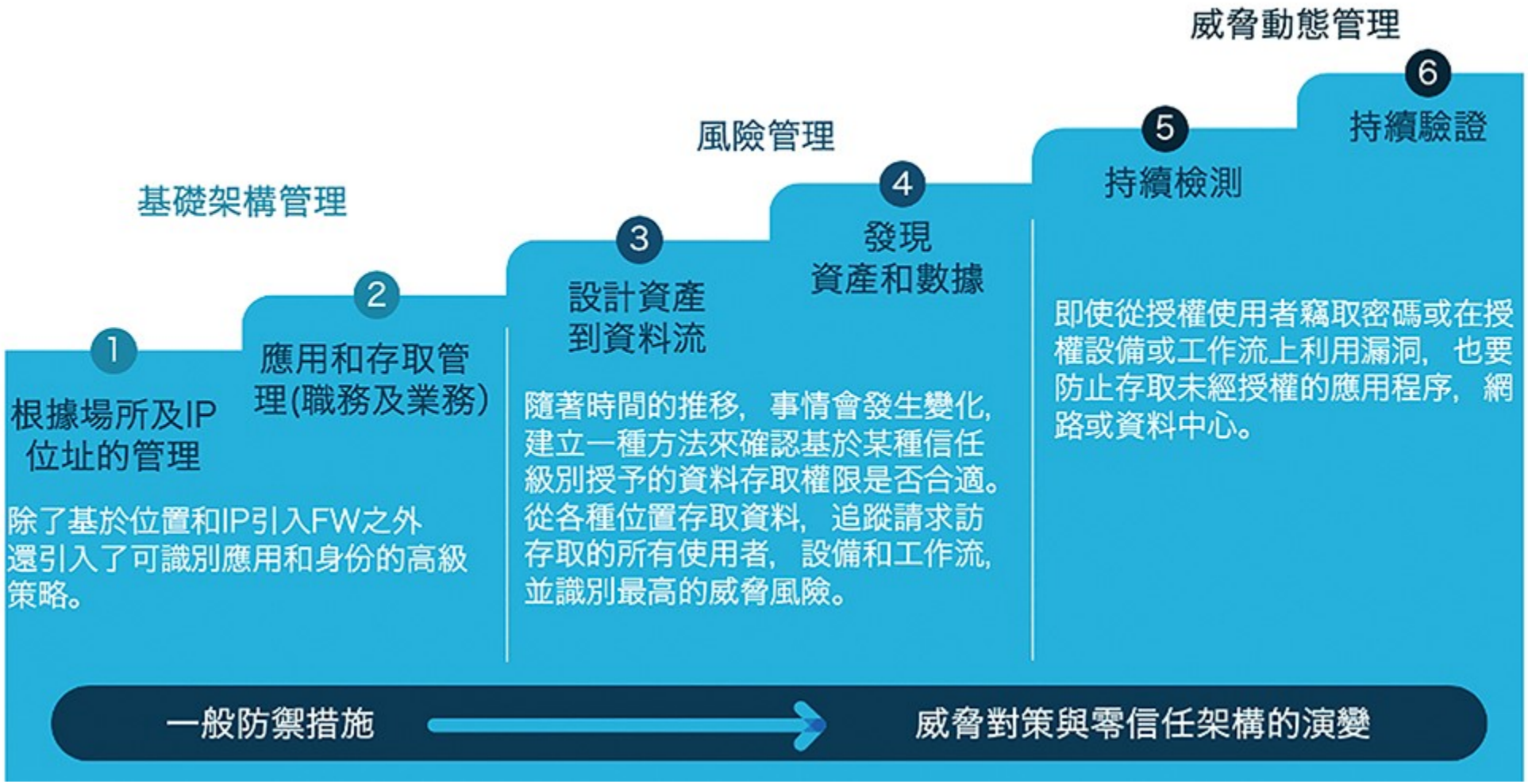
資安風險下的零信任架構

「數位轉型　資安共行」

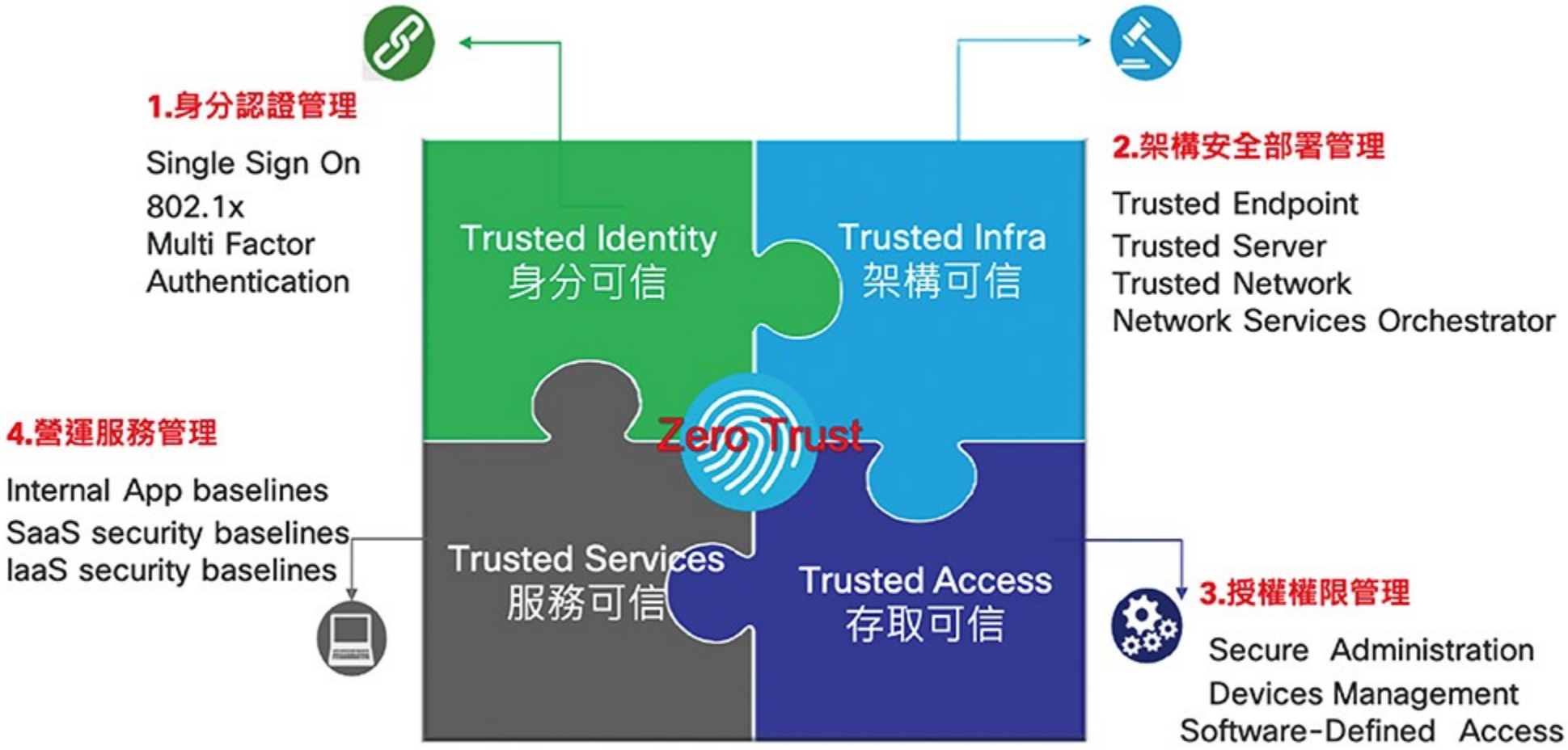
零信任安全架構

不管是連接裝置、應用程式或是組件，都視為威脅向量，必須經過認可及驗證

零信任安全架構成熟模型



零信任安全架構四大支柱

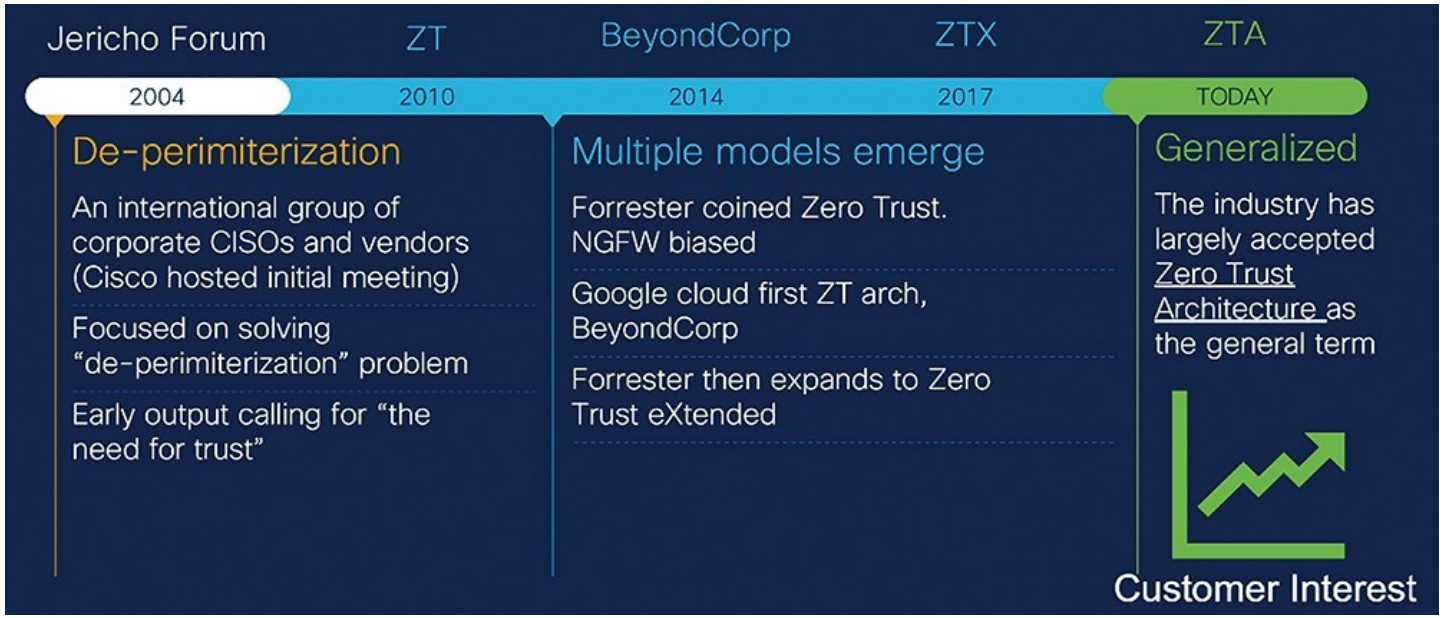


零信任安全模型 – 三個核心基礎概念

1. 不論身在何處，須確保所有資源都是以安全的方式存取
2. 採用最低權限的策略，並且嚴格實施存取控制
3. 檢測與記錄所有流量

by John Kindervag, 2010

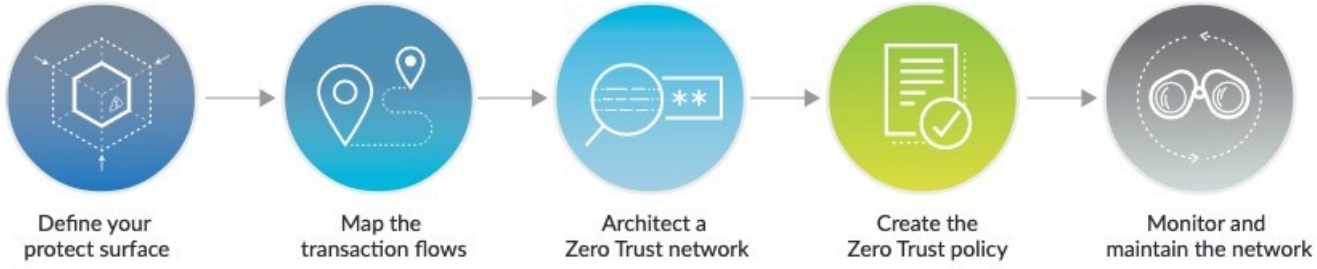
Never trust, Always verify



零信任資安架構及核心組成元件

The Five-Step Methodology

Source : Palo Alto Networks

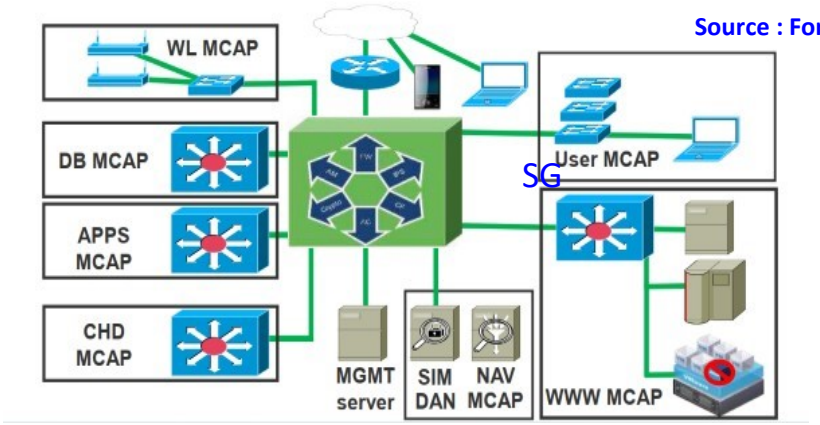


零信任架構核心元件

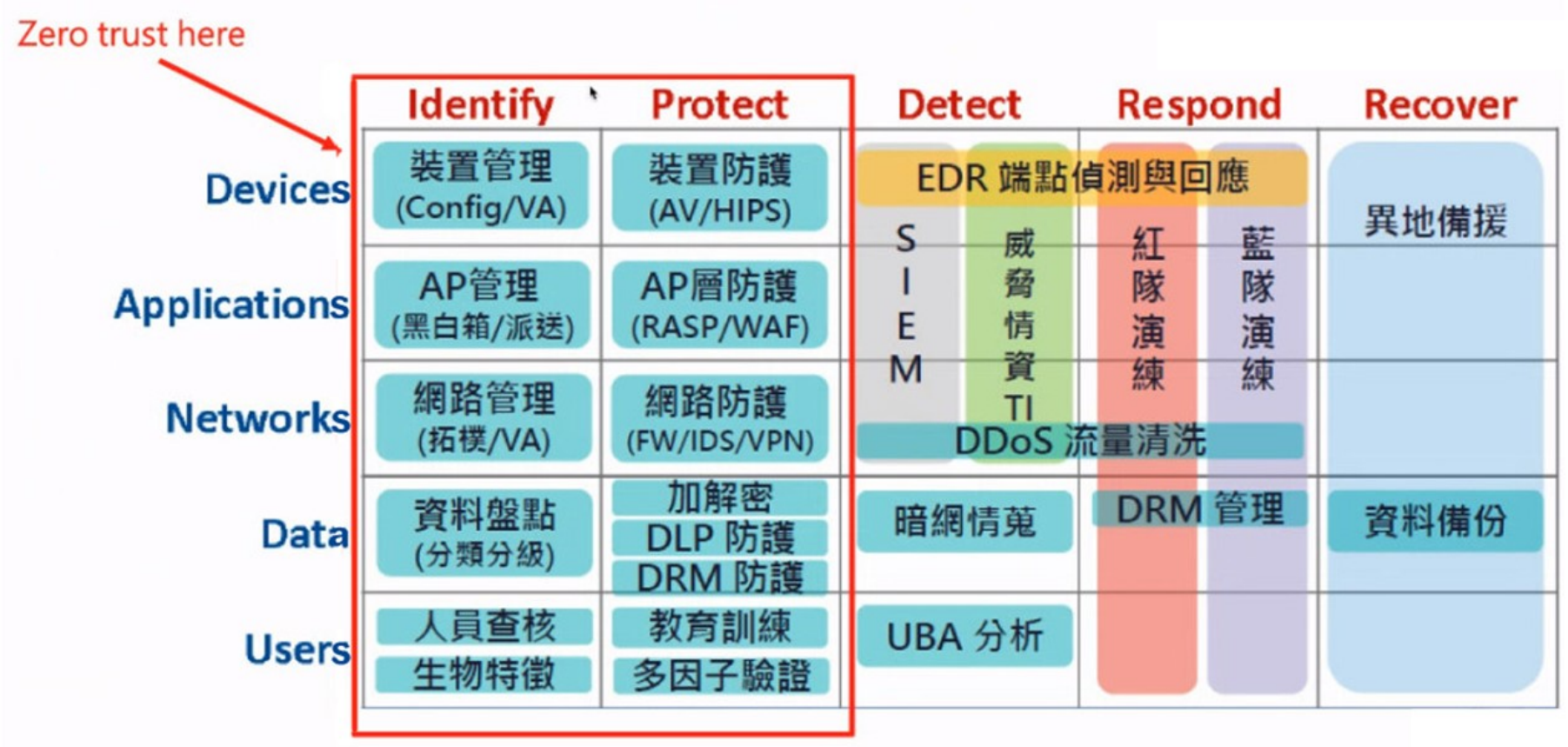
網路分區閘道 (SG)
微核心與邊界 (MCAP)
集中管理
資料擷取網路(DAN)

SG : Segmentation Gateway
MCAP : Micro Core and Perimeter
DAN : Data Acquisition Network
NAV : Network Analysis and Visibility
SIM : Security Information Management

Source : Forrester's



從攻防角度看零信任網路安全



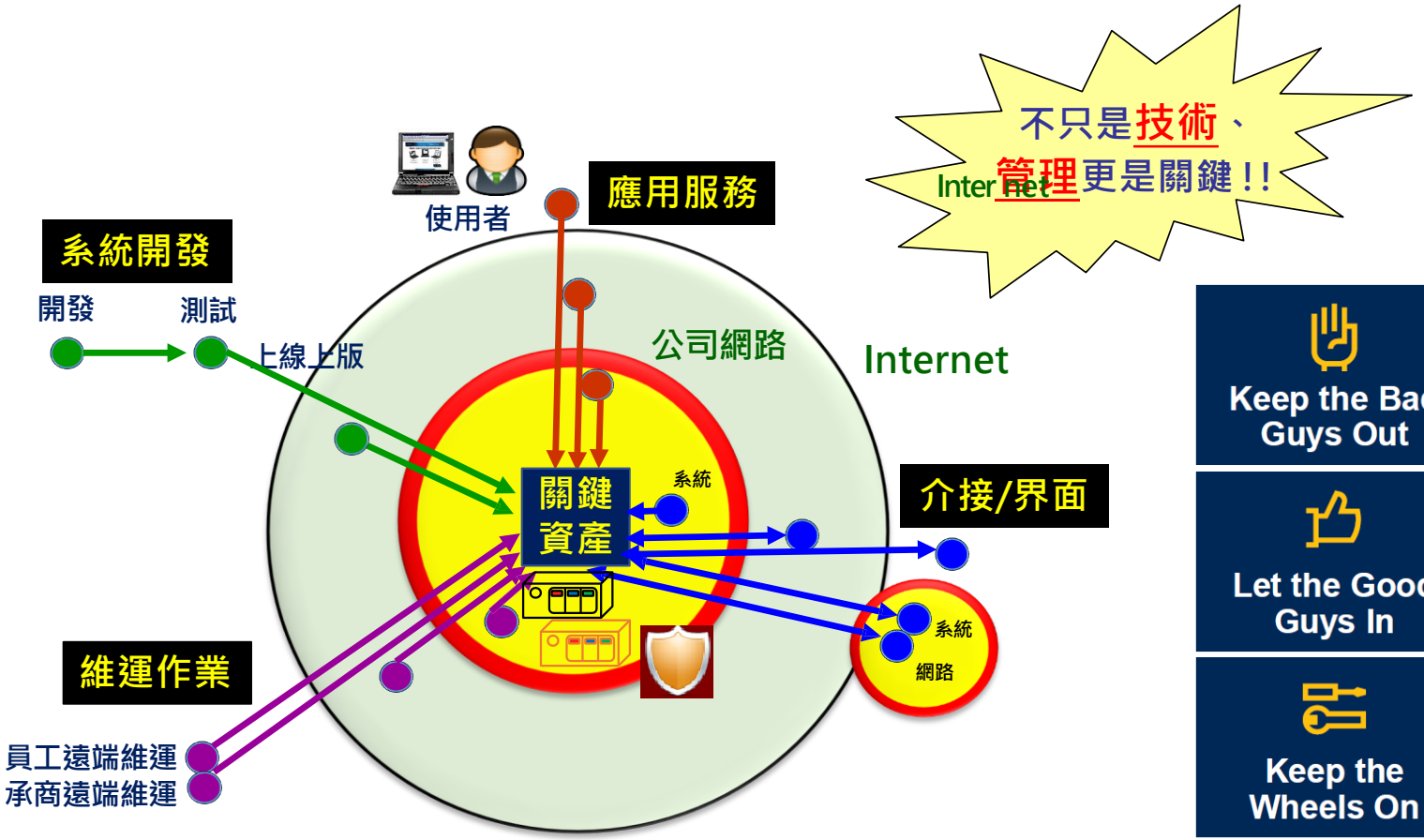
04

面對資安風險的管理策略

「數位轉型　資安共行」

企業面對資安議題的困境

挑戰：關鍵資產出入管控之複雜度



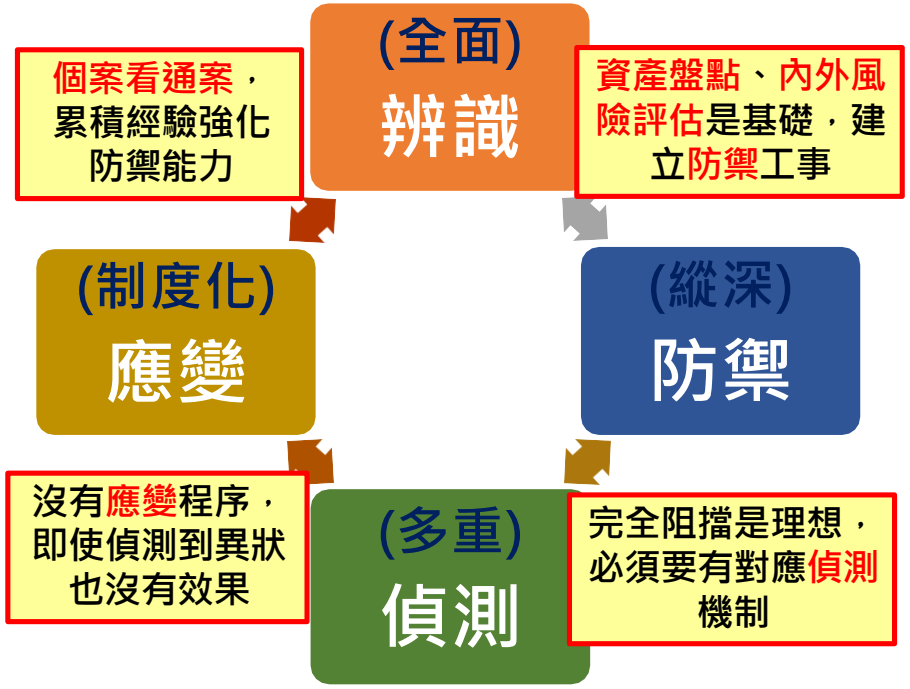
面對資安風險的因應作法

- 結合People/Process/Technology執行預測、防護、監控、應變工作
- Focus of Cyber-Risk Mitigation Activities Among **Top Performers**

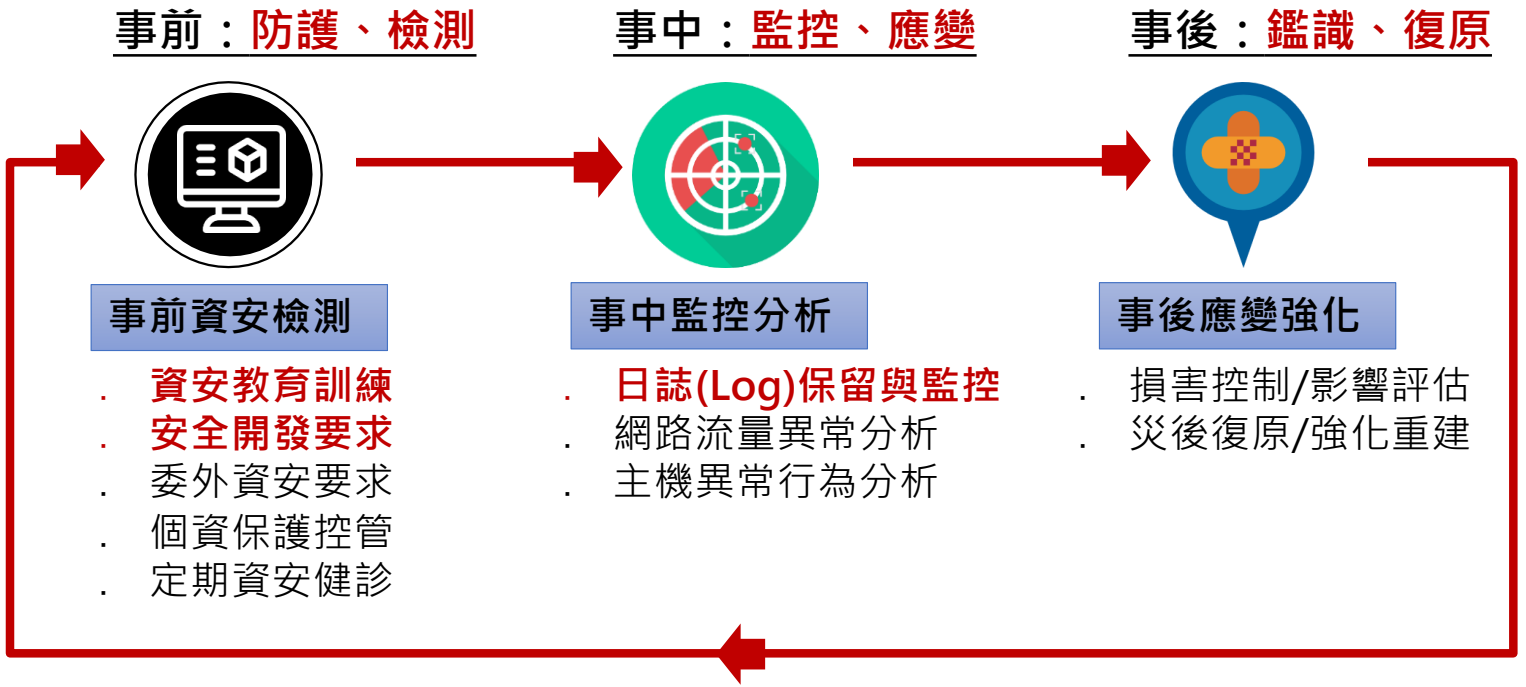
面對資安風險的因應作法

- 例如，選擇美國NIST網路安全框架（Cybersecurity Framework，CSF）為資訊安全的基準(baseline)， IPDRR

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

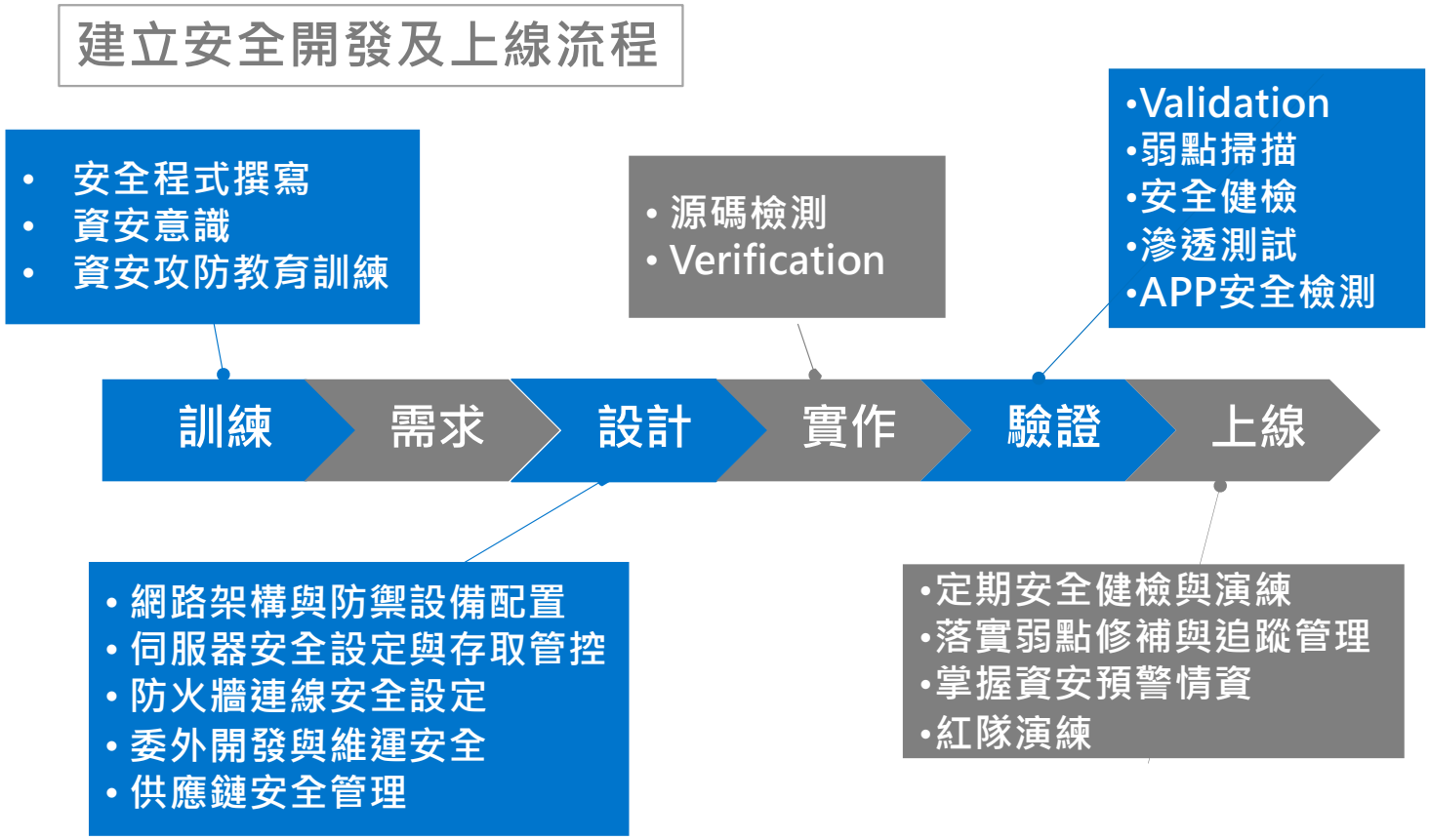


建立持續性的資安防護與評估機制



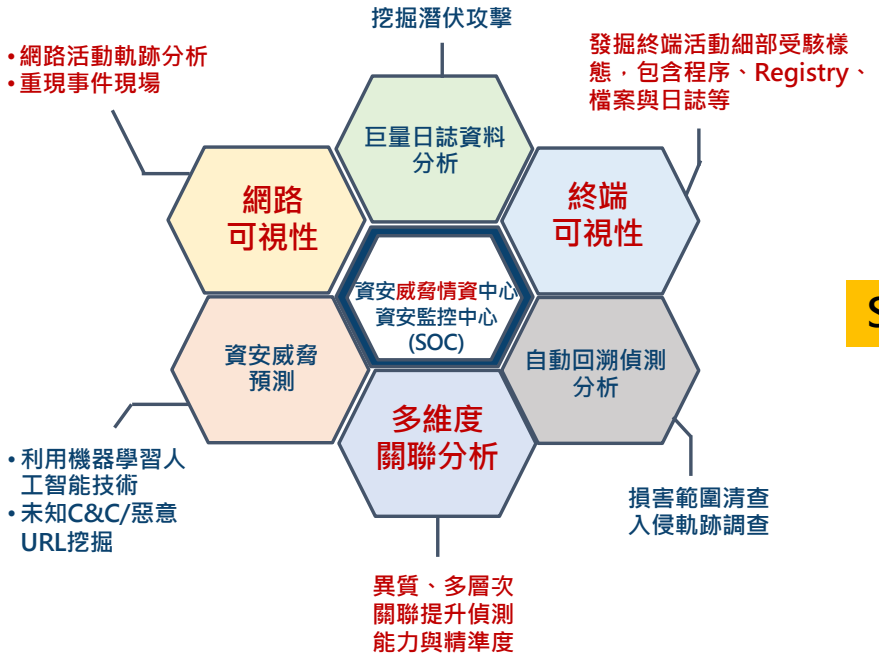
可以參考Gartner CARTA 持續性的適應風險和信任評估（Continuous Adaptive Risk and Trust Assessment），提高資安防護適應能力

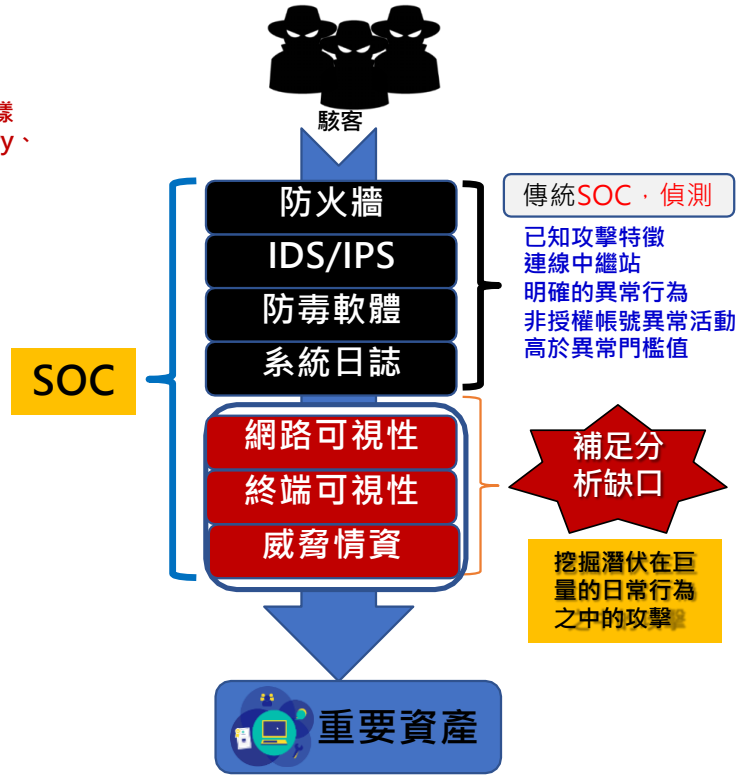
事前：開發安全的軟體與資安檢測



事中：即時監控異常活動與遠端調查應變

新世代SOC + MDR偵測應變服務





事中：即時監控異常活動與遠端調查應變

事件單即時通報、處理過程追蹤

事件追蹤管理系統效益

- **客製化**符合企業事件通報組織及處理機制
- **完整紀錄事件處理內容及各類型報表**，大幅降低日後稽核時間
- 管理人員可透過圖形化介面**即時掌控事件處理狀態**
- **帳號可與企業內LDAP整合**，提高安全性與方便性

提升整體通報效率高達5倍以上

縮短事件及弱點追蹤時間50%以上

事後：調查事件根因、災損與復原

事件應變與數位鑑識

1 現場訪談
- 了解案情背景資訊
- 了解現有資訊架構

2 損害控制
- 提供緊急阻擋威脅建議
- 資安設備租借支援(7天)

3 證據採集
- 消逝性/邏輯性資料採集
- 製作映像檔/證據資料備份

4 進階鑑識
- 各式Log/映像檔/記憶體/封包流量檢測
- 惡意程式逆向分析/沙箱檢測/線上資源)

5 損害評估
- 實體系統感染範圍評估(台數、網段數...)
- 資料洩漏範圍評估(數量、內容...)

6 快篩檢測
- 大範圍快速檢測是否有其他標的遭惡意程式感染、側錄及分析網路封包

7 災害復原
- 移除惡意程式
- 提供弱點修補建議

8 出具報告
- 解釋入侵管道/ 案件原委
- 出具改善建議

05

補充:資安價值評估

「數位轉型　資安共行」

資安保險

為您的企業量身打造客製化保單

中小企業資訊網路安全保險

1.違反資料保護義務

2.違反資訊安全義務

3.媒體錯誤行為

4.未遵守支付卡產業標準

5.危機事件調查及通知費用

6.預付抗辯費用

7.資料重建費用

8.調查費用

9.延長報案期間

10.受勒索損失

為您的企業量身打造客製化保單

中小企業資訊網路安全保險

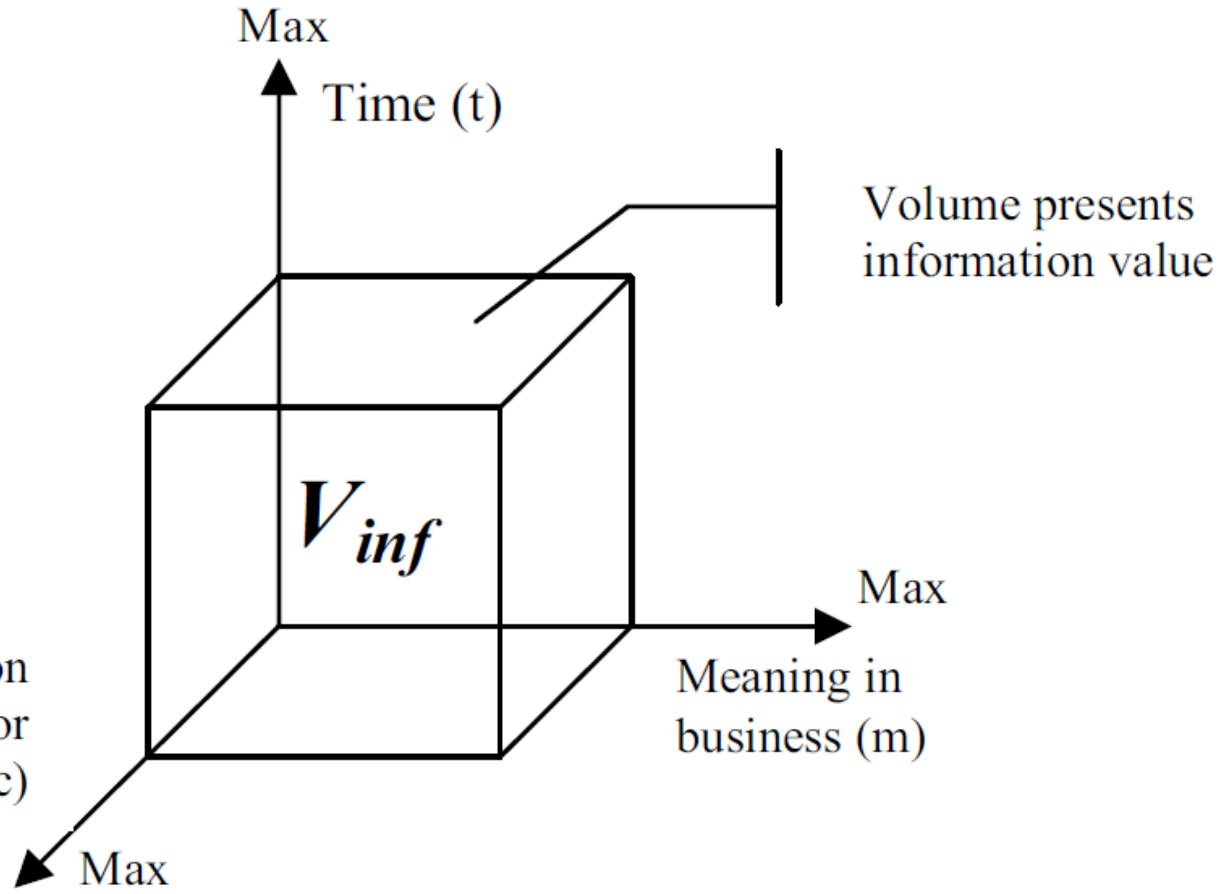
讓您大可不必默默地承擔公司因為網路資訊系統漏洞、員工疏失或有心人的刻意盜取，造成您企業重大損失與後續求償責任與相關費用支出。

下載條款

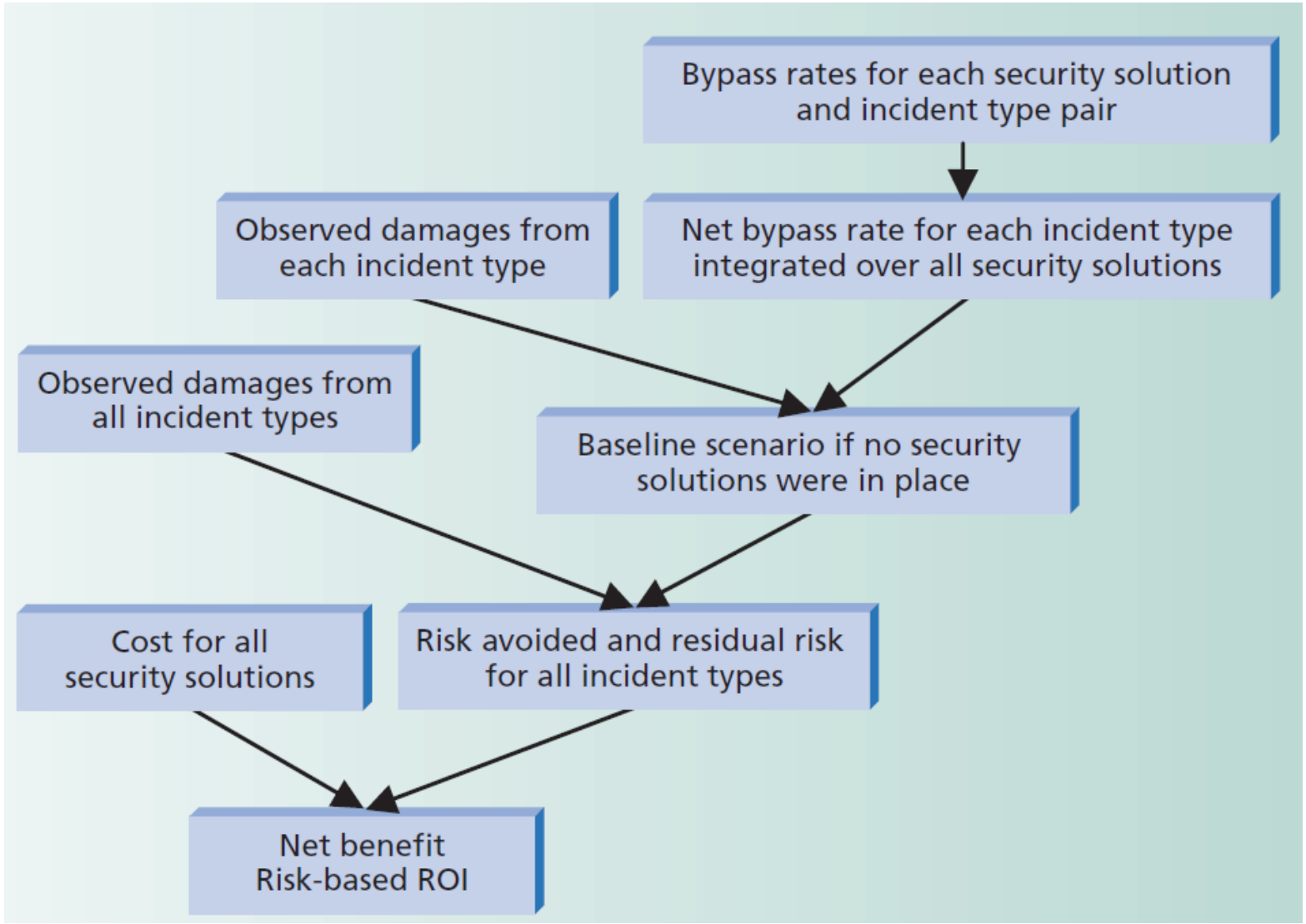
資安價值評估
無形資產鑑價
誰來評估?

Dimensions of information value

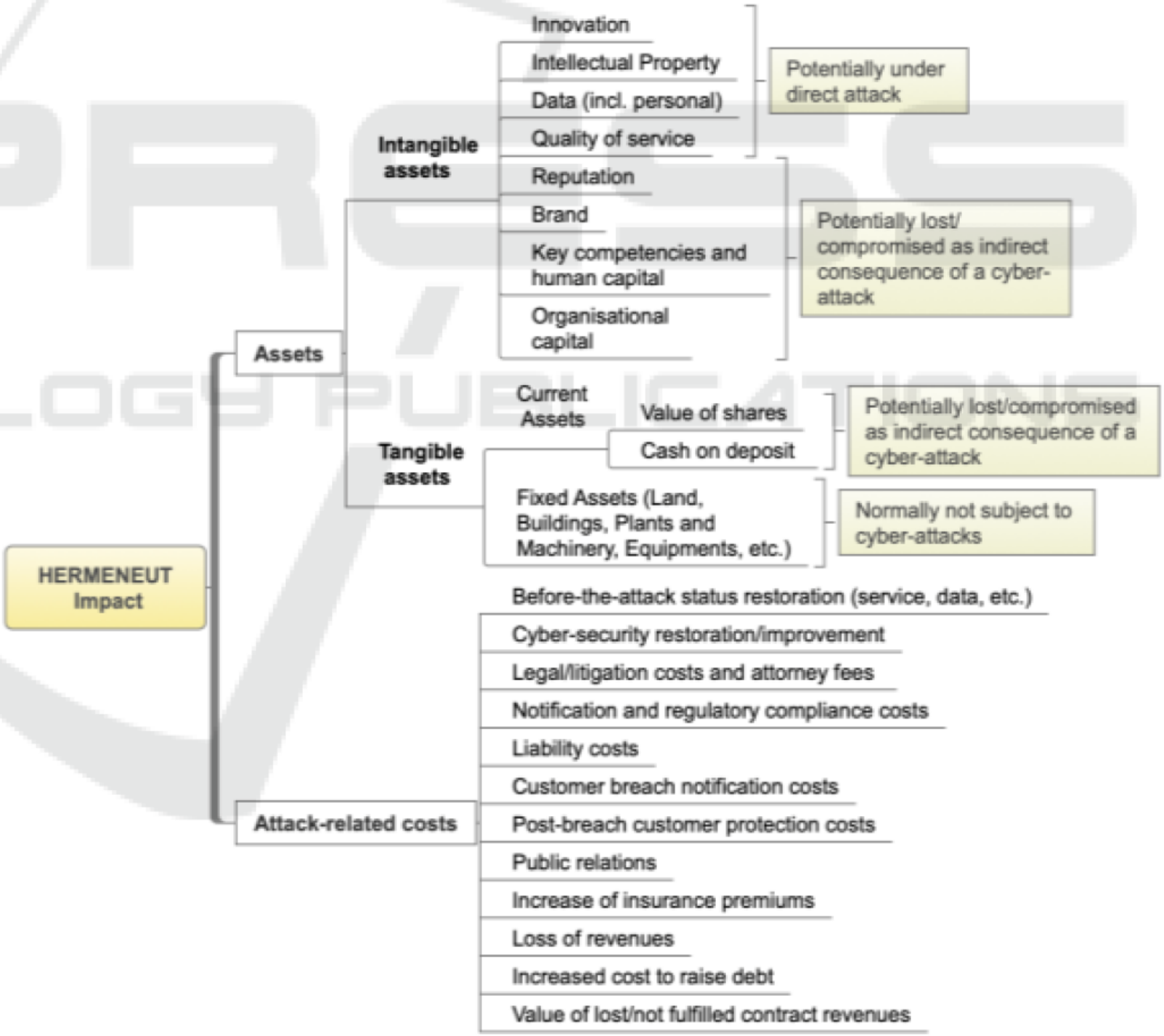
$V_{inf}=f\{m, t, c\}$



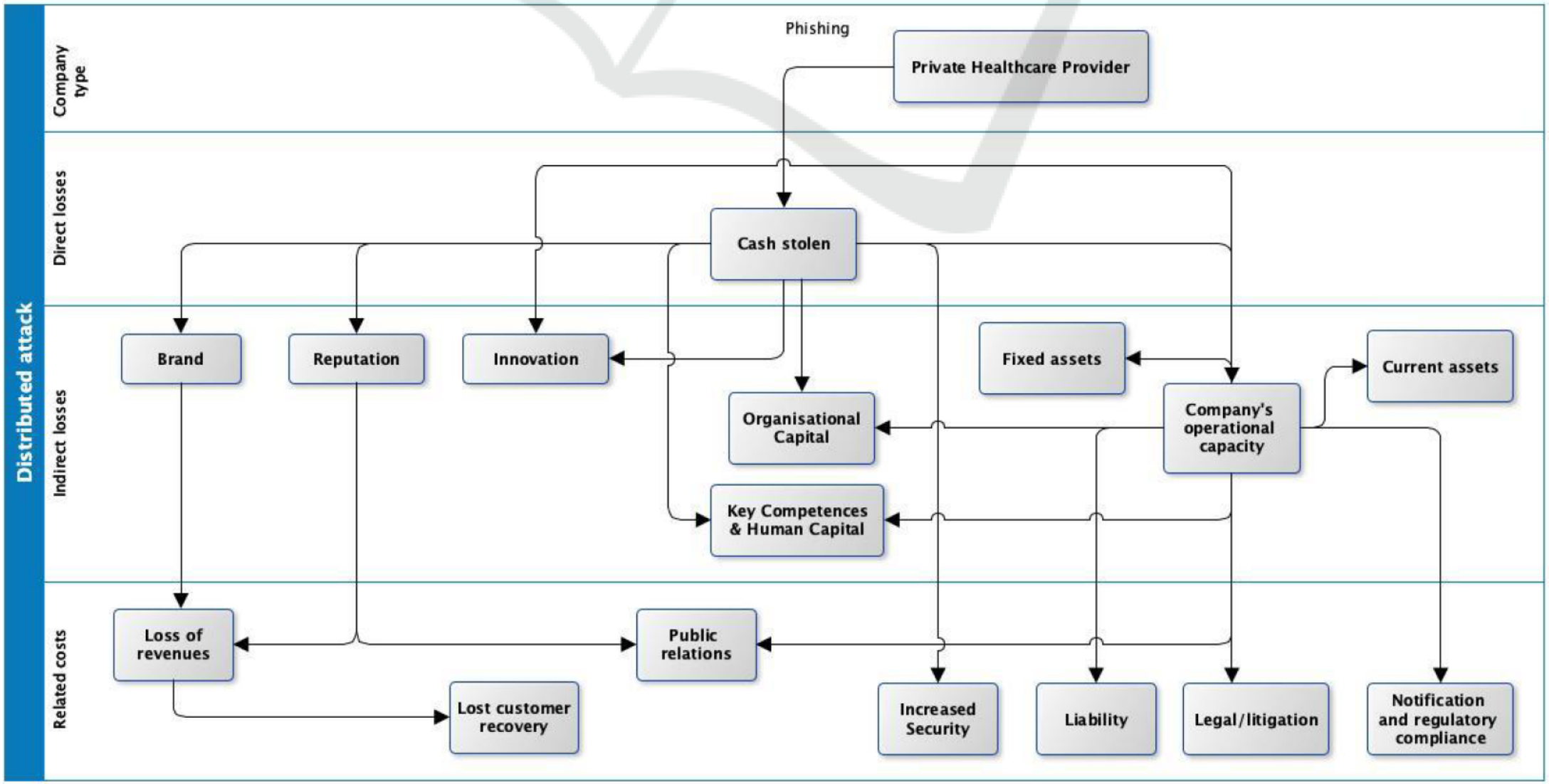
Basic process for estimating risk-based return on investment



HERMENEUT impact tree



Losses generated to a Private Healthcare Provider by a Phishing attack with cash stolen.



Information Asset Valuation Method for Information Technology Security Risk Assessment

Financial Focus	• revenues / employee ($) • revenues from new customers / total revenue ($) • profits resulting from new business operations ($)
Customer Focus	• days spent visiting customers (#) • ratio of sales contacts to sales closed (%) • number of customers gained versus lost (%)
Process Focus	• PCs / employee (#) • IT capacity – CPU (#) • processing time (#)
Renewal and Development Focus	• satisfied employee index (#) • training expense / administrative expense (%) • average age of patents (#)
Human Focus	• managers with advanced degrees (%) • annual turnover of staff (%) • leadership index (%)

「數位轉型　資安共行」

數位轉型下的資安風險管理

Thank you for listening.