資訊安全系統規劃與設計

吳宗成
臺灣科技大學資訊管理系 特聘教授
臺灣科技大學資通安全研究與教學中心
TWISC@NTUST
tcwu@cs.ntust.edu.tw

講者學經歷簡介

- 學歷
  - 臺灣大學資訊工程系學士(1979/9~1983/6)
  - 中興大學應用數學研究所碩士(1987/9~1989/6)
  - 交通大學資訊工程研究所博士(1989/9~1992/6)
- 經歷
  - 臺灣科技大學資訊管理系副教授(1992/8~1997/1)
  - 臺灣科技大學資訊管理系教授(1997/2~2014/3)
  - 臺灣科技大學資訊管理系主任(1999/8~2003/7)
  - 臺灣科技大學管理學院院長(2007/8~2010/7)
  - 臺灣科技大學資訊管理系特聘教授(2014/3~)
  - 中華民國資訊安全學會理事長(2006/6~2012/5)

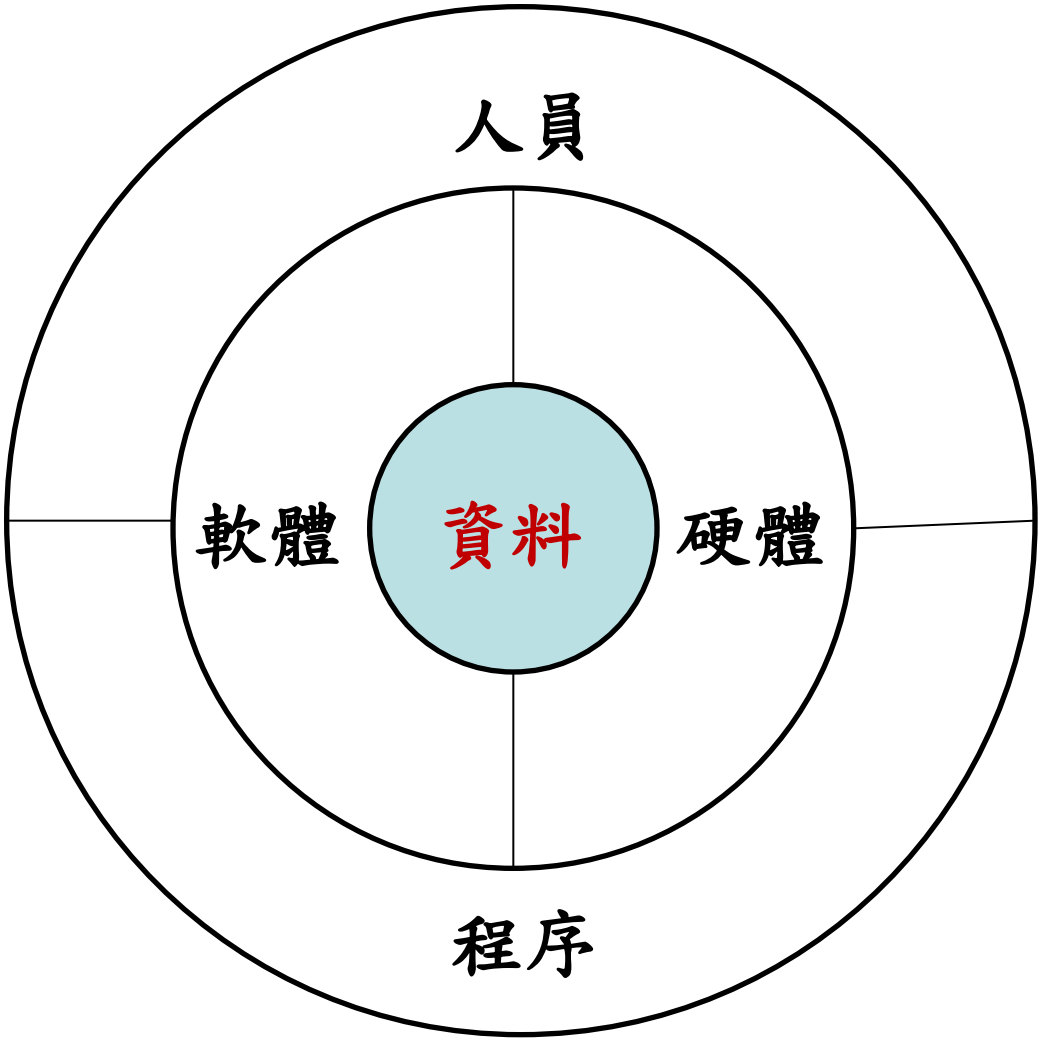
開宗明義

資訊系統五大組件

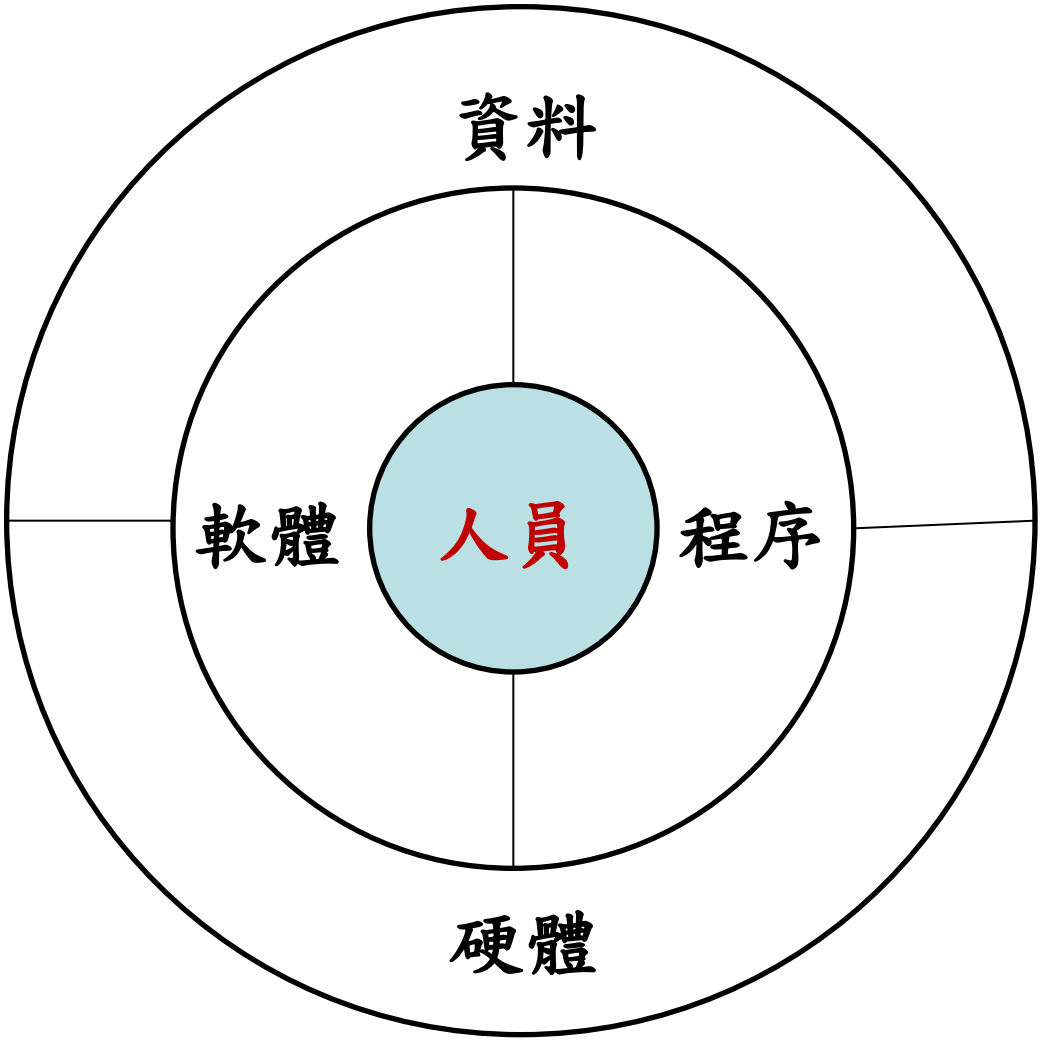
- **資料**
  - ✓傳輸資料 vs. 儲存資料(檔案、資料庫)
- **軟體**
  - ✓作業系統 vs. 應用系統
- **硬體**
  - ✓固定裝置 vs. 可攜(行動)裝置
- **人員**
  - ✓系統發展者 vs. 系統管理者 vs. 端末使用者
- **程序**
  - ✓正常程序 vs. 例外程序(exceptional procedure)

➢資訊系統的價值何在？關鍵組件為何？

資料導向的資訊系統示意圖



服務導向的資訊系統示意圖



系統發展生命週期

- **System Development Life Cycle(SDLC)**
  - **R**equirement（需求/規劃）
  - **E**valuation（評估）
  - **D**esign（設計）
  - **I**mplementation（實作/建置）
  - **O**peration & **M**aintenance（運作與維護）

系統發展生命週期參與的角色

- 每一個系統發展階段皆涉及不同屬性及不同角色的參與人員
- 規劃角色
  - 決策者、開發/專案管理者、使用者
- 設計/操作/維護角色
  - 系統擁有者、系統建置者、系統管理者、端末使用者

系統發展的困境－溝通

- 系統需求階段(R)參與人員的溝通介面
  - 規劃角色間的溝通
- 系統評估階段(E)參與人員的溝通介面
  - 涵蓋規劃與設計/操作/維護角色間的溝通 → 影響系統生命週期
- 系統設計、建置、操作、維護(D&I, O&M)階段參與人員的溝通介面
  - 設計/操作/維護角色間的溝通

系統發展的困境–限制

- 依系統需求目標，列出資訊系統的所有可行方案（概念式系統）或Proof-of-Concept
- 在具限制性的資源（人力、經費、時間）之下，評估系統的實務可行性，以及是否可達成既定的系統需求目標
- 擬定「發展策略」(strategy)及相對應的「行動方案」(action plans)

系統發展的困境－策略

- 管理策略
  - 業務營運(business)
  - 運作(operation)及維護(maintenance)
  - 冰山堡效應(ice-burg effect)
- 技術策略
  - 效能(performance)
  - 有用性(availability)
  - 世代轉換(generation changeover)

管理策略

- 關鍵績效指標（Key Performance Index）
  - 量化指標 → 組合最佳化
    - 投最少的人力
    - 用最少的經費
    - 花最短的時間
  - 質化指標 → 影響力
    - 最高品質（0%）
    - 中上品質（30%）
    - 可接受的最低品質（70%）
- 落實管理策略 → 業務資訊化

技術策略

- **What: Problem**
  - 從使用者需求面來確立問題
- **hoW: Solution**
  - 從供給面找出可能的解決方案
- **Why: Innovation**
  - 從業務應用面創造出擬用技術的新價值
- 技術策略 → 資訊業務化

管理策略VS.技術策略

- **CASE 1**
  - 管理策略與技術策略沒有交集 → 雞同鴨講
- **CASE 2**
  - 管理策略凌駕技術策略之上 → 畫大餅
- **CASE 3**
  - 技術策略凌駕管理策略之上 → 不食人間煙火
- **CASE 4**
  - 管理策略與技術策略彼此融合 → **Bingo!**

資訊系統的規劃與投資策略

- 基礎建設投資（Infrastructural investment）
  - 配合組織改造(restructuring)
- 交易投資（Transactional investment）
  - 配合流程改造(reengineering)
- 資訊投資（Informational investment）
  - 創造知識管理(knowledge management, KM)的價值
- 策略投資（Strategic investment）
  - 延續商業智慧(business intelligence, BI)

系統規劃與設計原則

- 採用模組化(modularization)方式，適當切割系統，降低系統發展工作的複雜度與困難度
  - 資料獨立性(data independence)
  - 子系統獨立性(sub-systems independence)
  - Why? → system changeover(系統轉換)
- 設立足夠的審核檢查點，以利管理工作的進行
  - 7±2個工作活動設立一個檢查點
- 選擇適當的人員參與規劃與設計工作
  - 端末使用者、管理人員(含一般管理人員與財務人員)、技術專家

資訊系統發展評估

- 可行性因子（feasibility factors, TELOS）
  - Technological feasibility：技術可行性
  - Economic feasibility：經濟可行性
  - Legislative feasibility：法律可行性
  - Operational feasibility：操作可行性
  - Schedule feasibility：時程可行性
- 策略性因子（strategic factors, PDM）
  - Productivity：提升生產力
  - Differentiation：創造差距（或差異化）
  - Management：強化管理

技術可行性

- **既有技術能力**
  - ✓IT/IS趨勢：能否完成概念性系統設計
  - ✓人員能量：能否完成細部性系統設計、系統製作與系統維護
- **新增技術能力**
  - ✓對既有之系統發展人員施予教育訓練
  - ✓新加入具有新技術能力的系統發展人員

經濟可行性

- **直接成本與間接**
  - ✓有形成本：軟硬體設備、人力
  - ✓無形成本：管理、折舊
- **直接效益與衍生效益**
  - ✓有形效益：量化指標
  - ✓無形效益：質化指標

法律可行性

- 權利保障及服務水準要求
  - ✓合約書、契約書之權利義務關係
  - ✓法律規範
- 避免權利侵犯
  - ✓採行技術是否侵犯專利權、著作權 **(The best-seller software → Copy everything in the disk)**
  - ✓採行技術是否侵犯個人隱私保護

操作可行性

- 操作介面
  - ✓Procedure-oriented vs. Icon-based
  - ✓General-purpose vs. Customization
- 教育訓練計畫
  - ✓端末使用者
  - ✓系統管理者

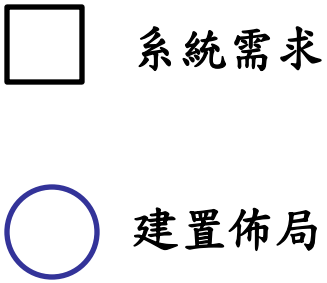
時程可行性

- 有例可循
  - ✓參考既有系統發展之經驗值
- 新系統發展
  - ✓常用的工作分解技術
    - 條列法(check-list method)
    - 階段法(phase method) ：系統導向或資料導向
  - ✓常用的排程技術
    - CPM 網路(Critical Path Method)
    - 甘特圖(Gantt chart)

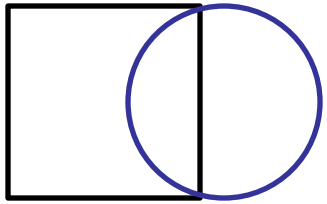
策略性因子評估

- 系統擁有者評估
  - ✓財務規劃(Return of Invest, ROI)
  - ✓KPI：量化＋質化(saving)
  - ✓與競爭對手的差距化(differentiation)
- 系統管理者評估
  - ✓可維護性
  - ✓可擴充性
- 端末使用者評估
  - ✓親和性(介面)及正確性（處理程序）
  - ✓提升生產力（效能）

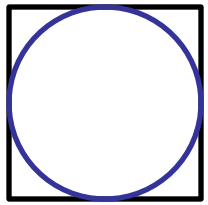
Discussions of Pseudo Cases



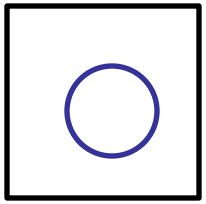
A



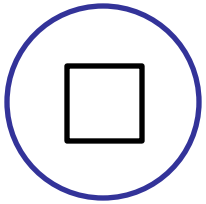
B



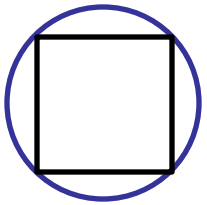
C



D



E



資訊安全需求

資訊安全（資安）的定義

- 維基百科(Wikipedia)
  - **Information security means protecting information and information system from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction**
- 何謂「資訊」“information”?
  - 有價值的格式化資料(valuable formatted data)
  - 涉及「傳輸」與「儲存」形式的相關業務應用
- 何謂 「資訊系統」“information system”?
  - 資料、軟體、硬體、人員、程序

系統運作與資安特性

- 運作
  - ✓ 電腦計算取代人工作業
  - ✓ 理論基礎取代土法煉鋼
  - ✓ 應用/系統導向(app-oriented)取代模組導向(module-oriented)
  - ✓ 從看得到的有線(wired)到摸不著的無線(wireless)
- 特性
  - ✓ 無所不在(ubiquitous)的*u*-化生活：**any time, any where, any device, any thing (content)**
  - ✓ 無法捉摸的威脅來源，無法想像的攻擊能量

資安趨勢－過去、現在、未來

- 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、數位簽章
- 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/雲端安全(ubiquitous/cloud security)
  - 2010? 2015? 2020? → *u*化
  - IoT（Internet of Things）安全、隱私與智財保護（privacy & piracy）、數位鑑識（digital forensics）

資安需求 – CIA + NR

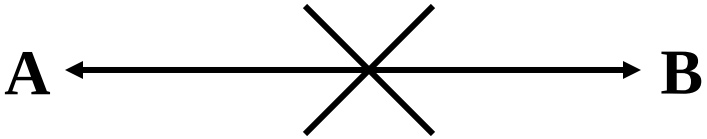
- 機密性(Confidentiality) – 資料
- 完整性(Integrity) – 資料與系統
- 可用性(Availability) – 系統服務
- 鑑別性(Authenticity) – 通信個體
- 不可否認性(Non-Repudiation) – 應用

➔新型態的資安需求：

- 個人資料及隱私保護(Personal Information & Privacy Protection)
- 數位鑑識(Digital Forensics)

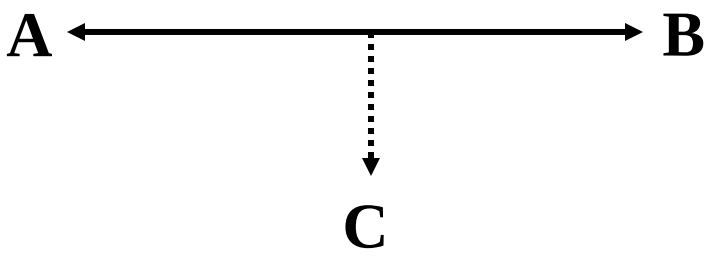
資安威脅來源之一

- 中斷(interruption) – 違反可用性
  - ✓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)



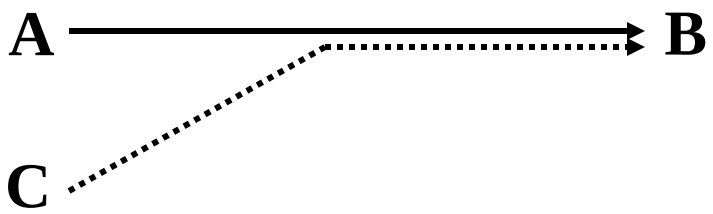
資安威脅來源之二

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



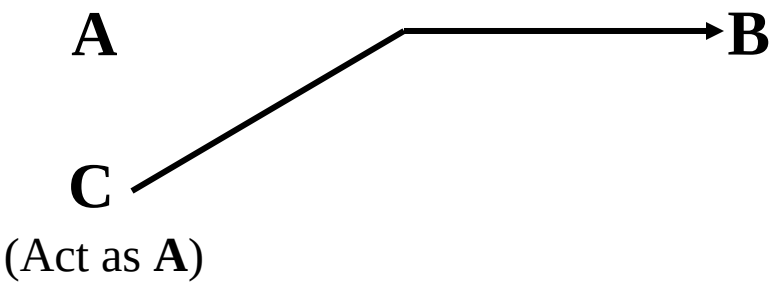
資安威脅來源之三

- 更改(modification) – 違反完整性
  - ✓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) – 違反鑑別性、不可否認性**
  - ✓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

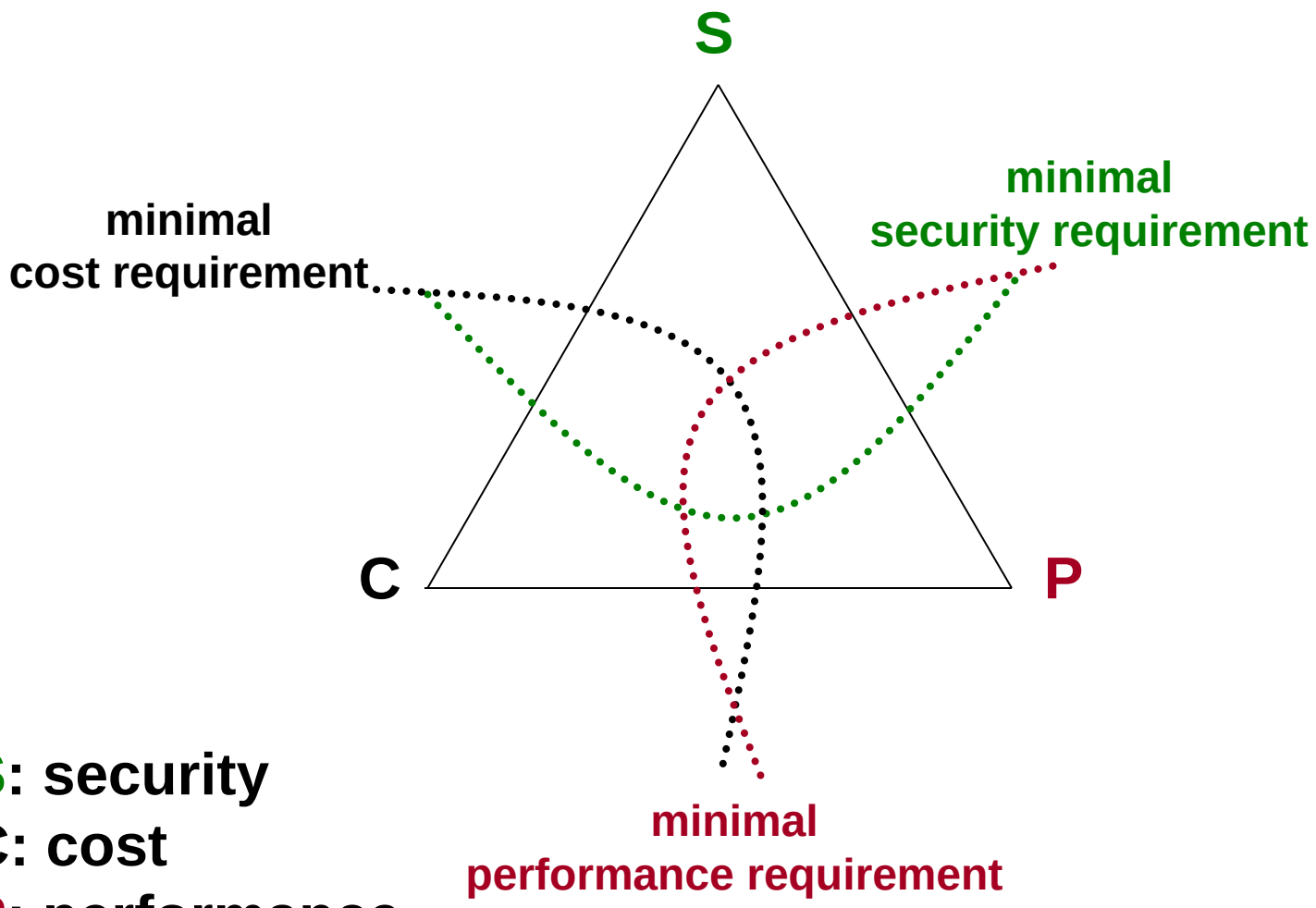


資訊安全系統發展
及
實務可行性評估

資訊安全系統開發的生命週期

- **Security System Development Life Cycle (SSDLC)**
  - 兼顧SDLC（系統發展生命週期）的各階段要求
  - **S**ecurity（安全）
  - **C**ost（成本）
  - **P**erformance（效能）

SCP model



S: security
C: cost
P: performance

SCP 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

企業系統發展思維 VS. 政府系統發展思維

成本　　安全

資訊安全系統的主要投資類型

- 基礎建設投資（Infrastructural investment）
  - 軟體/硬體運作環境：網路、資料庫、MIS等
- 交易投資（Transactional investment）
  - 程序：正常及例外處理
- 資訊投資（Informational investment）
  - 資料：資料本身或其衍生應用服務的價值
- 策略投資（Strategic investment）
  - 人員：客戶關係管理(Customer Relation Management)及企業資源規劃(Enterprise Resource Planning)

資訊安全系統的必要成本

- 實體/硬體Hardware (physical)
  - Network (wired and wireless) and access devices
  - Database (data store)
- 軟體Software (logical)
  - Applications and security control
- 人員People (resources)
  - Restructuring of organization and reengineering of processes
- 推廣Promotion (awareness and resistance)
  - Education and training

資安投資者的思維 – ROI在哪？

- 是否可獲得有形價值（tangible value）
  - No (in most of cases)
  - Yes (only for security services provider)
- 是否增加無形價值（ intangible value）
  - As used to the trigger of “indirect” value
    - Image of enterprise/organization
    - Effective management of application or production system
  - As used to reduce the loss of property
    - The winner is the one who loses less

資安端末使用者的思維

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

→ No security, no talk!

資訊安全系統
實務佈局

每天都在發生的資安攻擊事件

- **技術攻擊法（technical attacks）**
  - 資料：破解加解密或數位簽章機制
  - 軟體：利用系統防護漏洞、應用程式漏洞（動態分析）或程式語言缺陷（靜態分析）
  - 硬體：利用硬體設備或外裝之脆弱性
  - 程序：利用操作程序之邏輯錯誤
  - 人員：破解過短或懶人通行密碼
- **非技術攻擊法（non-technical attacks）**
  - 暴力（brute forces）：使用刀、槍、或肢體暴力，讓使用者被動提供敏感個資、密碼金鑰或系統控制權
  - 社交工程（social engineering）：在不自覺或非自主意志的情況之下，誘導或詐騙使用者提供敏感個資、密碼金鑰或系統控制權 → 完美攻擊？

資安佈局思維

- 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)
- 安全目標導向（target-oriented）
  - 有形價值 vs. 無形價值
  - 最小安全能力 vs. 可控制安全

資安佈局思維切入點

- 資料導向(data-oriented)的系統
  - 物件：儲存資料或資料庫
  - 主體：人員(使用者)
- 程序導向(process-oriented)的系統
  - 物件：傳輸資料或交易
  - 主體：程序或軟體
- 人員導向(people-oriented)的系統
  - 物件：資料、軟體、硬體
  - 主體：人員或程序

從系統角度看資安需求佈局

- 軟體(software)
  - 完整性、鑑別性、可用性
- 硬體(hardware)
  - 鑑別性、可用性
- 資料(data)
  - 機密性、完整性、可用性、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、可用性、不可否認性

Physical system

Logical system

資安佈局的策略目標

安全 ⇔ 信任

SECURITY ⇔ TRUST

TRUST的基礎 – SCDR

- **SCOPE（範圍）**
  - **Do you fully recognize the security requirements you want in the business domain?**
- **CONTROL（掌控）**
  - **Controlled security to the design of white box (engineer-oriented) or black box (end user-oriented)**
- **DEPLOYMENT（導入）**
  - **Selection of automatic (more efficient) or manual (more secure) procedures**
- **RISK（風險）**
  - **Do you fully understand the impact of security leak?**

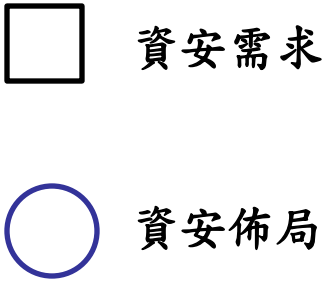
資安新思維 – 3W model

- **Know-What → 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 vs. 封閉系統
- **Know-hoW → for engineer/designer**
  - 資安設計邏輯應是「White-box」，而非「Black-box」
- **Know-Why → for administrator/decision maker**
  - 清楚瞭解安全風險與衝擊分析(impact analysis)
  - 預防？抵抗？善後？

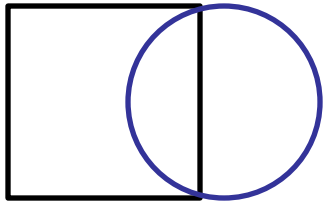
資安實務評估 – TELOS +PDM

- 可行性因子（TELOS）
  - Technological feasibility：技術可行性
  - Economic feasibility：經濟可行性
  - Legislative feasibility：法律可行性
  - Operational feasibility：操作可行性
  - Schedule feasibility：時程可行性
- 策略性因子（PDM）
  - Productivity：提升生產力
  - Differentiation：創造差距（或差異化）
  - Management：強化管理

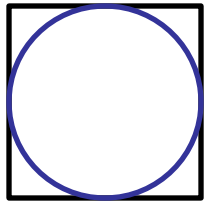
Discussions of Pseudo Cases



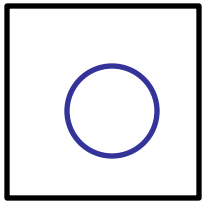
A



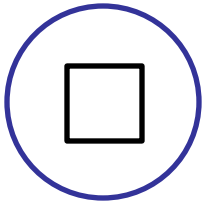
B



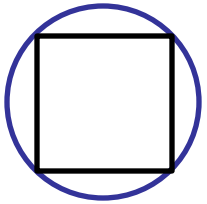
C



D



E



資訊安全系統
實務管理

實務上常見的資安脆弱性(1/2)

- 基於效率考量，採用大量集中的同質資料庫設計
  - 當一條蛇找到一顆蛋，就表示它已找到了一窩蛋！
- 無法認定所採用之作業系統、網路通信協定、資料庫系統、密碼模組的整合安全等級
  - 解決個別安全問題注意是否達成整體安全問題
- 過度強調「系統保護」（例如防火牆、入侵偵測等運作機制）而忽視「資訊保護」（例如加解密、數位簽章等密碼學機制）的重要性
  - 前線吃緊或失守，後線就要轉成前線了！

實務上常見的資安脆弱性(2/2)

- 所採用之技術能量來源的單一性太強，大都是採用來自極少數廠商之產品，無法有效分散資安技術風險
  - 天若塌下來，是會壓垮一大堆人的
- 資安稽核過度偏重安全管理稽核，而忽略安全技術稽核
  - 落實資安研發人才培育計畫
  - 通資安人才升遷管道

值得關注的資安實務(1/2)

- 功能目標需求
  - ✓ 完整性(integrity)的重要性將耀居首位
  - ✓ 匿名性(anonymity)及隱私性(privacy)的需求與日俱增
- 技術規格需求
  - ✓ 更安全的加解密技術：AES完全取代DES的時代已來臨
  - ✓ 更具效率的數位簽章技術：基於橢圓曲線（金鑰長度短）或多變量密碼學（計算速度快）的數位簽章
  - ✓ 更智慧的入侵偵測、病毒防治：基於智慧型或機器學習(machine learning)的資訊系統將再引領風騷
  - ✓ 無所不在的行動安全：無線網路或行動裝置(Smart phone, iPad, RFID, NFC, etc.)將更為普及

值得關注的資安實務(2/2)

- 應用需求
  - ✓ 電子商務/行動商務：結合Web services的整合式行動電子交易（採購、線上付款、電子發票等）或創新商業模式
  - ✓ 智慧財產：多媒體數位內容保護（傳播）
  - ✓ 個人資料保護：法令遵循(compliance)及資料遮罩(masking)
  - ✓ 資安仲裁：數位證據(digital forensics) → 科技＋法律遵循

結語: A → A+ → A++

- **Awareness(認知): A**
  - 管理人員的技術認知
  - 技術人員的管理認知
- **Accountability(責任): A+**
  - 每一位參與人員都有其責任歸屬
- **Alliance(聯盟): A++**
  - 防衛聯盟或產業聯盟 (國內外、產官學研)

資安哲學

見小曰明、守柔曰強

– 老子道德經

From the view point of

Application planners and designers

資安哲學

眾裡尋他千百度，驀然回首，
那人卻在燈火闌珊處
－辛棄疾「青玉案」

From the view point of
end users

贈後語

諸可還者，自然非汝
不汝還者，非汝而誰

（楞嚴經文）