臺灣資安大會
CYBERSEC 2019

IT及OT環境的資安挑戰與因應之道

中華資安國際股份有限公司
游峯鵬 副總經理

2019年3月20日

PRESENTED BY iThome

Outline

一.OT與IT的融合
二.工控(ICS)資安檢測實務
三.OT資安的資安挑戰及因應之道
四.結語

IT x OT

有處理資訊需求之產業

關鍵基礎設施、製造、機械、醫療.....

產 業

IT(Information Technology)

主要用於管理和處理資訊所採用的技術總稱，可包含軟體、硬體及應用等三個層次

OT(Operation Technology)

泛指可對實體設備進行監測、控制及操作的軟體及硬體

應用

應用場景

產業環境轉變

→ OT 與 IT 融合

產業環境轉變 – OT與IT融合

能源

民生資源

醫療

ERP系統

行政PC

叫號系統

IT

機械設備

投藥設備

控制設備

超音波儀

CT攝影儀器

核磁共振儀器

OT

Purdue Architecture (PERA)

SOC

ERP Server

Lv 5

Site Server

Lv 4

Patch Server

Remote Access Server

Lv 3

Historian

EWS

HMI

Alert System

Lv 2

PLC

DCS

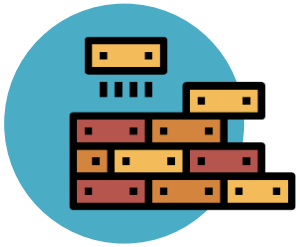
Lv 1

I/O I/O I/O I/O

Lv 0

中華資安國際

OT資安的重要性



在同時擁有IT及OT網路的環境中，若只專注在IT安全而忽略OT的話，很容易讓攻擊者由OT網路進入整個企業環境

OT不是為了資安而設計

- 注重穩定性及可用性
- 設備及協定存在資安風險
- 汰換週期長
- 更新修補程式不易(或無法)

卻面臨資安相關威脅

- 需適應資安議題的快速步調
- 惡意程式可潛伏長達10年以上
- 老舊的惡意程式仍可造成威脅

(如：MS 17-010、MS 08-067)

產生之危害影響甚鉅

- 人身安全(如：爆炸、能源外洩)
- 資訊洩漏(如：個資、商業機密)
- 國家安全

OT資安脆弱點

IT與OT已同時存在並互相融合，已成為OT環境的資安挑戰

來自人員的安全威脅:

- 不安全的供應鏈人員/軟硬體
- 未落實SOP之內部人員

開始於ICS環境中使用IT系統：

- 使用基於Windows/ Unix的系統 (ERP、LIMS)
- 資安意識及實作速度未能跟上
- 面對與IT相等的威脅性

過時的IT威脅仍可對ICS系統造成重大威脅：

- 未(無法)更新修補程式

不安全的網路架構及規則審查:

- 尚未(無)導入資安相關制度
- 邊界防禦、隔離管制尚未完善

缺少同時熟悉IT及OT之專家:

- IT及OT人員互不了解各自領域(CIA ⟶ AIC)

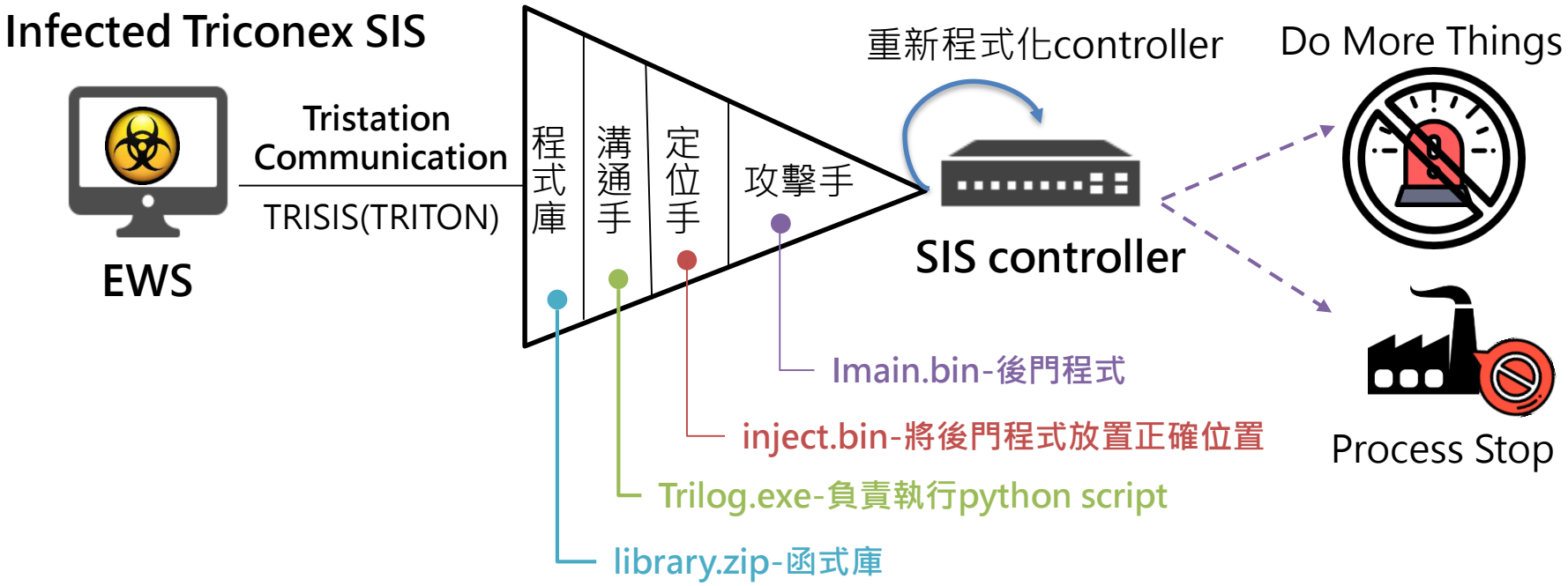
工控系統(ICS)遭攻擊實例

2018	台灣科技廠 – WANNACRY Variant 新加坡醫療集團 -SingHealth遭駭客入侵
2017	日本車廠 – WANNACRY 中東能源廠- TRITON
2015	烏克蘭電廠 – BLACKENERGY3
2014	美國電廠 – HAVEX
2010	伊朗核電廠 – STUNEX
2009	美國醫療中心遭駭客入侵

ICS遭攻擊實例 - 工業安全系統

工業安全系統
(Safety instrumented System, SIS)

在緊急情況或其他異常條件發生時，將程序(Process)恢復至正常狀態



ICS遭攻擊實例 - 醫療系統

新聞

新加坡SingHealth醫療系統遭駭客入侵，150萬人個資外洩

新加坡衛生部（Ministry Of Health Singapore）對外公告，醫療系統的資料庫遭遇駭客入侵攻擊，150萬人個資恐外洩。他們同時強調這起網路攻擊事件，是針對總理李顯龍而來。

文/ 羅正漢 | 2018-07-21 發表

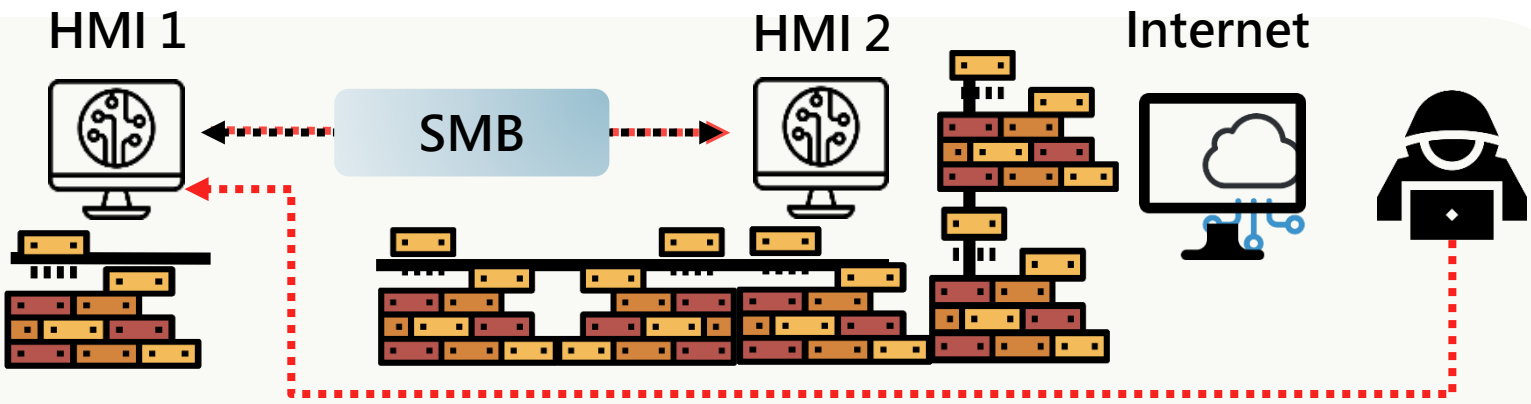
讚5.3萬 按讚加入iThome粉絲團 讚413 分享

二、工控(ICS)資安檢測實務

ICS資安檢測實務一

ICS環境發現不安全的通訊協定、對外部Internet網路連線

=> 隔離失效，設備或整個系統遭受惡意程式攻擊的機率大幅升高



駭客可從外部網路潛入

入侵後可造成內部大範圍感染

導致設備遭控制、遭勒索軟體影響……

圖片來源：https://support.flaticon.com/hc/en-us

醫療業之資安相關風險

根據美國緊急醫療研究機構(ECRI)發布的2019年十大醫療技術危害清單，【駭客可遠端存取系統，以破壞醫療照護服務】列於首位

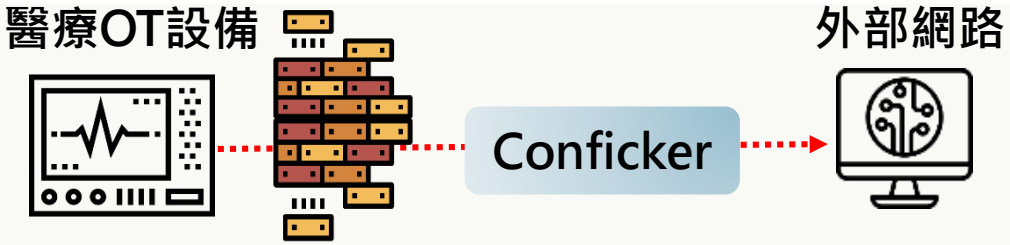
The List for 2019

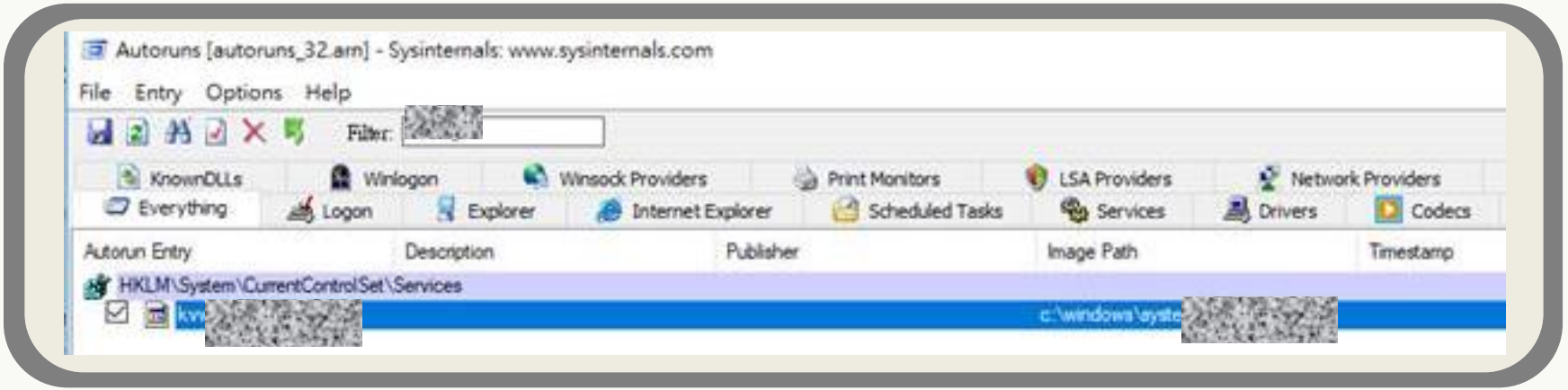
1. Hackers Can Exploit Remote Access to Systems, Disrupting Healthcare Operations
2. "Clean" Mattresses Can Ooze Body Fluids onto Patients
3. Retained Sponges Persist as a Surgical Complication Despite Manual Counts
4. Improperly Set Ventilator Alarms Put Patients at Risk for Hypoxic Brain Injury or Death
5. Mishandling Flexible Endoscopes after Disinfection Can Lead to Patient Infections
6. Confusing Dose Rate with Flow Rate Can Lead to Infusion Pump Medication Errors
7. Improper Customization of Physiologic Monitor Alarm Settings May Result in Missed Alarms
8. Injury Risk from Overhead Patient Lift Systems
9. Cleaning Fluid Seeping into Electrical Components Can Lead to Equipment Damage and Fires
10. Flawed Battery Charging Systems and Practices Can Affect Device Operation

參考資料：美國緊急醫療研究機構(Emergency Care Research Institute，ECRI)【2019 TOP 10 Health Technology Hazards】

ICS資安檢測實務二

發現**重要醫療設備**存在**古老的惡意程式**，因沒有適當的弱點管理或資安檢測機制，導致危害存在長達**超過10年**

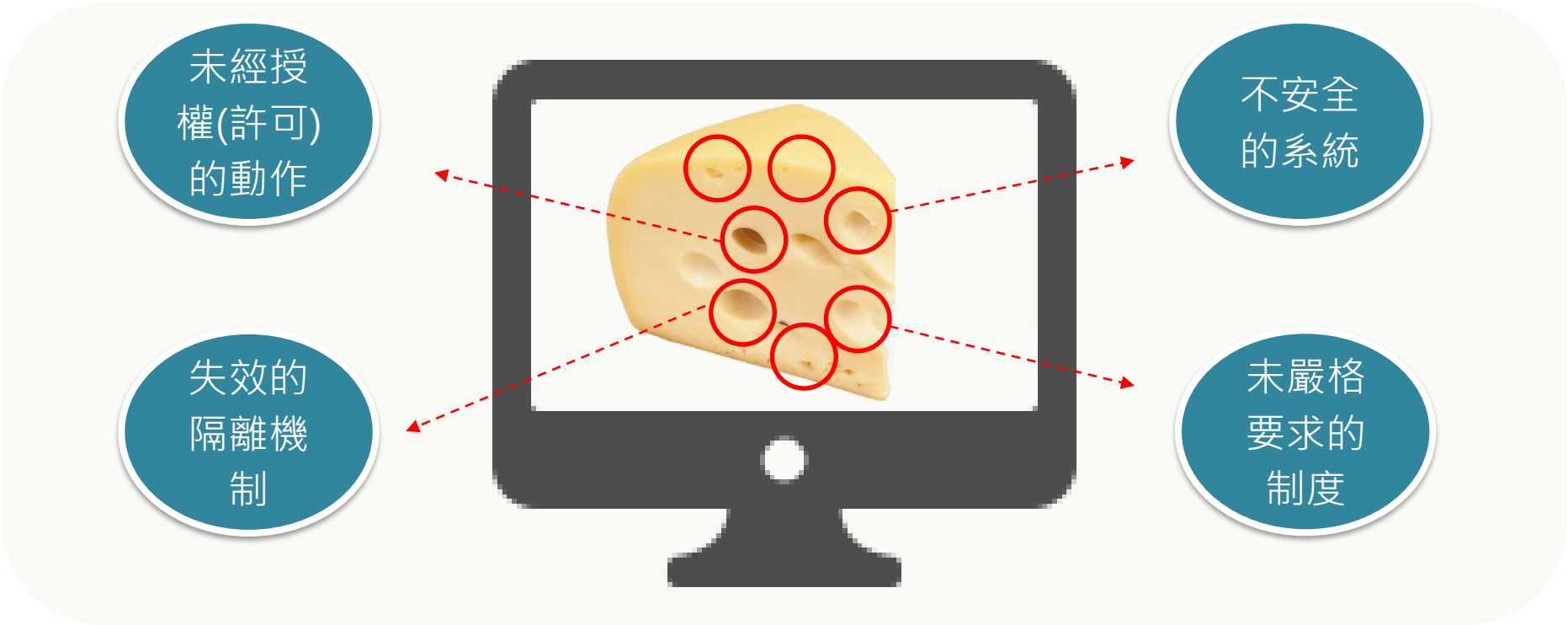




▲ 在開機啟動項中發現Conficker惡意程式建立的服務

圖片來源：https://support.flaticon.com/hc/en-us

損害通常來自多個弱點的疊加



敏感資訊外洩

影響國家安全

影響人身安全

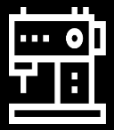
圖片取自網路

三、OT的資安挑戰及因應之道

OT資安挑戰

資產

- 系統老舊(**EOS**)
- 無法抵禦已知威脅(**未/無法安裝修補程式**)
- 難以掌握現有**資產狀態**，無法採取縱深防禦



感知

- 無法確認**隔離機制**有效性
- 無**弱點**識別與管理機制
- 無資安**監控**與**健診**機制

制度

- 未導入資安相關制度
- 未建立/落實**資安管控**、**權限分級**等機制

人員

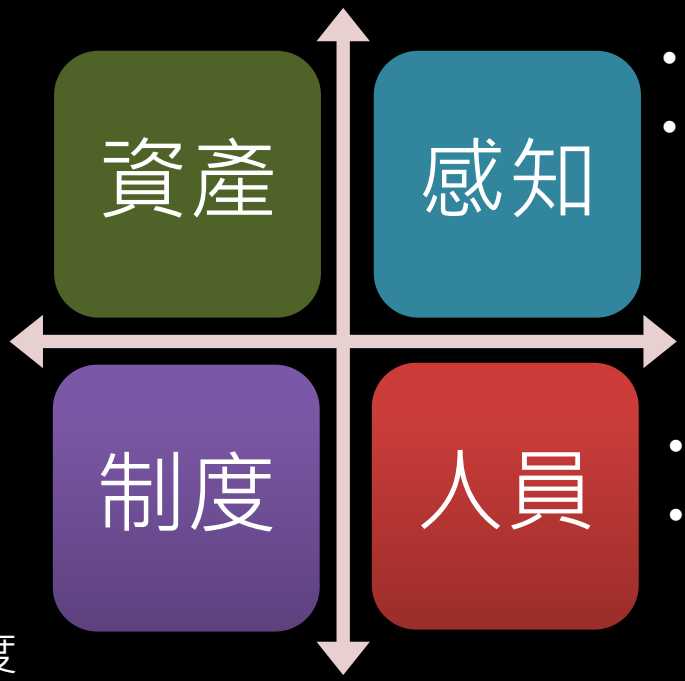
- 內部人員
- **供應鏈廠商**
- 維運人員

中華資安國際

圖片來源：https://support.flaticon.com/hc/en-us

因應OT資安挑戰之切入點

- 提高資產可視性
- 掌握資產清單及網路拓樸
- 建置/落實資安管控及權限分級機制



- 落實弱點管理與風險評估
- 建立內外部的威脅警報
- 強化SOC監控範圍與能力
- 適當的資安檢測

- 完善隔離機制
- 建置監控及應變機制 (OT-SOC、IR)
- 落實資安相關管理制度 (如：ISO 27001/ BS10012)

- 提高內部人員資安意識
- 管控或規範供應鏈人員

因應OT資安挑戰之切入點-資產

提高資產可視性

適當檢測

- 資產識別
- 已知弱點查找

權限識別

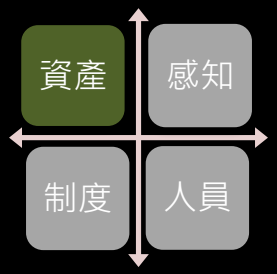
- 最小權限原則
- 現有資產與權限分配

安全措施盤點

- 安全相關政策(實體/資料)
- 搭配網路架構
- 資安設備增/汰需求

網路架構檢視

- 檢視網路架構及各項設備配置



中華資安國際

圖片來源：https://support.flaticon.com/hc/en-us

因應OT資安挑戰之切入點-感知

弱點與風險管理

風險評估

- 系統重要性評定
- 脆弱性識別
- 風險管理
- 風險緩解

弱點評估

- 安全的弱點掃描
- 安全的滲透測試
- 追蹤安全更新資訊
- 追蹤歷史弱點修復

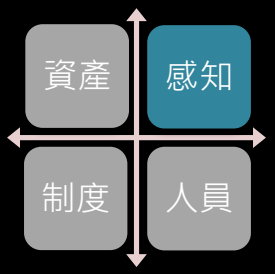
強化既有監控能力

SOC監控/通報

- 建立正常行為基準線(Baseline)
- 針對OT/IT領域特性進行監控
- 建立包含OT與IT專家的監控團隊
- 建立適當的通報及緊急處理機制

遠端行為管制

- 各帳號依權限管控
- 異常行為告警



圖片來源：https://support.flaticon.com/hc/en-us

因應OT資安挑戰之切入點-制度

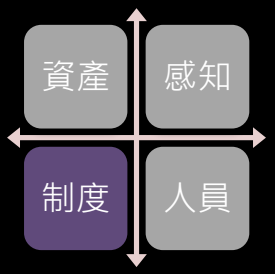
導入制度&落實隔離機制

導入制度

- 完善隔離/權限分級制度
- BS 10012 個人資訊管理
- **ISO/IEC 27001 資訊安全**

落實隔離機制

- 制定門禁管制機制
- 落實網段隔離及防火牆建置

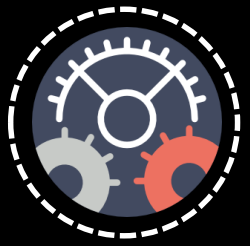


中華資安國際

圖片來源：https://support.flaticon.com/hc/en-us

因應OT資安挑戰之切入點-人員

教育訓練&建立規範

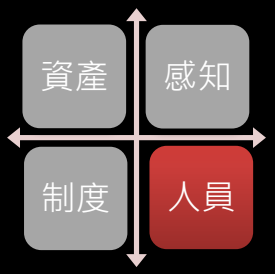


教育訓練

- 資安觀念課程
- 資安反應訓練
- 資安事故演練

建立規範

- 供應鏈人員操作限制
- 外部人員進入限制規範
- 落實文件紀錄(交班、門禁.....)



中華資安國際

圖片來源：https://support.flaticon.com/hc/en-us

四、結語

IT與OT網路已逐步融合，OT資安威脅上升，需共同合作打造安全的場域環境

人員教育訓練/
導入資安制度

實施風險評估

定期進行資安檢測

OT-SOC 7*24監控

臺灣資安大會
CYBERSEC 2019

Value Creator for
Investors, Customers, Employees, and Society

敬請指教
Thank you!