

資安策略思維

-- 從ROI談資安技術佈局

吳宗成

台灣科技大學管理學院院長
台灣科技大學資訊管理系教授
中華民國資訊安全學會理事長
TWISC@NTUST

IT投資

■ 類型

- 基礎建設型投資 (infrastructure investment)
 - 進入門檻必要條件
- 交易型投資 (transactional investment)
 - 改進作業流程或組織，創造交易價值
- 資訊型投資 (informational investment)
 - 改進管理資訊，創造資訊價值
- 策略型投資 (strategic investment)
 - 擊退競爭對手，獲得選擇優勢

■ 成本

- 硬體 (實體) & 軟體 (邏輯)
- 人員 (教育訓練) & 推廣 (認知)

IT的ROI

■ 創新服務 (Creative Service)

- 有形價值 → 可正確估算
 - 可創造利益的營運模式 (business model)
 - 回收利益值大於投資值
- 無形價值 → 無法正確估算
 - 企業或組織形象

■ 有效管理 (Effective Management)

- 有形價值 → 直接利潤
 - 時間 (降低生產時間)
 - 數量 (提高銷售數量)
- 無形價值 → 間接利潤
 - 企業或組織形象
 - 能量或能力提升 (尤其是人力資源方面)

資安投資

■ 類型

－ 攻擊 (Offense)

- 企業不宜涉及
- 僅有少數國家或個人會從事此類投資

－ 防衛 (Defense)

- 國家、企業或個人應投入此類投資

■ 成本

－ 硬體 (實體) & 軟體 (邏輯)

－ 人員 (教育訓練) & 推廣 (祛除阻力)

資安投資的期待結果

■ 期待結果 – 業務單位的觀點

- 回收利益大於投資

■ 真實結果

- 防衛投資 >> 攻擊投資
- 無形價值 > 投資值 > 有形價值

■ No security no talk – 沒有安全，免談！

- No security, no trust
- No trust, no fairness
- No fairness, no transaction
- No transaction, no money
- No money, no talk

如何估算資安的ROI？

■ 獲取有形價值

- No (大多數的結局)
- Yes (僅安全服務提供者適用之)

■ 產生無形價值

- 當作間接利潤的「藥引」(例如：提供作業程序的有效安全管理作為，進而創造高品質的產品)
- 降低損失(例如：降低有價值的資訊資產或系統失能後對組織所產生的衝擊)

資安趨勢

- 資料安全 (data security)
 - 1970s
 - 加解密技術
- 系統安全 (system security)
 - 1980s → 自動化
 - 電腦病毒
- 網路安全 (network security)
 - 1990s → e化
 - 入侵偵測
- 網站與無線網路安全 (web & wireless network security)
 - 2000s → M化
 - 應用系統安全、內容安全 (content)
- 普及計算安全 (ubiquitous computing security)
 - 2005? 2010? → U化
 - 低資源計算或行動裝置安全、隱私保護 (privacy)

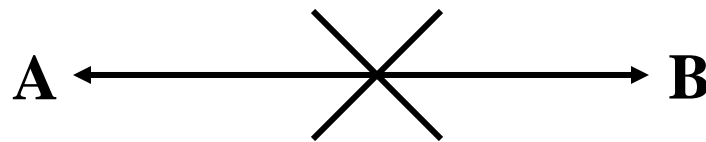
資安基本需求

■ CIA + NR

- 機密性(**C**onfidentiality) – 資料
- 完整性(**I**ntegrity) – 資料與系統
- 可取用性(**A**vailability) – 系統服務
- 鑑別性(**A**uthenticity) – 通信個體
- 不可否認性(**N**on-**R**epudiation) – 應用

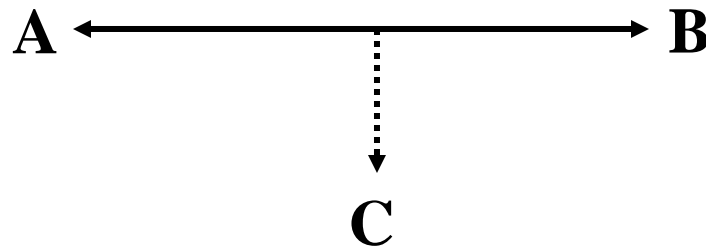
資安威脅來源之一

- 中斷(interruption) – 可用性(availability)
 - ✓ 使系統資源遺失、不可取用、不堪使用
 - ✓ 惡意破壞硬體設備、刪除程式或資料檔、使系統阻絕服務(Denial of Services, DoS)



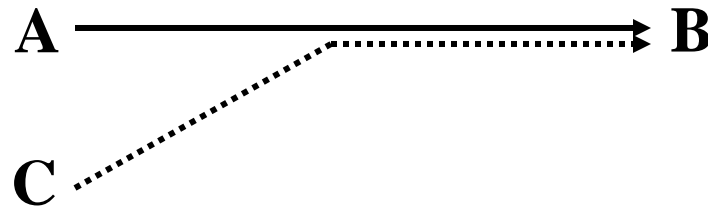
資安威脅來源之二

- 截取(interception) – 機密性(confidentiality)
 - ✓ 未授權者能非法存取資料
 - ✓ 網路測錄



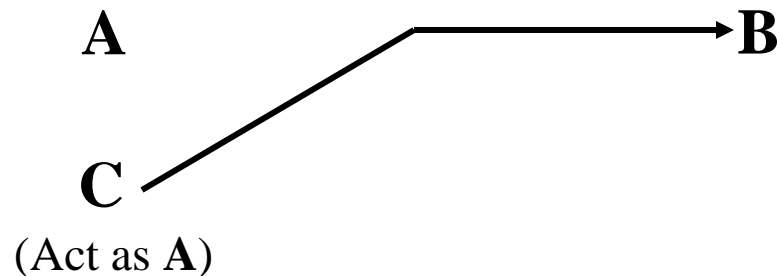
資安威脅來源之三

- 更改(modification) – 完整性(integrity)
 - ✓ 未授權者能更改系統程式或資料
 - ✓ 更改儲存或傳輸資料之數值、或更改程式，以執行額外運算



資安威脅來源之四

- 仿造(fabrication) – 鑑別性(authenticity)、不可否認性(non-repudiation)
 - ✓ 未授權者仿造資料，資料使用者無法分辨真偽
 - ✓ 插入額外的交易訊息、偽造資料記錄



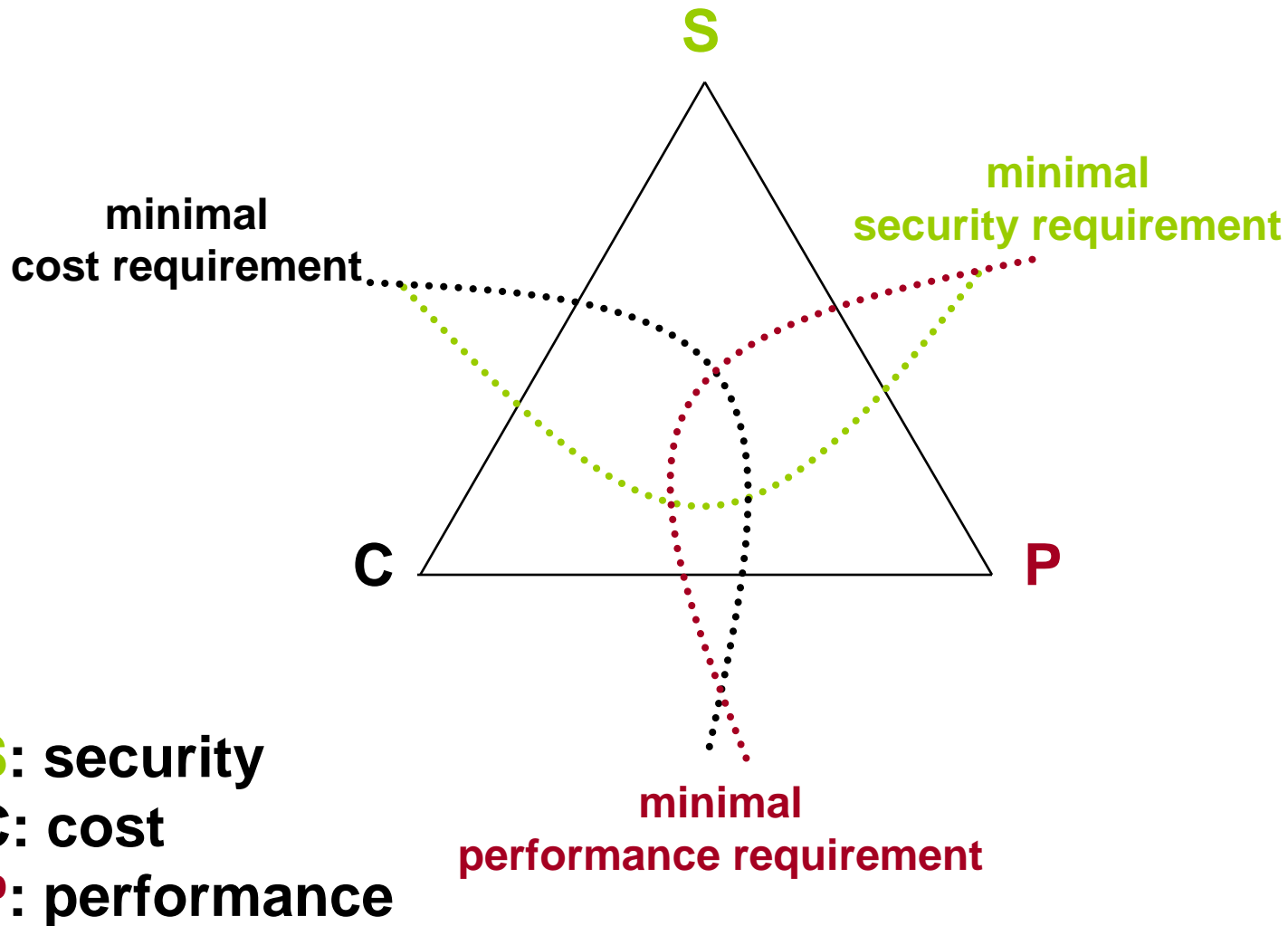
從系統角度看資安技術佈局

- 軟體(software)
 - 完整性、可取用性
- 硬體(hardware)
 - 鑑別性、可取用性
- 資料(data)
 - 機密性、完整性、可取用性、鑑別性、不可否認性
- 人員(people)
 - 鑑別性、不可否認性
- 程序(procedure)
 - 完整性、可取用性、不可否認性

資通安全最高策略原則

安全 ⇔ 信任
SECURITY ⇔ **TRUST**

資通安全新思維 – SCP model



SCP 重新詮釋

不是找出「最佳的」解決方案
是要找出「最可接受的」解決方案

企業系統思維 VS 政府系統思維

成本

安全

資通安全新思維 – 3W model

- Know-**W**hat → for end user
 - 清楚界定資安「定位」與「範圍」
 - 定位：資料？軟體？硬體？程序？人員？
 - 範圍：開放系統versus封閉系統
- Know-**h**o**W** → for engineer/designer
 - 資安設計邏輯應是「White-box」，而非「Black-box」
- Know-**W**hy → for administrator/decision maker
 - 清楚瞭解安全風險與衝擊分析(impaction analysis)
 - 預防？抵抗？善後？

全面與整體思維

- 安全能力 (capability)
 - Capability = Hardware + Software + Data + Application (Procedure) + People
- 未雨綢繆
 - 安全生命週期 vs 系統生命週期
 - 長期安全 (實體空間 vs 虛擬空間)
- 安全需求導向 (target orientation)
 - 獲得有形價值抑或無形價值
 - 最小安全能力 + 可控制安全 (controlled security)

結語

■ A → A+ → A++

- **Awareness**(認知): A
 - 技術認知（研發人員）與非技術認知（使用者）
- **Accountability**(責任): A+
 - 每一位參與人員都有其責任歸屬
- **Alliance**(聯盟): A++
 - 防衛聯盟（國內外、產官學研）