

企業永續的資安思維



大綱

- 1 | 何謂企業永續？
- 2 | 企業永續目標實踐
- 3 | 數位轉型是現在進行式
- 4 | 數位轉型下的資安風險
- 5 | **企業營運資安治理策略**
- 6 | **企業營運資安治理解決方案**
- 7 | 資訊安全的最佳解決方案
- 8 | 結論



企業永續

是指企業在經濟、社會和環境三個層面上的可持續發展和負責任經營。這種經營方式強調在滿足當前需求的同時，也要保護未來世代的需求，並尊重社會和環境的平衡。

「賺取適當利潤，講求誠信，不以賺取最大利潤為目標」
永續 - 「用多少拿多少、取一個還一個」

永續常見3大名詞

CSR

Corporate Social
Responsibility

1999年
聯合國倡議提出
「全球盟約」

ESG

Environment,
Social and Governance

2006年
聯合國提出
「責任投資原則」

SDGs

Sustainable
Development Goals

2015年
聯合國宣布
「2030永續發展目標」

具體涵義

企業承諾持續遵守道德規範，為經濟發展做出貢獻，並且改善員工及其家庭、當地整體社區、社會的生活品質。

由3面向評估企業是否善盡社會責任：

- 環境 (Environmental)
- 社會參與 (Social)
- 公司治理 (Governance)

針對人類面臨的挑戰，提出17項內容和169項細則，作為2030年前世界各國努力推動永續發展的指導方針。

CSR、ESG、SDGs 說明

<https://www.leadercampus.com.tw/course/free/2561>

企業永續目標實踐 - CSR、ESG

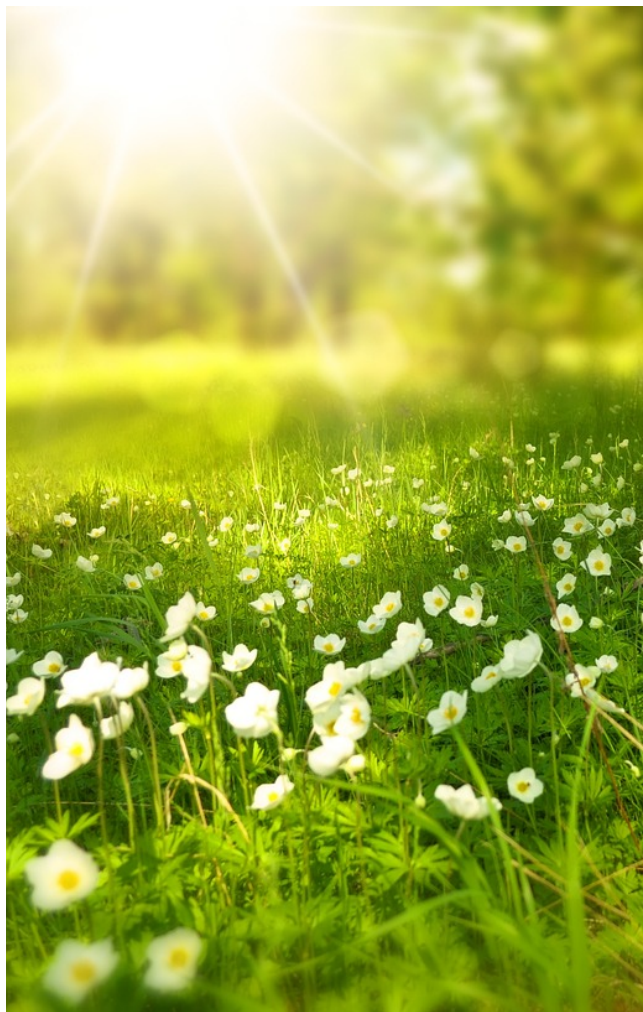
1 | CSR：企業對社會的責任擔當

指企業不能只著重追求金錢利益，更需要對小至供應鏈、股東、勞工雇員等利害人關係，大至環境、經濟等必須擔起一定的責任，促進社會提供正向成長的影響力，其核心所涵蓋的內容，是以「企業」為主體。

2 | ESG：永續發展的實質行動，企業社會責任的實踐

ESG可以說是企業實踐社會的責任的實質行動，原因是因為CSR是一個範圍也蠻廣的概念，而ESG將其更明確的理出能實現的行動，讓企業有方向去執行。

企業永續目標實踐 - 由內而外



永續是目標而韌性是過程，歸納「營運不中斷」以及「客戶信任」是企業永續以及企業韌性的交集。

G：韌性 - 營運不中斷、客戶要信任

S：多贏 - 企業與利害關係人建立良好關係

E：知足 - 企業與環境的和諧共存

企業永續目標實踐 - 韌性



顧客信任



產品優異



營運有效

成本決定價格？ 價格決定成本？

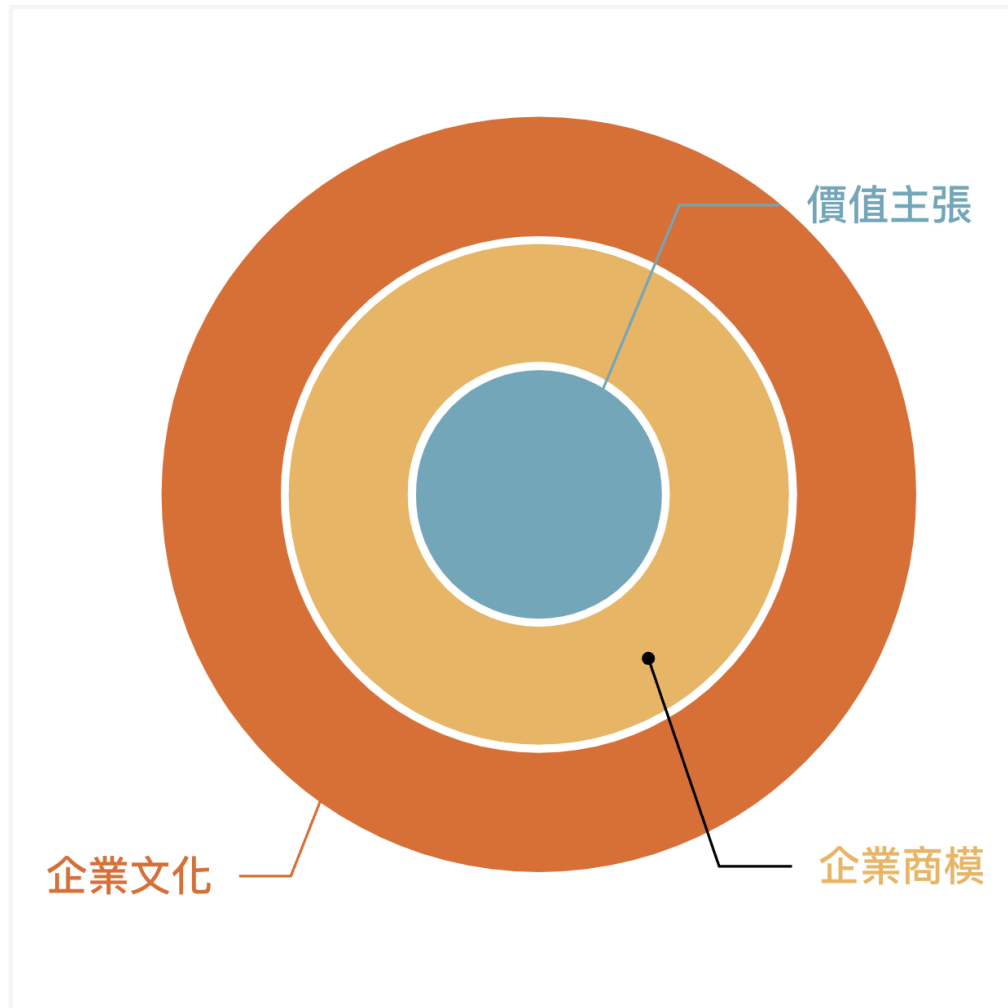


企業永續目標實踐 - 企業營運五要事



1. 顧客市場：價值與擴展策略
2. 產品服務：成本與品質策略
3. 人員組織：上手與順手策略
4. 現金流量：運籌與遠慮策略
5. 基礎建設：穩定與安全策略

企業永續目標實踐 - 企業永續唯一不變的是變



- 「轉型」是劇烈變革
- 企業轉型 - 企業價值主張
- 企業商模 - 企業服務流程
- 企業文化 - 企業品牌塑造

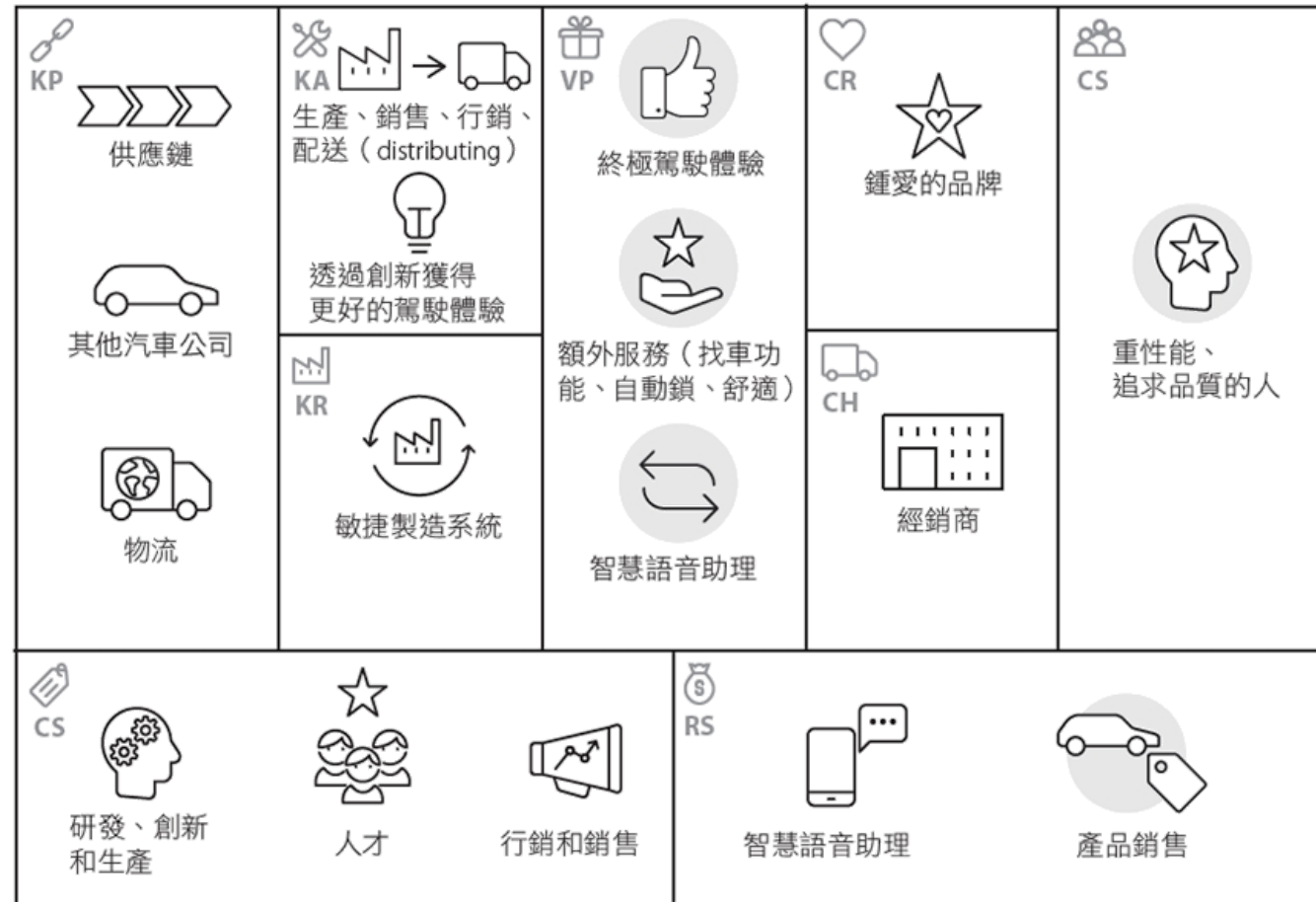
轉型從企業價值開始 - BMW的商業模式轉型

從產品製造到
全方位移動服務提供者



轉型從企業價值開始 – 移動服務，純粹駕駛樂趣

- 卓越設計技術
- 領先車子性能
- 優良客戶服務

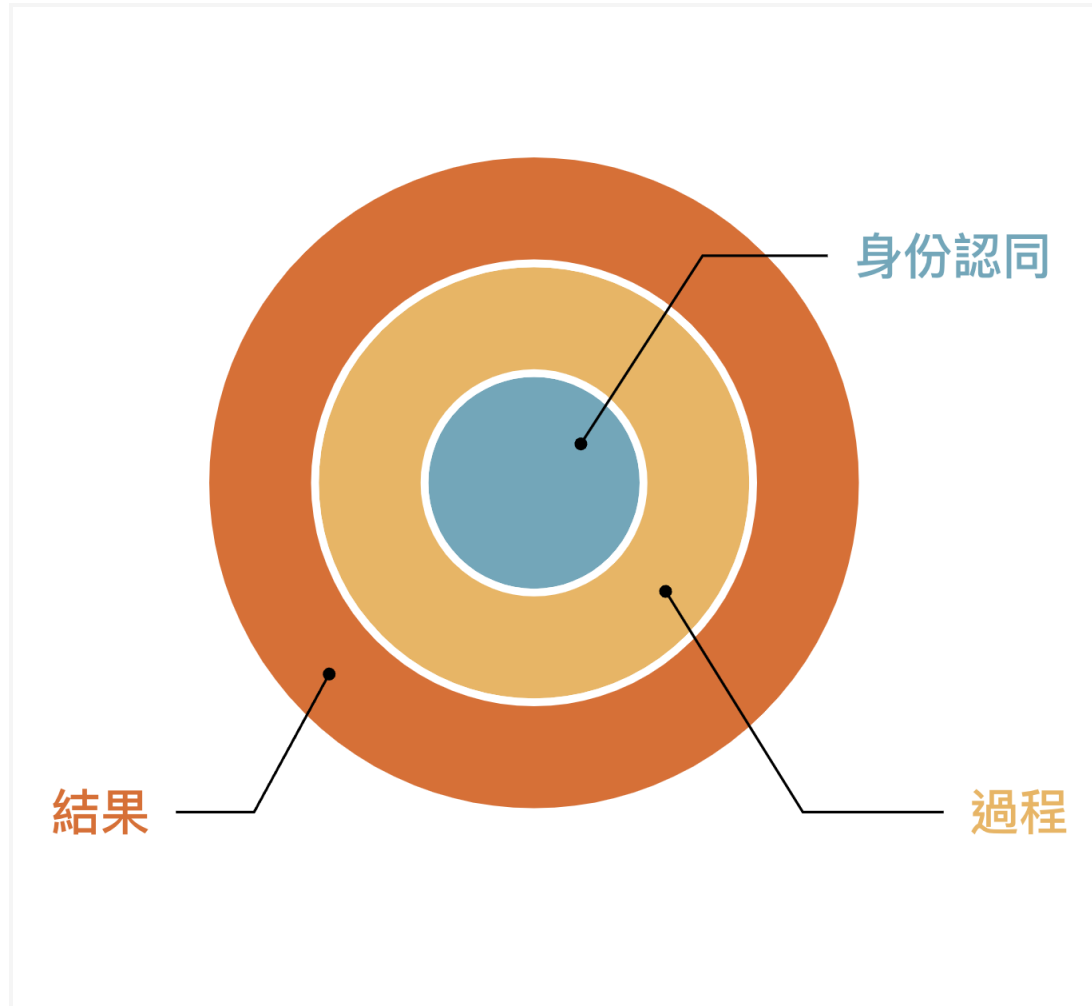


企業永續目標實踐 - 企業永續的挑戰



- 平衡短期與長期目標
- 完整規劃與適當的資源分配
- 全體員工的理解和實踐

企業永續目標實踐 - 企業永續 vs 成長思維



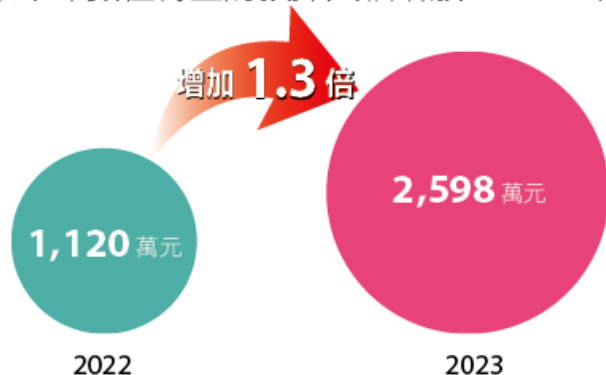
- 「**改變**」是改變慣性
- 身份認同 - 您相信什麼？
- 過程(**行爲**) - 您做了什麼？
- 結果(**習慣**) - 您得到什麼？

數位轉型是現在進行式

數位轉型是趨勢

高科技製造業近 2 年數位轉型投資變化

高科技製造業今年數位轉型的預算大幅增漲 131%，遠高於其他產業

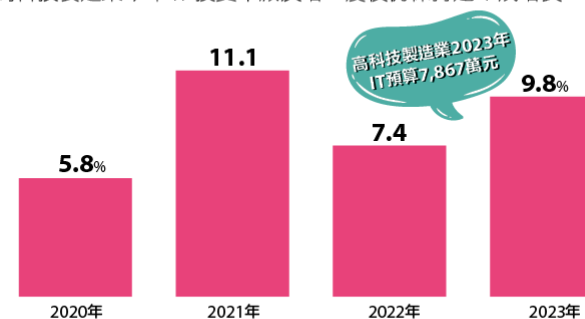


資料來源：2023 iThome CIO大調查，2023年7月

iThome

高科技製造產業歷年 IT 預算成長率

高科技製造業今年 IT 投資不減反增，疫後仍保持近 1 成增長

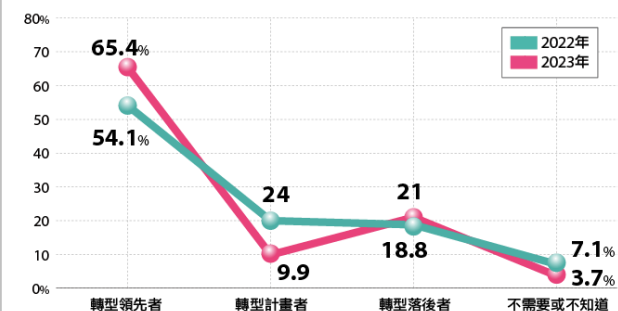


資料來源：2023 iThome CIO大調查，2023年7月

iThome

高科技製造業 2023 數位轉型成熟度分布

6 成企業已經成為轉型的領先者，但仍有 2 成在轉型方面落後



說明：百分比為企業自評屬於該階段的企業占比。轉型領先者指已經展開數位轉型的企業，落後者是指有需求但還沒採取行動者

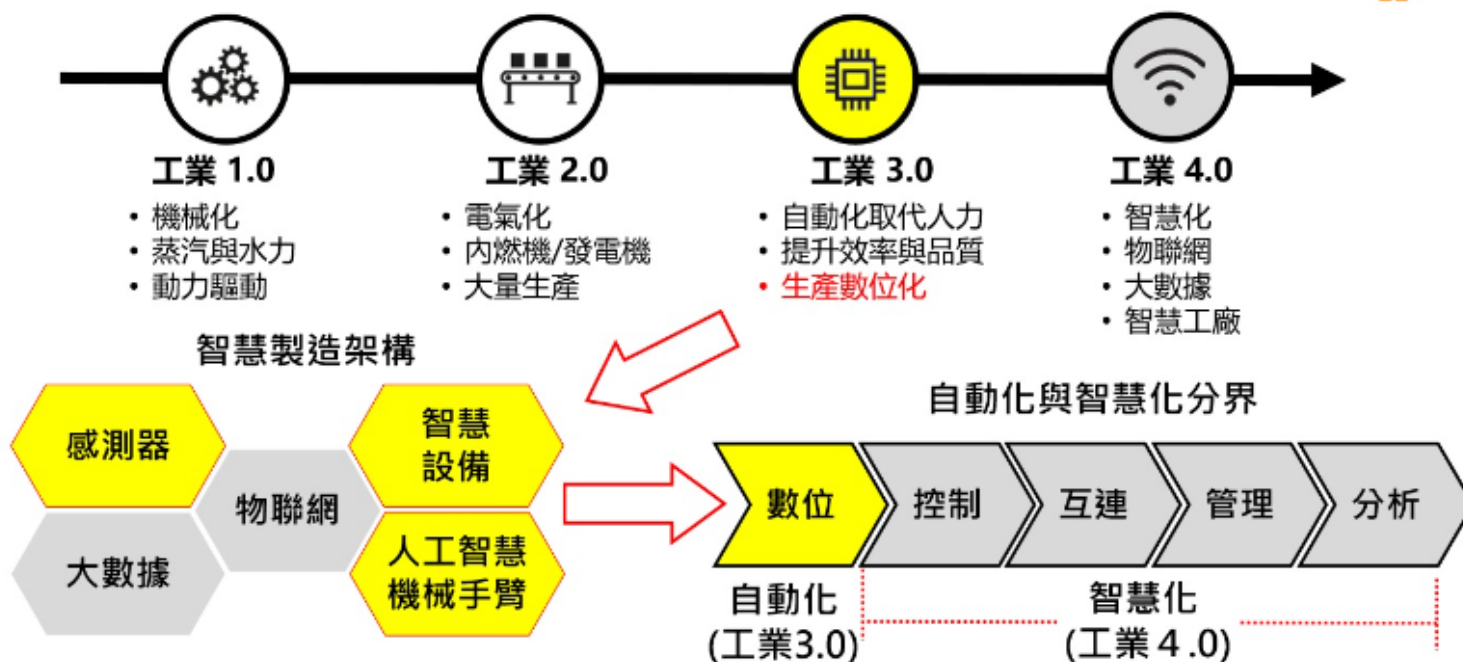
資料來源：2023 iThome CIO大調查，2023年7月

iThome

數位轉型是現在進行式

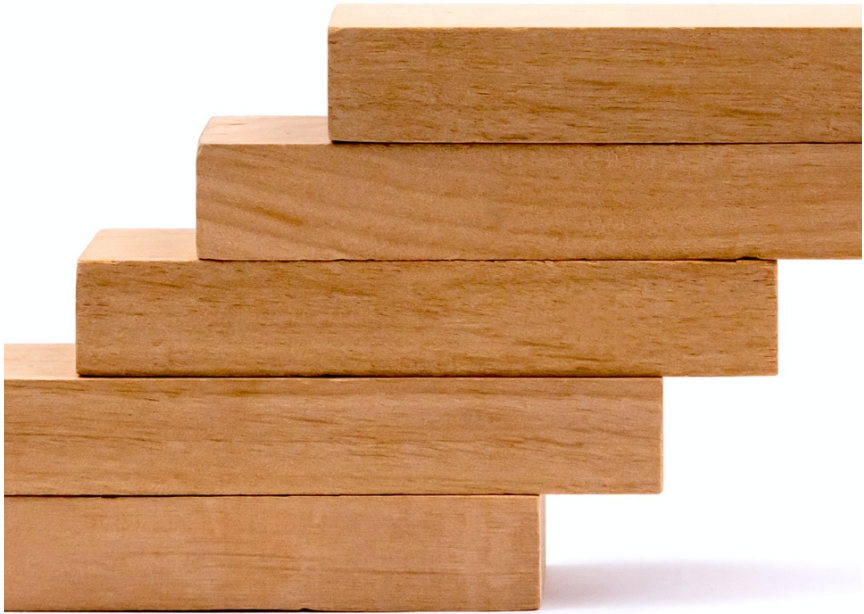
「智慧化」前需「數位化」、「數位化」前需要「標準化」

工業製造跨入智慧製造 必先完成生產數位化步驟



數位轉型是現在進行式

企業數位轉型三階段



1. **數位化 (Digitization)**
 - 運用數位工具
2. **數位優化 (Digital Optimization)**
 - 優化數位工具與流程
3. **數位轉型 (Digital Transformation)**
 - 使用數位資產進行商模再造

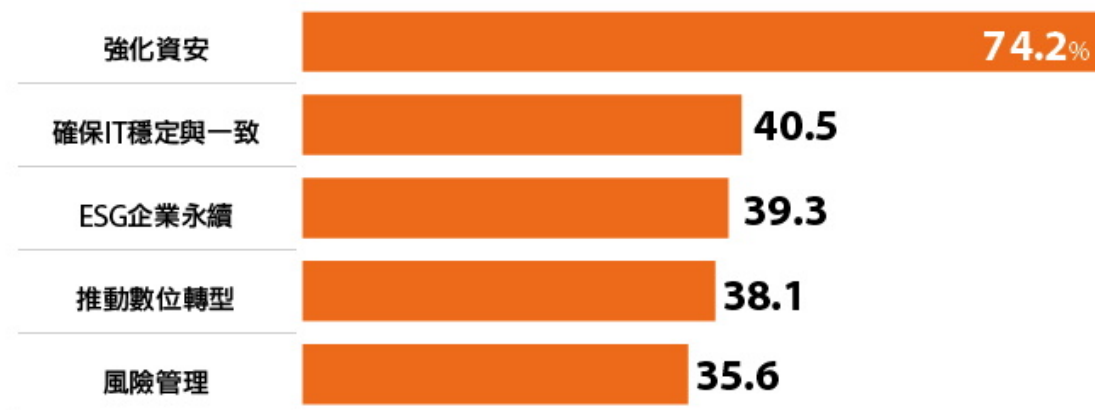
數位轉型是現在進行式

ESG企業永續、數位轉型是趨勢，而強化資安更是重中之重

企業CIO 資訊長
數位轉型後，資安避無可避

CIO 2023 年度優先目標 Top 5

ESG 企業永續目標排名大提升，甚至超過數位轉型目標



說明：百分比為年度目標納入該項的CIO比例 資料來源：2023 iThome CIO大調查，2023年6月

數位轉型下的企業資安風險

數位轉型重塑資安戰場



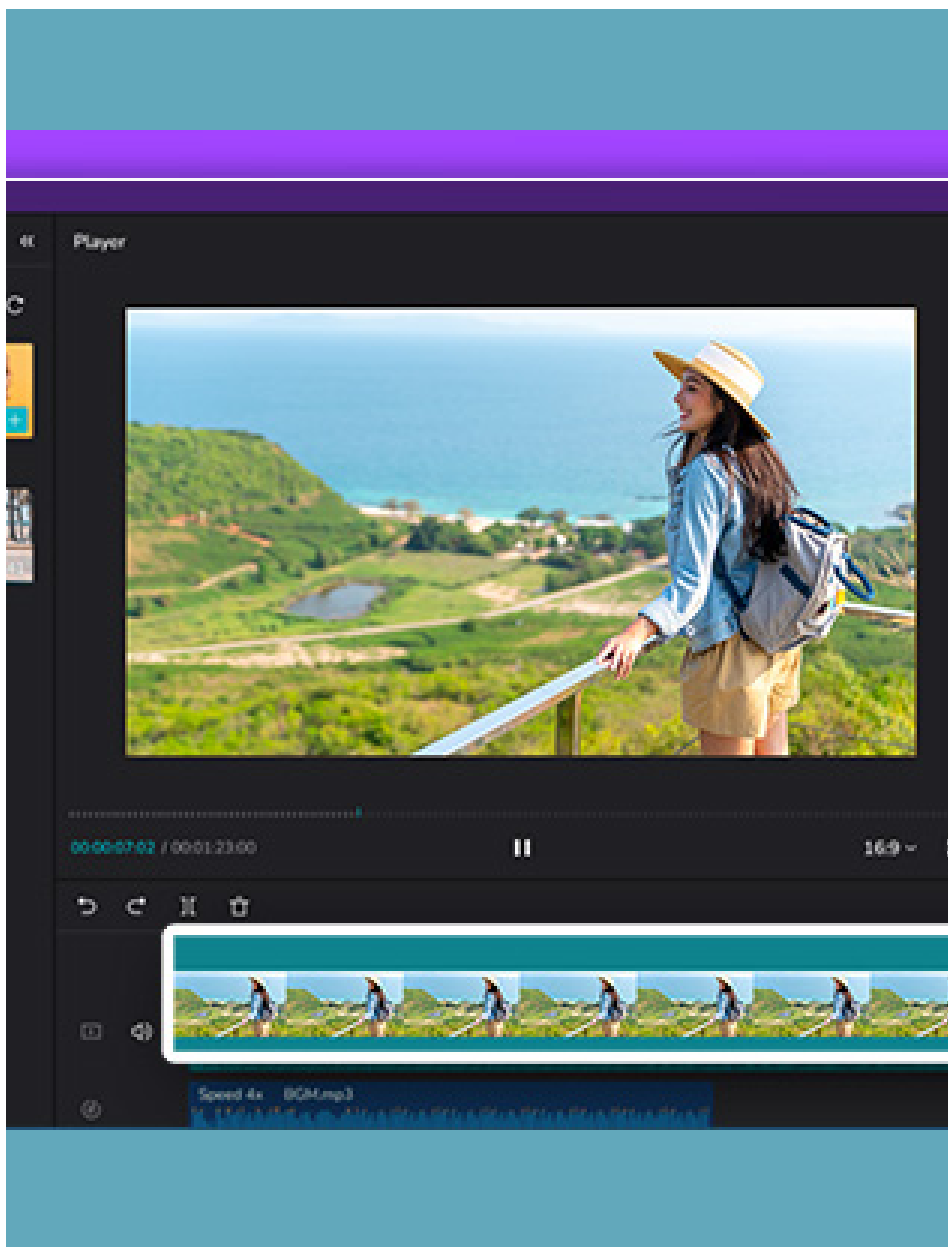
- 在全民都能感受到的**數位轉型**力道之下，產業生態翻轉，也**重塑了資安戰場**
- 數位轉型打造「**營運數位化、自動化環境**」，並創造「**數位化資產**」
- 「**道瓊永續發展指數（DJSI）**」及「**台灣企業永續獎**」等國內外永續獎項開始將資安管理納入評比項目

數位轉型下的企業資安風險

數位轉型後資安問題層出不窮



- **抖音影片剪輯軟體CapCut遭冒用**，駭客假借提供工具的名義散布竊密軟體
- **PyPI暫停新專案及使用者註冊**，原因是難以招架駭客大肆濫用的情況
- **共享單車服務YouBike**遭境外攻擊，2.1萬筆用戶資料恐外洩
- **台灣虎航**在2022年7月下旬，遭受駭客入侵，會員資料恐外洩



抖音影片剪輯軟體CapCut遭冒用

抖音影片剪輯軟體CapCut最近遭到冒用,許多惡意鏈接利用其名義發布。

使用者如果不小心點擊這些鏈接,可能會**下載包含木馬或勒索軟體的檔案**。

PyPI遭遇惡意套件攻擊,並採取因應措施

PyPI遭遇惡意套件攻擊

PyPI於2022/5/20宣布暫停新用戶與專案註冊,因**發現大量惡意使用者與專案**,加上管理員休假無法處理。

駭客利用PyPI植入惡意程式

駭客將惡意**Python套件**上傳PyPI,以**植入受害者電腦的木馬程式**竊取資訊。

PyPI採取因應措施

PyPI重新分組並暫停新註冊,計劃在年底前**強制維護者啟用雙重要素驗證(2FA)**,以提高安全性。

YouBike個資外洩事件,反思企業資安責任

YouBike遭遇網路攻擊,造成可能有**4萬會員**的個資外洩

外洩的個資包含**手機號碼、卡號、密碼**以及**交易資料**

當天YouBike已經暫停會員登入功能,並研擬補償機制



台灣虎航遭駭客攻擊,客戶資料恐外洩

- 台灣虎航遭駭客攻擊
2022年7月22日,台灣虎航宣布**遭受網路攻擊**
- 公司採取防禦措施
啟動防禦機制,聯繫資安專家和政府單位
- 官網發布反詐騙聲明
發布聲明**共同防制網路詐騙**,並強化資安

台灣虎航遭駭客攻擊,公司採取各項應對措施,並發布反詐騙聲明提醒旅客注意資安。

數位轉型下的企業資安風險

資安是保護企業競爭力的重要因素



資安是保護企業競爭力的重要因素

1. 確保營運不中斷
2. 維持客戶信任

企業營運資安治理策略

企業營運管理資安重點項目



網路安全

部署防火牆、入侵偵測系統,並定期進行漏洞掃描。



端點安全

在所有終端設備安裝防毒軟體,並启用加密及權限管制。



帳號安全

建立密碼複雜度規則,定期變更管理帳號密碼。



資料安全管理

建立資料分級制度,依敏感程度提供不同層級的保護。

企業必須建立完善的資安管理制度,從資料、網路、端點及帳號等面向,採取適當的防護措施,降低資安風險。

企業營運資安治理策略

企業資安文化、企業營運管理資安重點項目



- **企業資安文化**

- 資訊安全，不單單只是資訊部門的責任。
- 公司員工整體資安意識仍是首要關鍵。

- **企業營運管理資安重點項目**

- 在全球數位轉型趨勢下，企業應對「IT資訊安全（Information Technology）」、「OT營運自動化安全（Operational Technology）」以及「個資保護之資安防護」進行整體性規劃。

企業營運資安治理策略

企業營運管理資安重點項目



1. IT領域 - IT資訊安全

- 在IT環境中企業主要仰賴邊界的防火牆抵抗外部的攻擊，進而保障核心的ERP、WEB主機系統。**在IT環境中，思考角度主要是以人為對象**，不管在有線或無線的環境，都希望對人的行為進行妥善的管制。

2. OT領域 - OT營運自動化安全

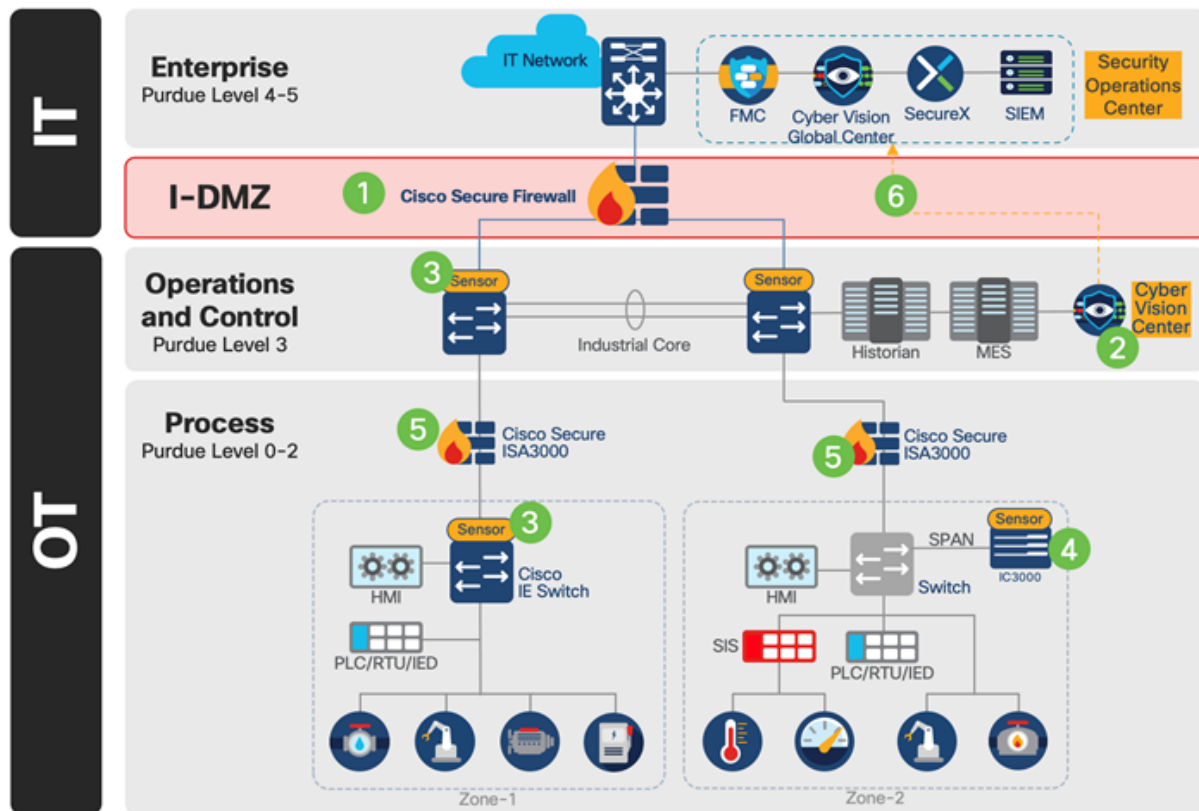
- OT的環境卻與IT關注的不同，**多數OT環境管的是機器**，負責控制生產製造，它最重要的任務就是能保持產線穩定運作。當不安全且含有漏洞的企業網路一旦與工控系統專屬的網路相結時，這會讓工控系統曝露在網路攻擊威脅之中。

3. 個資保護之資安防護 - 法規遵守

- 確保了**解並遵守當地和行業相關的隱私法規**，如歐盟的通用資料保護法（GDPR）、美國的加州消費者隱私法（CCPA）等。了解這些法規有助於建立合法、透明且負責任的資料處理流程。

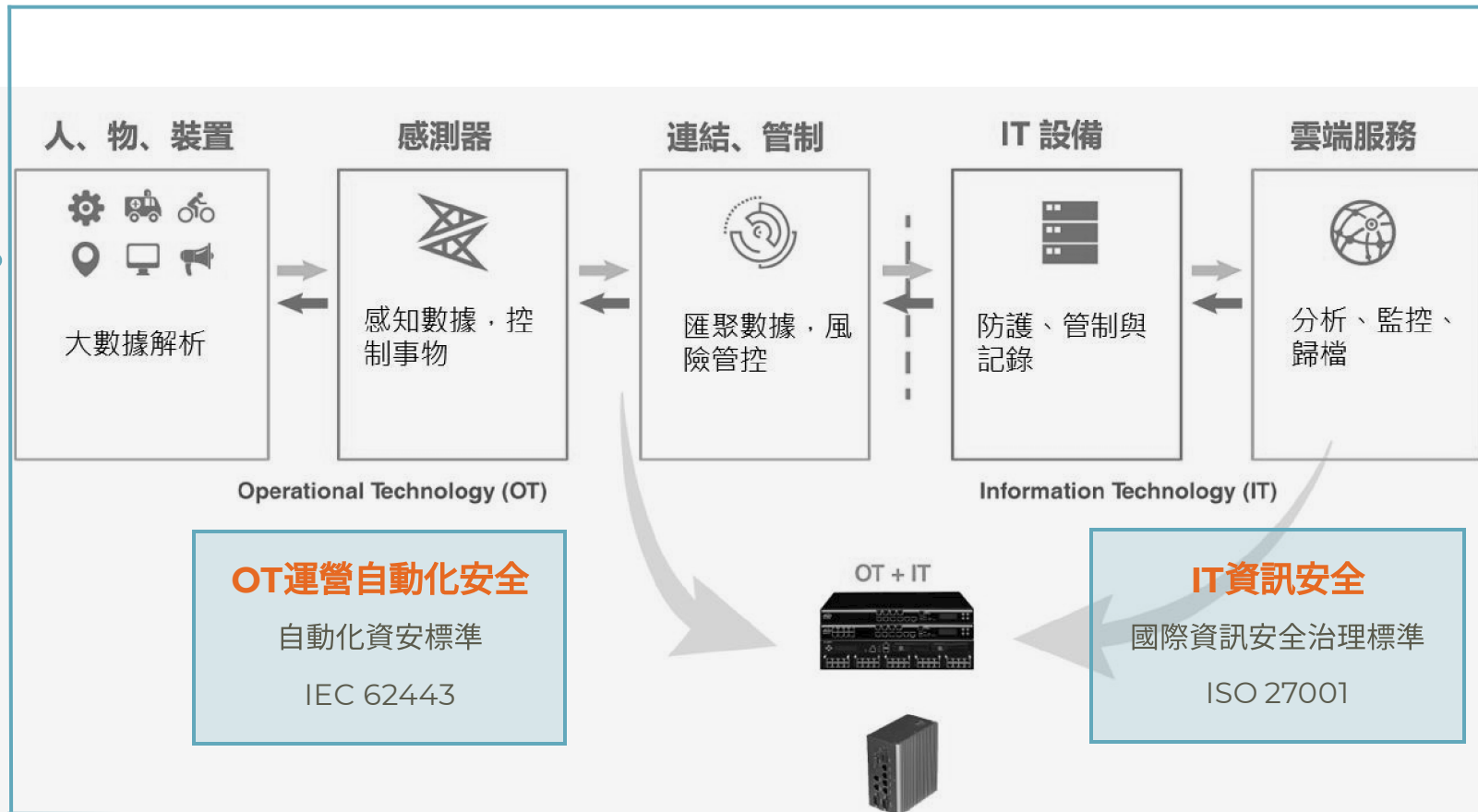
企業營運資安治理策略

以Cisco網路資安架構為例



企業營運資安治理策略

企業營運管理資安標準規範



隱私權保護
之資安防護

個資資安

ISO 27701

隱私權保護
之資安防護

個資資安

ISO 27701

企業營運資安治理解決方案

ICTD 2.0 工業控制資安威脅偵測系統 (1/3)

ABCD Cookbook

Active scanner

OT弱點資訊主動式探測 + 監控設施威脅資料庫風險比對

Behavior mesh monitor

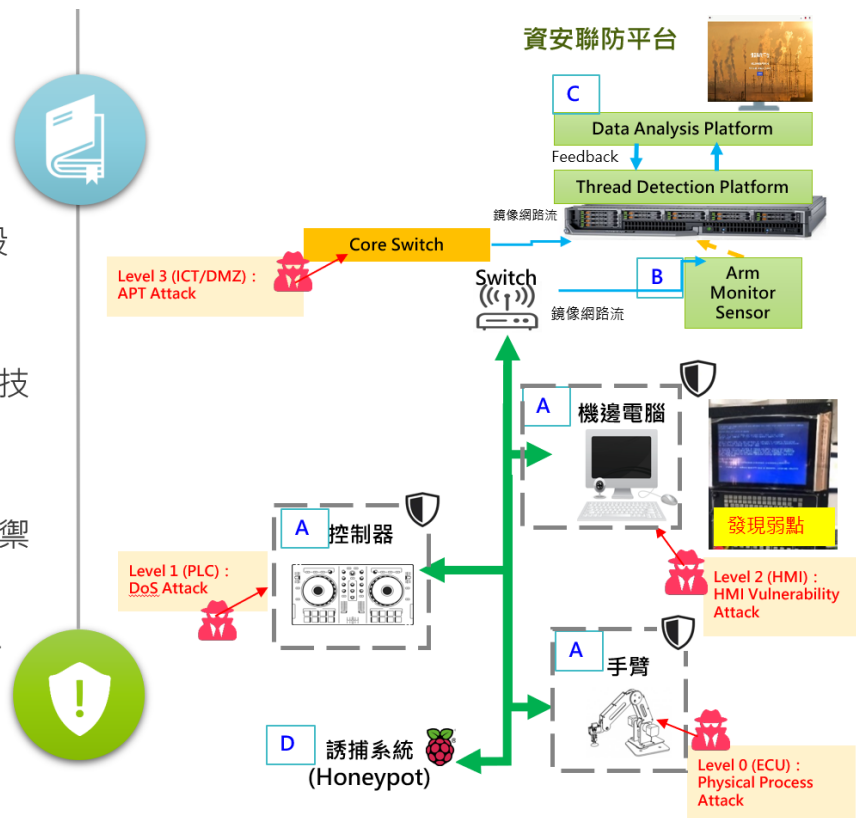
流量活動分群 + 狀態行為離群值技術 + 標準化監控

Correlation in defense

垂直串聯異質網路 + 橫向協同防禦

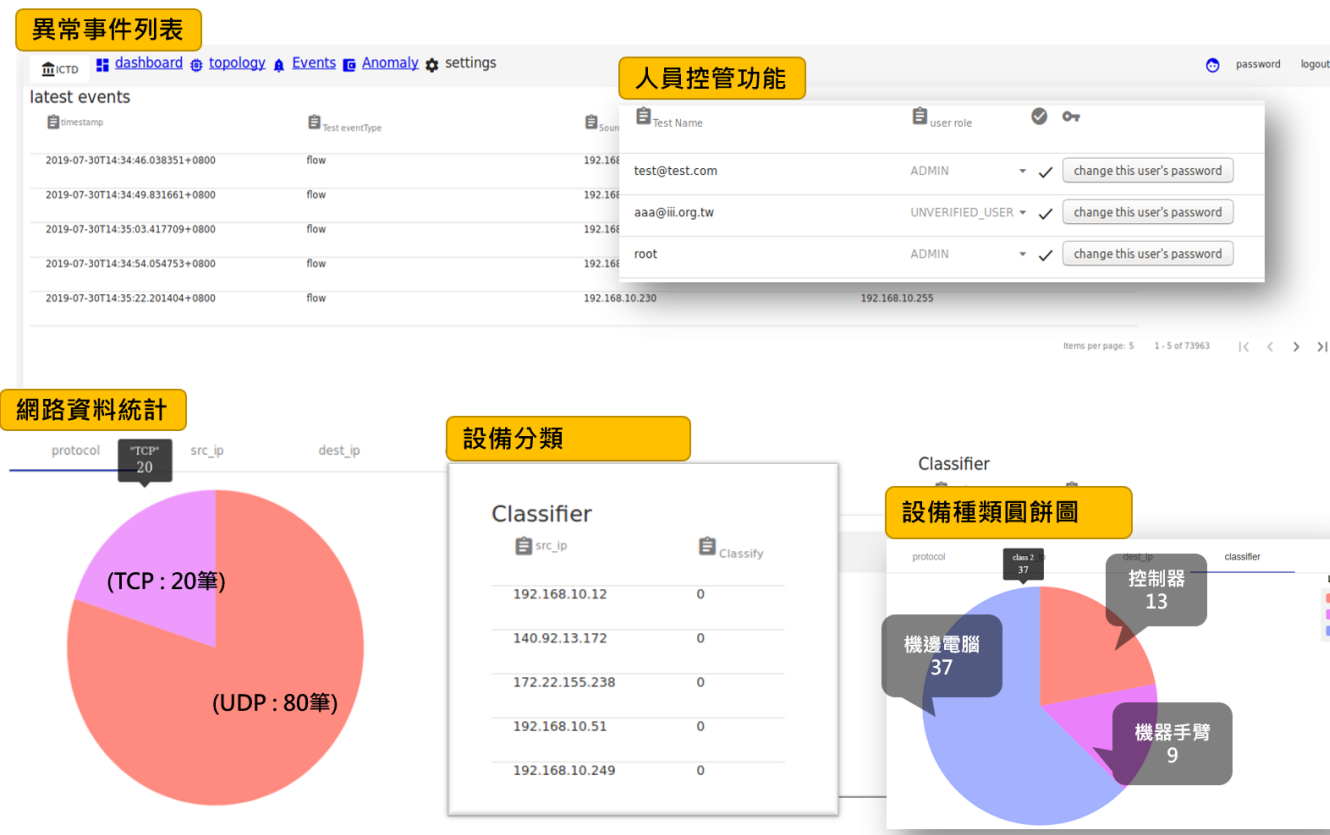
Dynamic honeypot

機器手臂pot + 無人搬運車pot + 製造程式pot



企業營運資安治理解決方案

ICTD 2.0 工業控制資安威脅偵測系統 - 數據匯集 (2/3)



ICTD 2.0 工業控制資安威脅偵測系統 - 數據分析 (3/3)



資訊安全的最佳解決方案

員工資安意識仍是首要關鍵

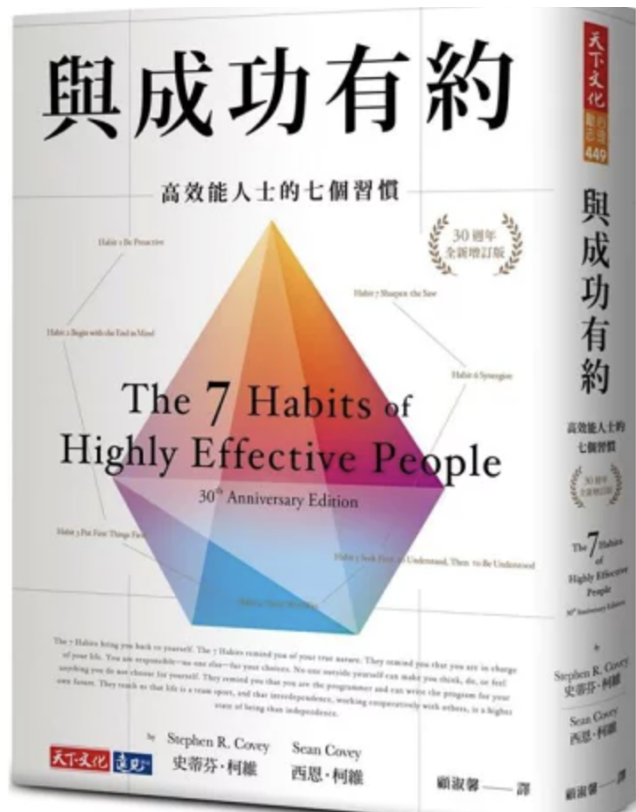


台積電中毒全臺產線大當機，營收
損失高達**52億元天價**

- 台積電向來是**資安模範生**，層層管制、嚴格把關的**種種資安措施**更為人津津樂道，甚至視為業界最高標準之一。
- 全球科技大廠執行長來臺參觀台積電廠房時，都得在**門口櫃臺繳出手機，筆電貼上封條**，任何一支**USB**都不能入廠，沒有例外。

結論

企業的成功與「人」脫不了關係



對的自己

對的團隊

對的客戶

覺察：由外而內，綜觀全局、改變：由內而外，從心開始

THANK YOU