經濟部
產業發展署
Industrial Development Administration, MOEA

114年度
智慧機械-產業聚落供應鏈數位串流暨AI應用
資安盤點工作坊

簡報單位：財團法人中國生產力中心
簡報日期：114年3月6日
林詠章 特聘教授 (iclin@nchu.edu.tw)
國立中興大學資訊管理系

簡報大綱

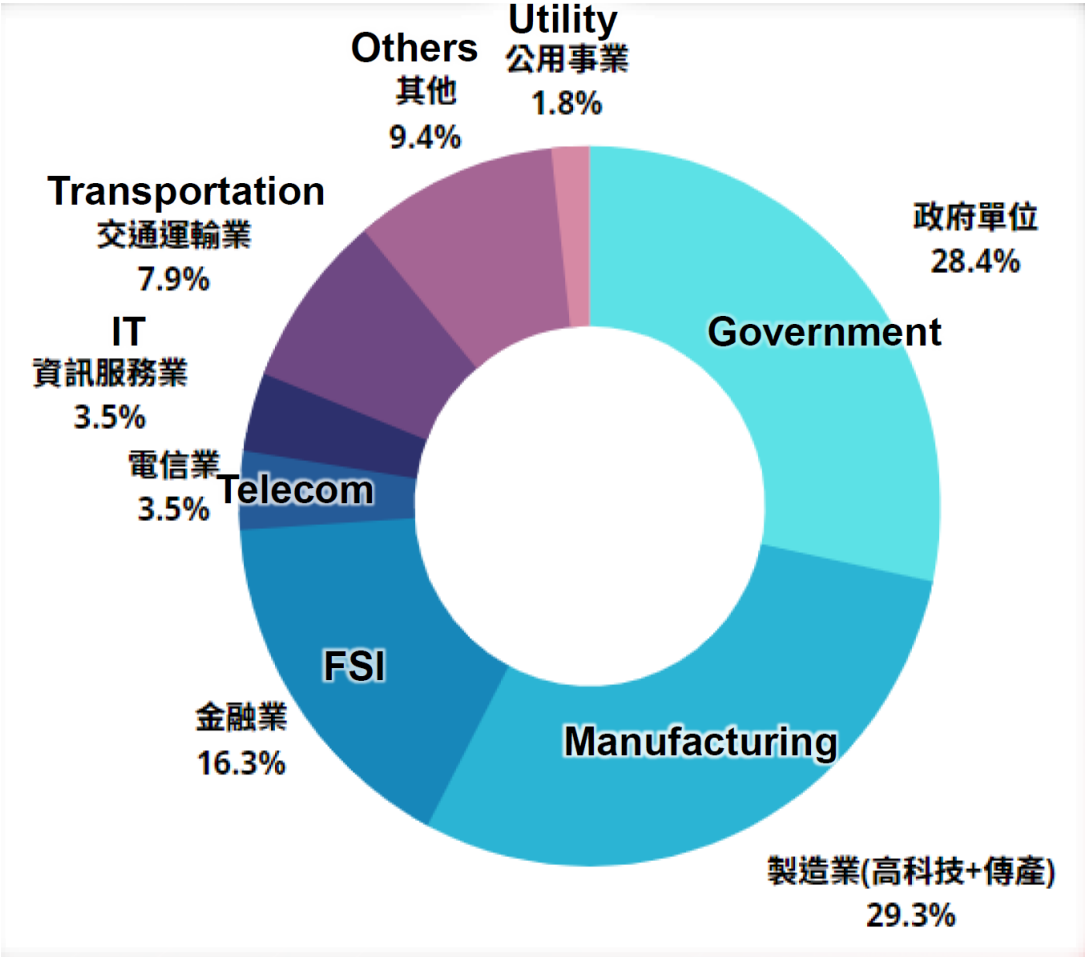
壹、資安自評與查核流程

貳、執行階段資安要求

附件一、過去獲補助廠商常見問題彙總

經濟部
產業發展署
Industrial Development Administration, MOEA

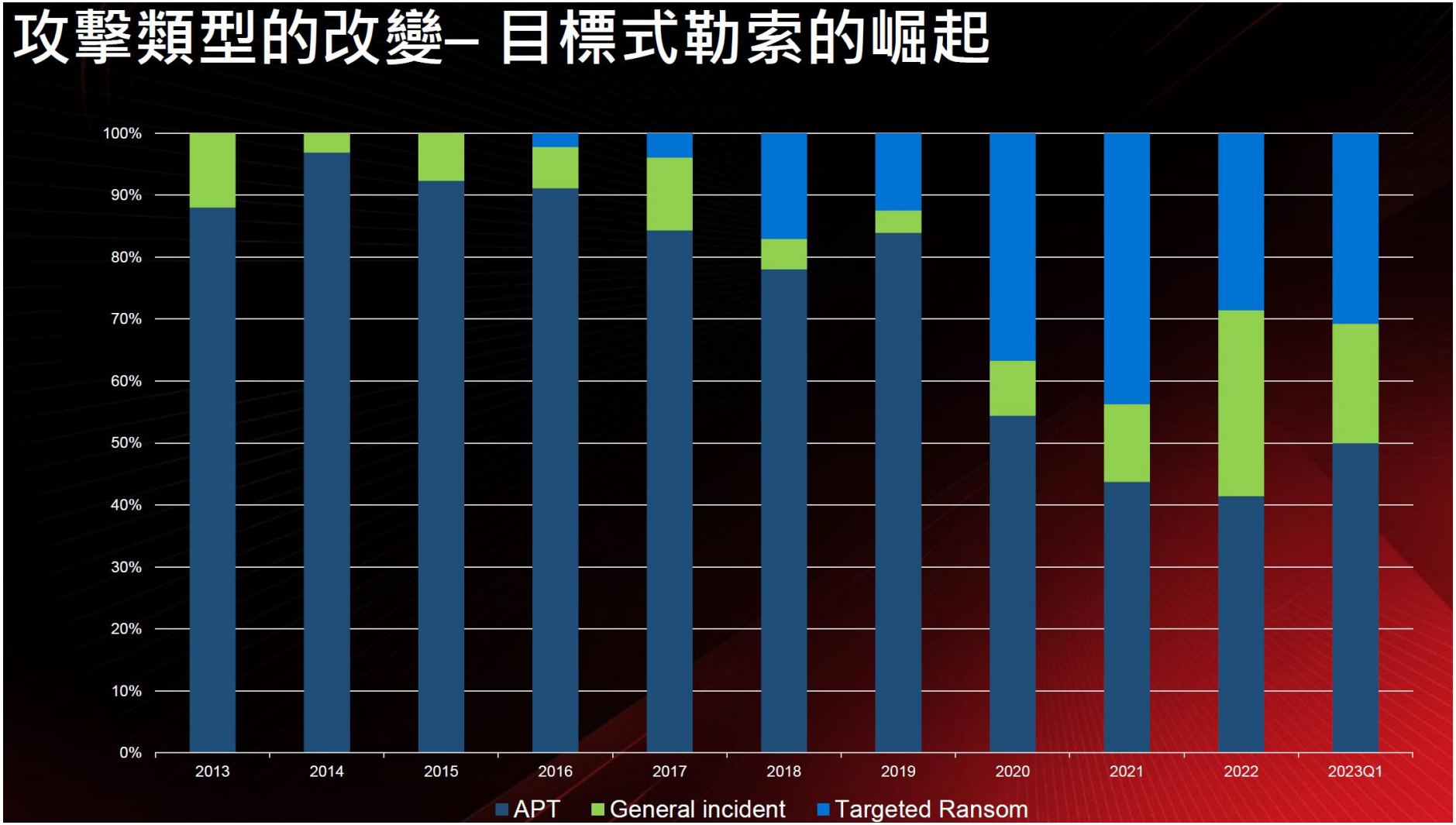
台灣本地整體資安事故統計



製造業災情最慘烈!

資料來源:趨勢科技

攻擊類型的改變– 目標式勒索的崛起



資料來源:趨勢科技

勒索病毒的衝擊

- 產能停頓: 平均6天的回復期，3天的產能損失
- 竊取機密資料: 資料拍賣→資料公開
- 加密資料，高額贖金

OT安全成為製造業營運的一大挑戰

- 太依賴實體隔離的封閉網路
  - 威脅無所不在
  - Email, USB, 設備 , AI, 系統, 供應商, 客戶...

- 資安可能產生的危害超出一般人的想像
  - 企業責任損失已不只是單一產線停工的營運損失，包含客戶不信任、賠償、訴訟、保險、監管罰款，以及人為失誤所產生的責任損失。
  - Gartner 預測企業在 2023 年因為 CPS(Cyber-Physical Systems) 遭受攻擊造成的財務損失將超過500億美元。

壹、資安自評與查核流程

一、資訊安全要求

審查原則

	盤點資安現況	構想及篩選解決方案	發展細部行動
規劃案	**提案廠商**須**盤點**與**供應鏈**間之**資**訊**安**全之**現況**，包含網路、應用及設備層的軟硬體。	**提案廠商**須進行問題分析與提出最佳調整方案之建議，需含**教育訓練**、**機制建立**、**系統導入**、導入後**查驗**、**資安架構圖**等規劃。	**提案廠商**須提出資安防護規劃構想 計畫書需敘明 (1)資訊安全組織 (2)資訊安全計畫

1. **資訊安全組織**：指派公司之**專責人員**負責資訊安全**計畫**、**執行**、**查核**及**改善**，並由管理階層指派**高階**人員負責**協調**專案資源。
2. **資訊安全計畫**：規劃資訊安全**風險評估**，可透過但不限於第三方單位執行**原始碼檢測**、**黑箱檢測**、**滲透測試**等，並針對重大威脅及脆弱性必須規劃**資安防護解決方案**。

經濟部
產業發展署
Industrial Development Administration, MOEA

資訊安全之推動規劃

1. 盤查: 說明提案廠商與供應鏈間之資訊安全之現況，包含網路、應用及設備層的軟硬體。

2. 資訊安全組織：依公司組織文化，指派公司之專責人員負責資訊安全計畫、執行、查核及改善，並由管理階層指派高階人員負責協調專案資源，成員最好跨部門。

3. 資訊安全計畫：透過資訊安全風險評估，找出主要資安威脅，導入資安防護措施。

破口在哪裡?

將有限的資源，優先運用在需要加強的部分

貳、執行階段資安要求

一、資安管理依據：

參考108年行政院國家資通安全會報技術服務中心整理之**政府機關資安治理評估機制**，依據製造業現況擬訂資訊安全，**計畫驗收至少須達必要要求之條件**：

依序	項目	說明
1	人員認知及訓練	經費編列可用於公司內部資安人力，及委外顧問，公司內部資訊人力需取得資通安全通識教育訓練，並定期召開會議。
2	存取控制管理	應具體說明網路安全管理、存取管理、家密管理等機制。
3	通訊與作業安全	應具體說明資安監控、資安防護、惡意軟體防護、遠距管理、電子郵件、安全性檢測，及資料備份等方式。
4	日誌記錄保存	應具體說明資安事件如何應對及日誌管理機制
5	資安系統開發與安全維護	說明如何落實安全系統發展生命周期。

經濟部
產業發展署
Industrial Development Administration, MOEA

企業網路層的資訊安全要求

1. 各層之間與各層對外網路應使用資安防護設備，如: IPS、VPN、URL Filter及APT偵測等。

2. 針對USB裝置進行管理與惡意程式掃描。

3. 具備日誌與稽核機制，須具備事件記錄功能，且須存查至少N+0.5年。

4. 各網路、系統、設備於上線前，須經弱點掃描確認，不可存在高風險等級之安全弱點。

5. 行動應用App須符合「行動應用App基本資安規範」之安全要求，並經合格實驗室測試通過。

6. 影像監控系統須符合「影像監控系統資安標準」之安全要求，並經合格實驗室測試通過。

經濟部
產業發展署
Industrial Development Administration, MOEA

監控與管理層資訊安全要求

1. 各個主機安裝資訊安全防護軟體

2. 採用白名單管控方式 (1) 建立作業系統控管執行程式白名單 (2) 建立連線控管白名單

3. 建立安全的軟/韌體與組態更新機制

手動更新

- 更新檔須加密保護以確保機密，且須採用FIPS 140-2 Annex A所核可之加密演算法。

線上更新:

- 須驗證下載來源，且其更新路徑須通過安全通道，且安全通道須使用SSL/TLS。
- 更新前必須驗證軟/韌體之正確性及完整性的功能。
- 更新失敗時，系統能回復正常運作。

備份機制要求

1. 有效備份，3-2-1原則。

2. 程式碼與設定檔須定期備份。

- 開發過程應遵循安全開發流程(SSDLC)。
- 根據資安政策制定備份流程與週期。

3. 資料分級後，重要資料定期備份。

- 依據資料用途進行風險評估，並設定風險等級。
- 風險等級高之重要資料，應依據資安政策定期進行備份

密碼管理

1. 更改初始密碼
2. 要求密碼強度
3. 密碼失效鎖定機制
4. 密碼加密保存
5. 密碼定期更改

該如何選擇優先導入的安全防禦機制?

降低風險的處理策略

- 控制: 減少自身弱點，ex. 進行弱點掃描
- 避免: 避免外在威脅，ex. 防火牆、IDS、IPS
- 轉移: 轉移資產價值，ex. 備分、備援、資安保險
- 接受: 接受風險

附件一、過去獲補助廠商常見問題彙總

一、提案技術審查：

1.資安著重於對外架構，未規劃**內部資安威脅**的**分析作法**及內部**系統串接規劃**。
2.未規劃如何進行**資料權限**的**控管**。

二、階段技術查證：

1.僅作社交工程演練，未進一步辦理**員工資安意識教育訓練**。
2.僅作**弱**點**掃**描初測，未規劃**防禦措施及後續複測**。
3.IT及OT部分未作資安監控、或**防護較弱**。
4.內部未有**資訊安全組織規劃**。
5.未明確計畫內導入**AI模型**的資料匯流方式及**安全性**。

簡報結束
敬請指教