全方位資訊安全防護-理論與實務

湧泉科技管理顧問有限公司
Alex Lai

Agenda

- 從資安小故事說起-資訊安全常見誤區
- 何謂全方位資訊安全防護？
- 資安實務Workshop
  - 風險管理實作
  - 事故處理與根因分析-理論與實務
  - 事故處理-流程繪製

資安～是門好生意-你（妳）準備好了沒？

從資安小故事說起！

~資訊安全常見誤區~

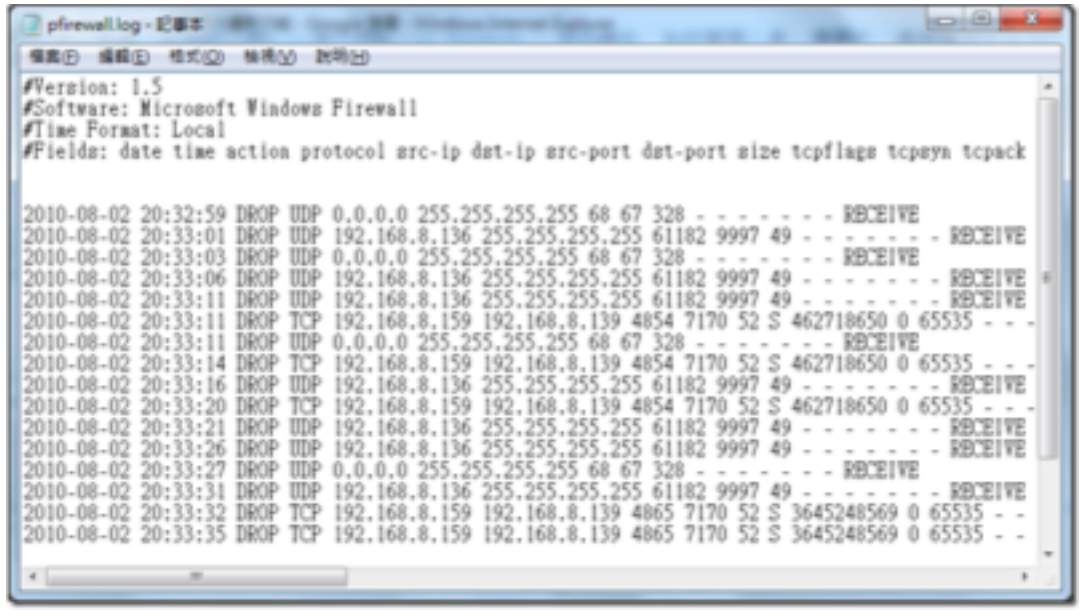
事故管理-我都有很認真做！

- 某家公司業務人員在網路上發現有駭客公布成功駭入其公司網站,客戶資料被盜取並PO網,該公司相關人員處理程序如下:

1. 發現網站遭駭的業務部門員工立即通報資訊單位。
2. 資訊單位依照通報,立即修補了系統漏洞與程式漏洞,調整資安設備的設定,並且在當天將網站漏洞修復完成並恢復正常運作。
3. 在此事件處理完畢之後,亦召開內部的檢討會議,建立了網站安全管理的機制,並確實執行。

看事情永遠只看到一面～解決方法還有很多種！

LINE



pfirewall.log - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

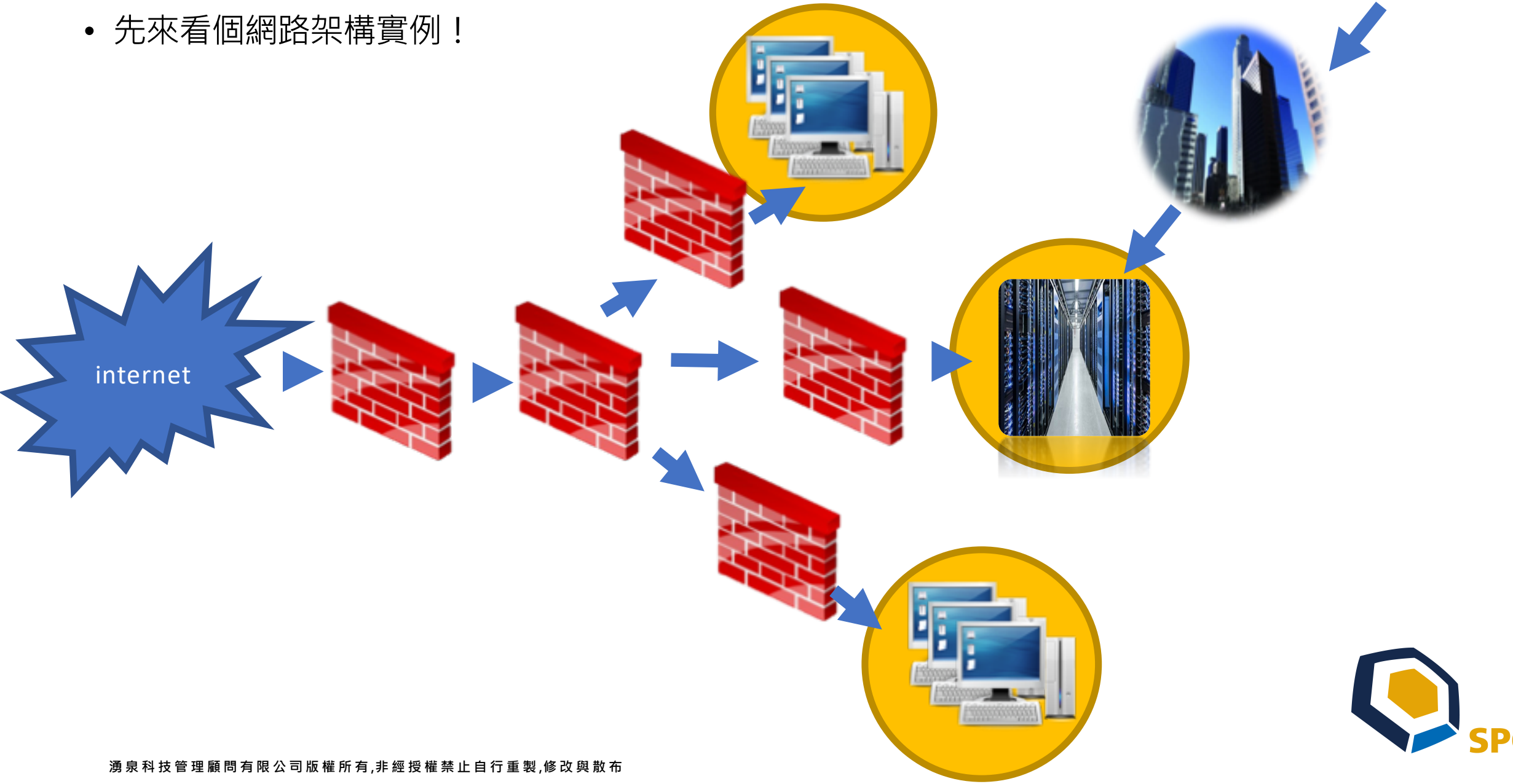
```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack


2010-08-02 20:32:59 DROP UDP 0.0.0.0 255.255.255.255 68 67 328 - - - - - - - - RECEIVE
2010-08-02 20:33:01 DROP UDP 192.168.8.136 255.255.255.255 61182 9997 49 - - - - - - - - RECEIVE
2010-08-02 20:33:03 DROP UDP 0.0.0.0 255.255.255.255 68 67 328 - - - - - - - - RECEIVE
2010-08-02 20:33:06 DROP UDP 192.168.8.136 255.255.255.255 61182 9997 49 - - - - - - - - RECEIVE
2010-08-02 20:33:11 DROP UDP 192.168.8.136 255.255.255.255 61182 9997 49 - - - - - - - - RECEIVE
2010-08-02 20:33:11 DROP TCP 192.168.8.159 192.168.8.139 4854 7170 52 S 462718650 0 65535 - - -
2010-08-02 20:33:11 DROP UDP 0.0.0.0 255.255.255.255 68 67 328 - - - - - - - - RECEIVE
2010-08-02 20:33:14 DROP TCP 192.168.8.159 192.168.8.139 4854 7170 52 S 462718650 0 65535 - - -
2010-08-02 20:33:16 DROP UDP 192.168.8.136 255.255.255.255 61182 9997 49 - - - - - - - - RECEIVE
2010-08-02 20:33:20 DROP TCP 192.168.8.159 192.168.8.139 4854 7170 52 S 462718650 0 65535 - - -
2010-08-02 20:33:21 DROP UDP 192.168.8.136 255.255.255.255 61182 9997 49 - - - - - - - - RECEIVE
2010-08-02 20:33:26 DROP UDP 192.168.8.136 255.255.255.255 61182 9997 49 - - - - - - - - RECEIVE
2010-08-02 20:33:27 DROP UDP 0.0.0.0 255.255.255.255 68 67 328 - - - - - - - - RECEIVE
2010-08-02 20:33:31 DROP UDP 192.168.8.136 255.255.255.255 61182 9997 49 - - - - - - - - RECEIVE
2010-08-02 20:33:32 DROP TCP 192.168.8.159 192.168.8.139 4865 7170 52 S 3645248569 0 65535 - -
2010-08-02 20:33:35 DROP TCP 192.168.8.159 192.168.8.139 4865 7170 52 S 3645248569 0 65535 - -
```

SPC

何謂全方位資安防護？

為什麼要做“全方位”資訊安全防護？

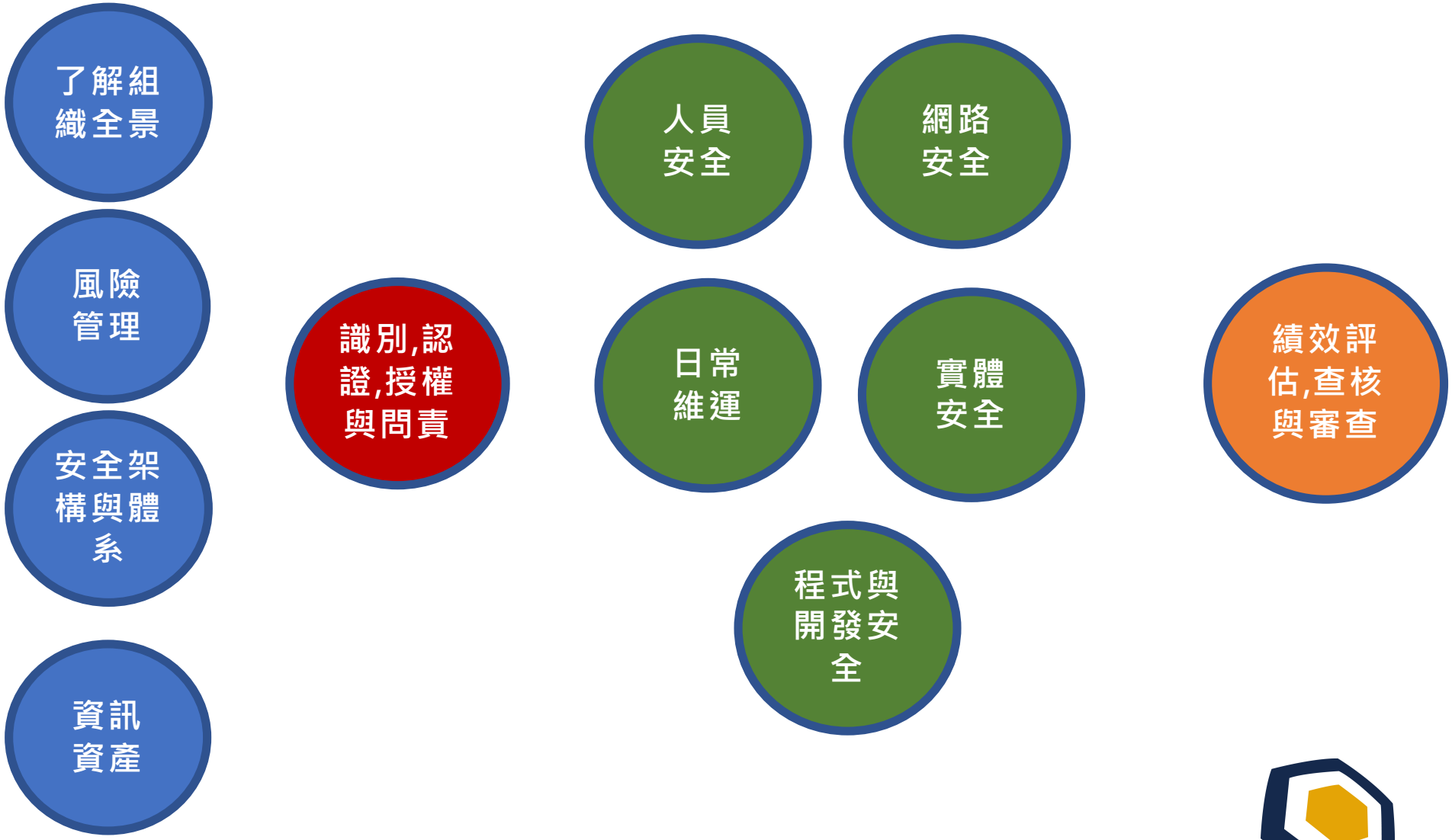
- 先來看個網路架構實例！



乳酪與資安！

資源與時間有限～只要駭客打不穿～我們就贏了！

全方位資安防護-包含哪些面向？



何謂組織全景

這些和我做資訊
安全有何關係？

競爭者

法令法規

股東

客戶/消費者/一般大眾

員工

身為一個資安人員,對於法律規範不可不知~

智慧財產權相關法規

差異何在?

何謂風險管理

- 風險：可以是好的也可以是壞的,不過大家通常都比較關注壞的
- 風險：非所欲的影響
- 風險 = Likelihood X Impact

風險管理的基礎概念

- 什麼是風險?

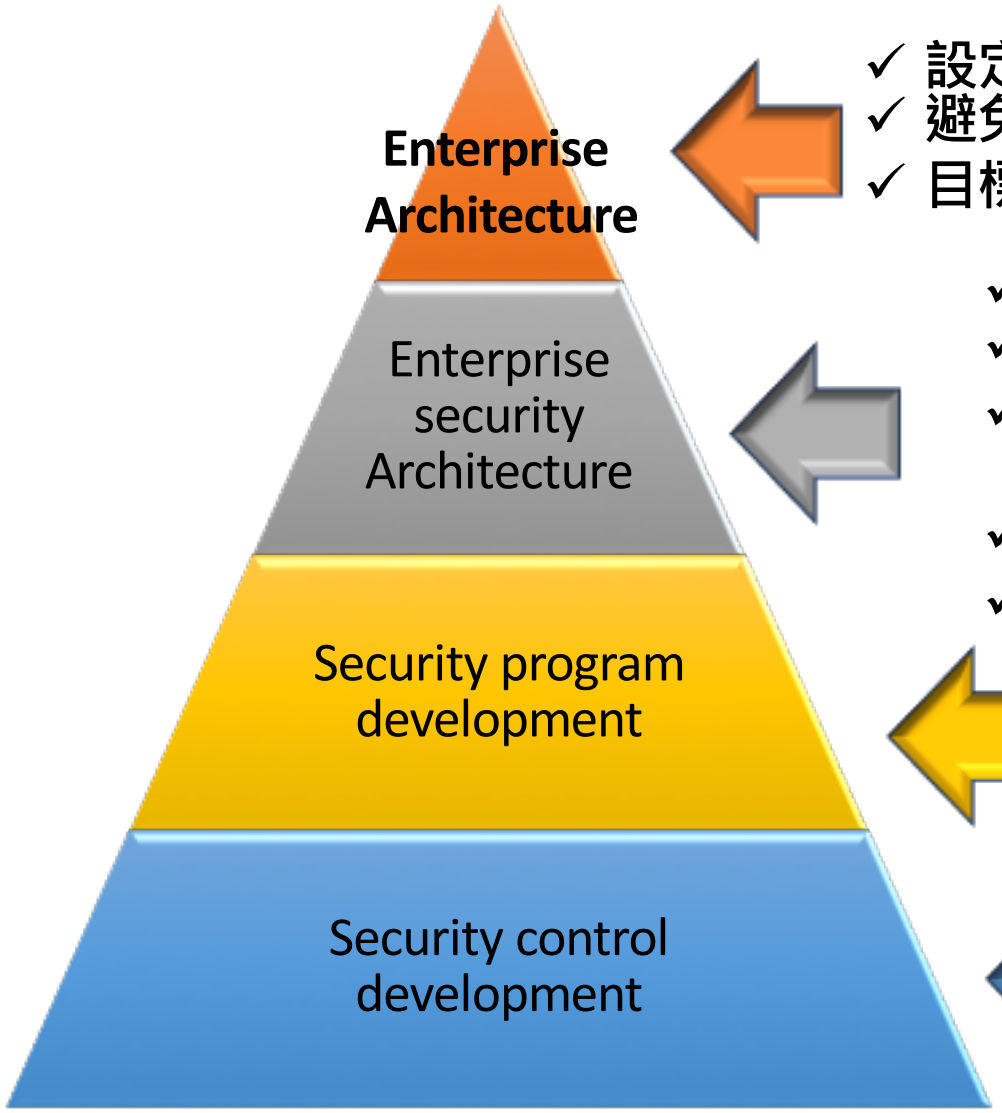
風險管理基本名詞-1

- Vulnerability
- Threat
- Exposure

問題:
1. 威脅與弱點哪個比較重要?
2. 重大弱點一定要處理?
3. 有違法的風險一定要處理?
你的想法是甚麼?為什麼?

安全體系與架構
-為何需要？

✓ 確保有效益,有效率且適當!



✓ 設定戰略方向
✓ 避免雞同鴨講
✓ 目標一致->Support營運方向

✓ 辦識利害關係人及其需求
✓ 提供不同檢視角度
✓ 確保Security solution與企業需求相符
✓ 提供一致性的安全標準
✓ 降低”驚喜”

✓ 建立資訊安全管理體系

✓ 具體的安全控制措施

何謂資訊資產？

- 任何對組織有價值的事物
- 所有的安全控制最終都將落實在資訊資產上！

何謂資訊資產？-續

- 既然所有的控制最終都會落實在資訊資產上,那麼你知道有哪些控制類別嗎？

Control Types

別把Control Types 和 Control functionalities 搞混了

- Control types
  - Administrative
  - Technical
  - Physical
- Control functionalities
  - Preventive
  - Detective
  - Corrective
  - Deterrent
  - Recovery
  - Compensating

最好的Control是能事先預防,但是通常不可能做到100%,若不能做到100%,那麼就應該要能夠及早偵測

- 問題: Which functionality is most productive?
  最好與哪一種functionality結合? WHY?

Workshop 10Min討論 5Min Report!

- 下列是屬與哪一種類型與功能的控制?

1. 資訊安全政策與程序
2. 警衛
3. 資料備份
4. 異地備分機房
5. 防毒軟體
6. 資訊資產分級分類
7. 監視器
8. 工作輪調
9. 燈光
10. 生物辨識系統
11. 職責分離
12. 移動偵測
13. 資訊資產分類
14. 數位鑑識
15. 加密
16. Server image
17. IDS

識別,驗證,授權與問責-從一個簡單的4步驟程序來理解!

我是ALEX啦
(公司有ALEX這個人嗎?)

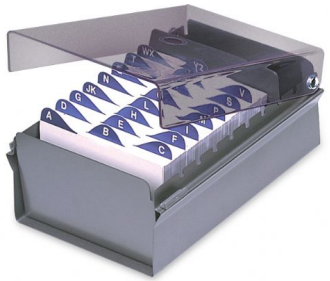
Identification

確認你是真的ALEX
(因為你知道只有ALEX知道或
擁有ALEX才有的...)

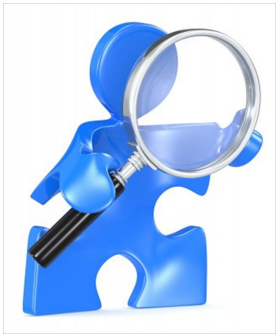
Authentication

嗯 Alex 你
有權限存取
這些檔案

Authorization



可存取的資源



紀錄Alex的行為
以供事後分析/查證

Accountability

識別的方式！

- Something you know-例如密碼
- Something you have-例如TOKEN
- Something you are-例如生物辨識

有關生物辨識的特性與議題

特性

- 獨特性
- 隱私性
- 不可修改
- 誤判

議題

- 很貴~(最貴的Authentication機制)
- 接受度
- 所需時間
- 處理速度
- 登錄時的方便度
- 有沒有考慮到對方不是活人嗎?
- 真正啟用時的不方便

人員安全-注意甚麼?

聘僱前

聘僱中

離職

人員安全-偵測異常的手法是？

- 工作輪調
- 強制休假

ＦＢＩ提示的“出包”人員特質

- 突然買平常買不起的物品或奢侈品
- 頻繁地進行沒有合理理由的旅行（往對手所在國家或地區）
- 拒絕接受稽核
- 對稽核非常抗拒/不合作
- 經濟上有重大壓力
- 對上司或公司極度不滿

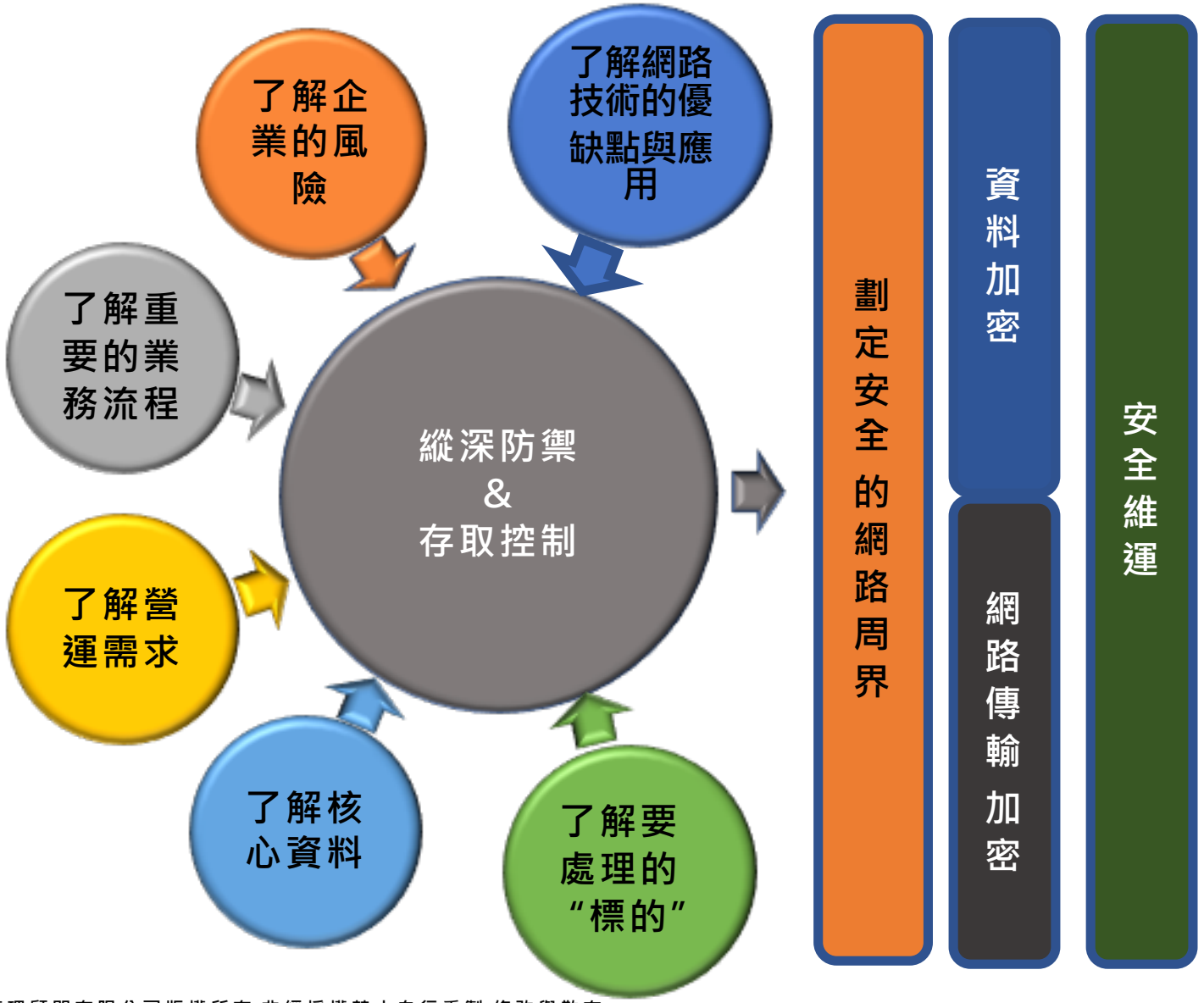
通常在離職前90天開始意圖“犯罪”

職位越高,造成損害越大

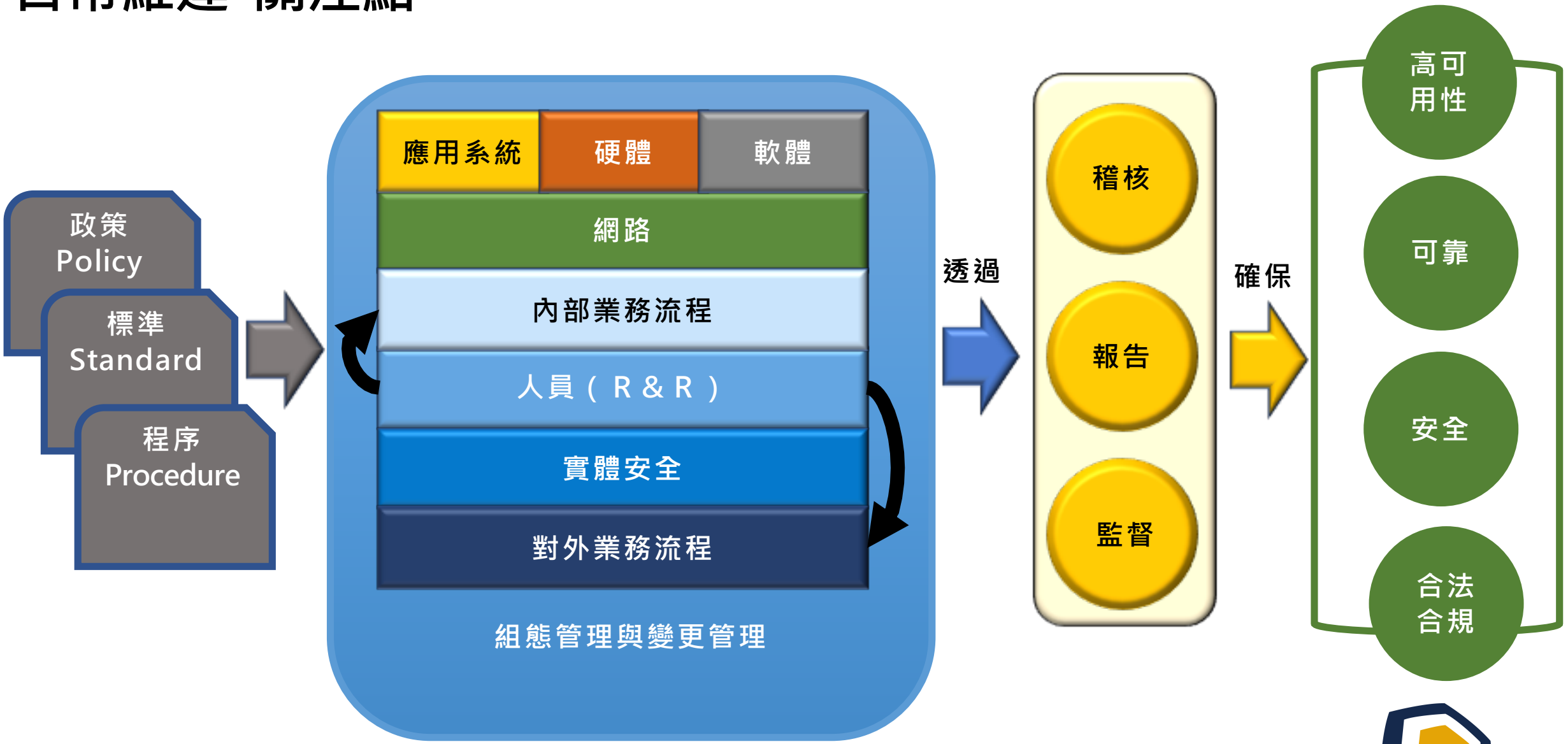
解法是？

網路安全-注意什麼？

網路安全-與其他資安領域的關聯關係是？



日常維運-關注點



展現Due care and Due diligence!

日常維運-關注點（續）

- 何謂Due care and Due diligence？
- 這個有重要嗎？？

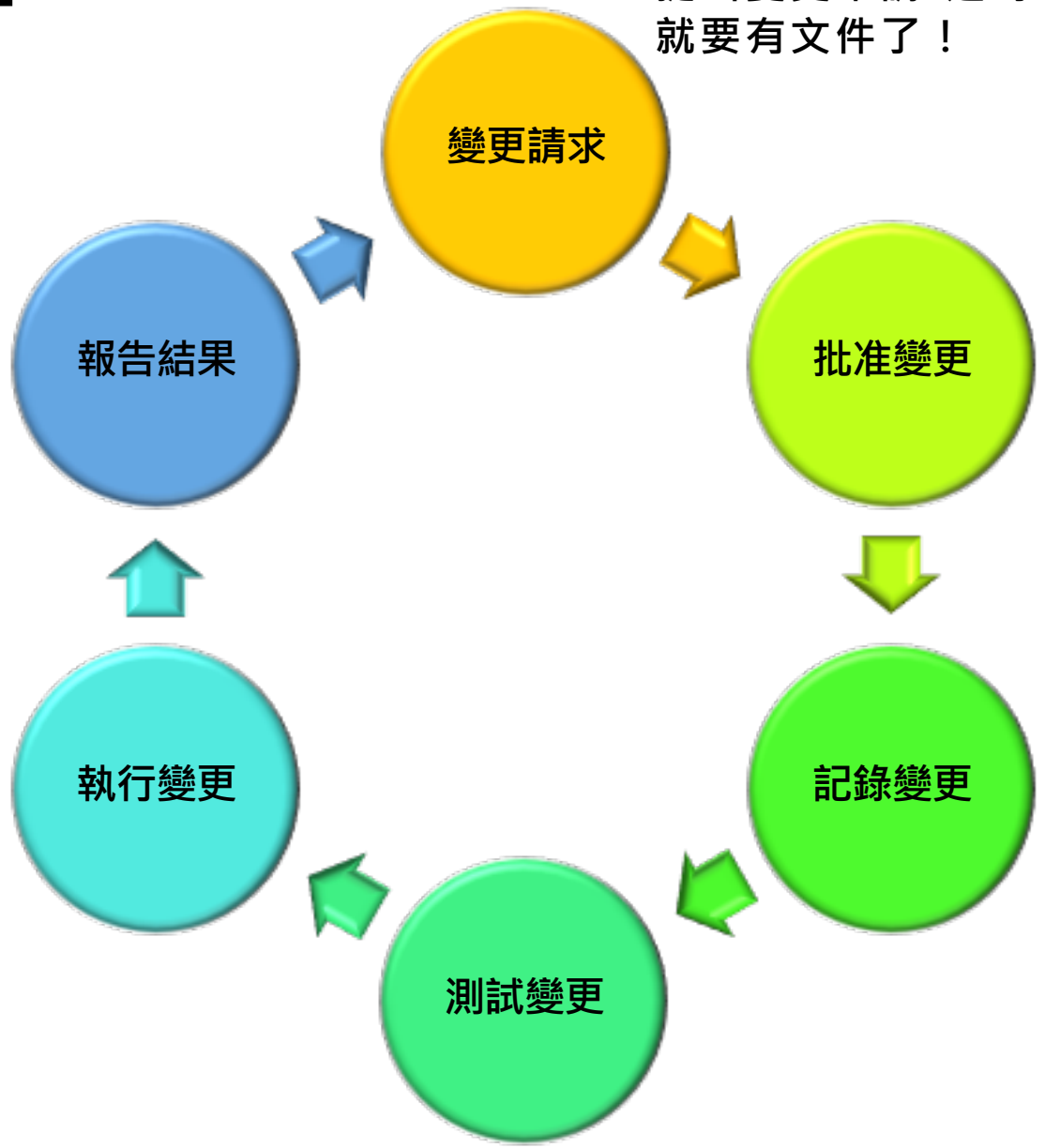
日常維運-組態管理（Configuration Management)?

- 何謂組態？
  - ✓業務流程與資訊系統的組成元件以及他們之間的關聯關係
  - ✓可能包含系統,場地,人員,權限,管理文件與設定值...等

- 為何要進行組態管理？

日常維運-變更管理

提出變更申請-這時就要有文件了！



萬一沒被批准就不管他了？

What if we fail :
- ✓ Rollback plan
- ✓ Incident management

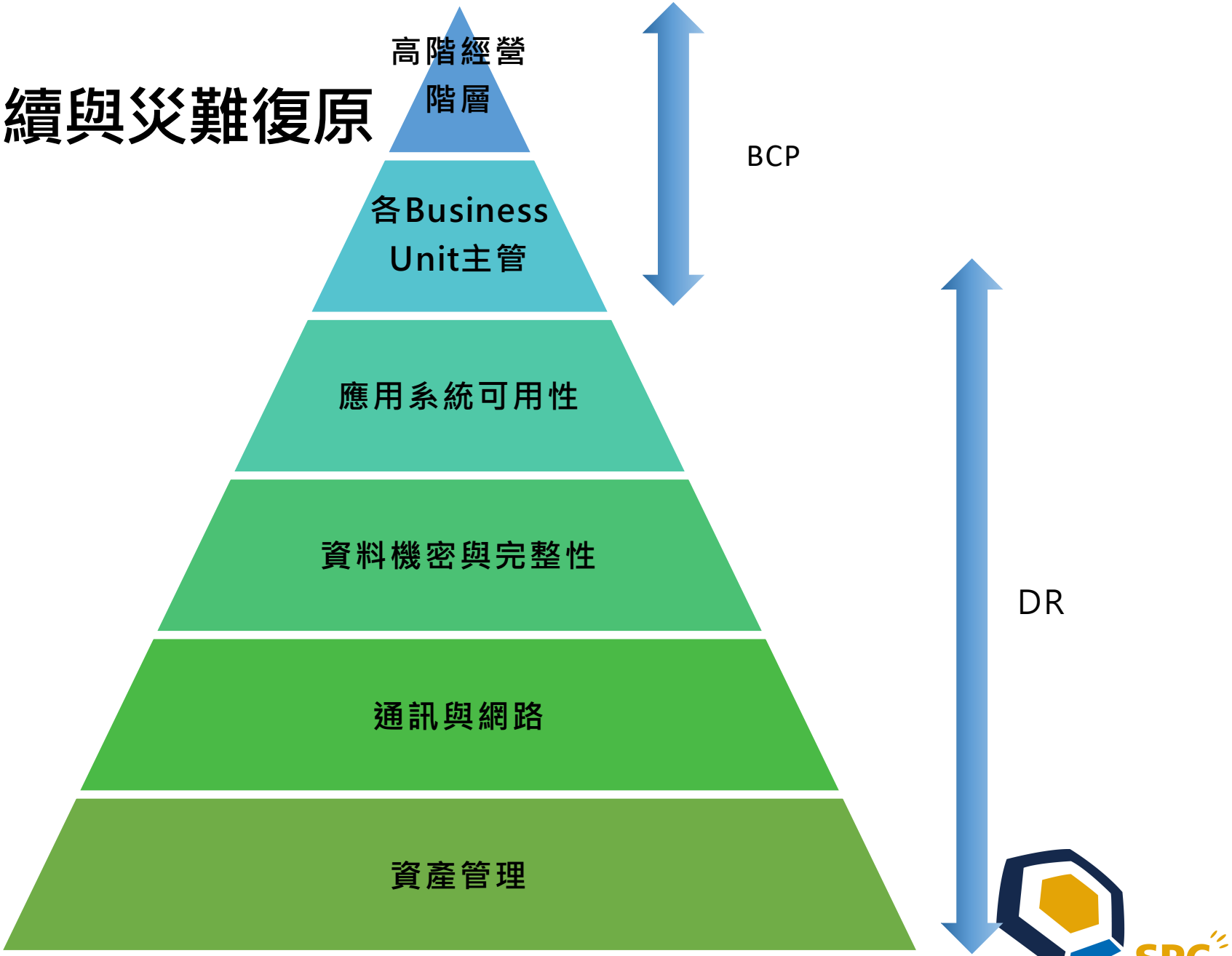
日常維運 - 修補程式管理！

- 不用駭客打你～自己就打趴自己
- 完整的程序應該是？

日常維運-資安事件管理

- 目的：儘快地回復到正常的運作狀態！
- 重要性：可以說是你最重要的管理程序之一,why?
- 重要事項：
  - 必須判定是否為真？
  - 必須要分 “等級”
  - 不同等級不同處理方法
  - 必須將過程加以記錄
  - 產出經驗學習
  - 事故處理完後～進行分析,預防再度發生

日常維運-營運持續與災難復原



日常維運-你知道自己都在忙什麼嗎？

實體安全-重點是什麼？

- Crime and disruption prevention through deterrence
  透過嚇阻的機制來達成犯罪與破壞的預防
- Reduction of damage through the use of delaying mechanisms
  透過拖延的方式來降低損害
- Crime or disruption detection
  犯罪與破壞偵測
- Incident assessment
  事故評估
- Response procedures
  建立回應機制

實體安全-續

Natural Access Control

人行道,燈柱,花圃...

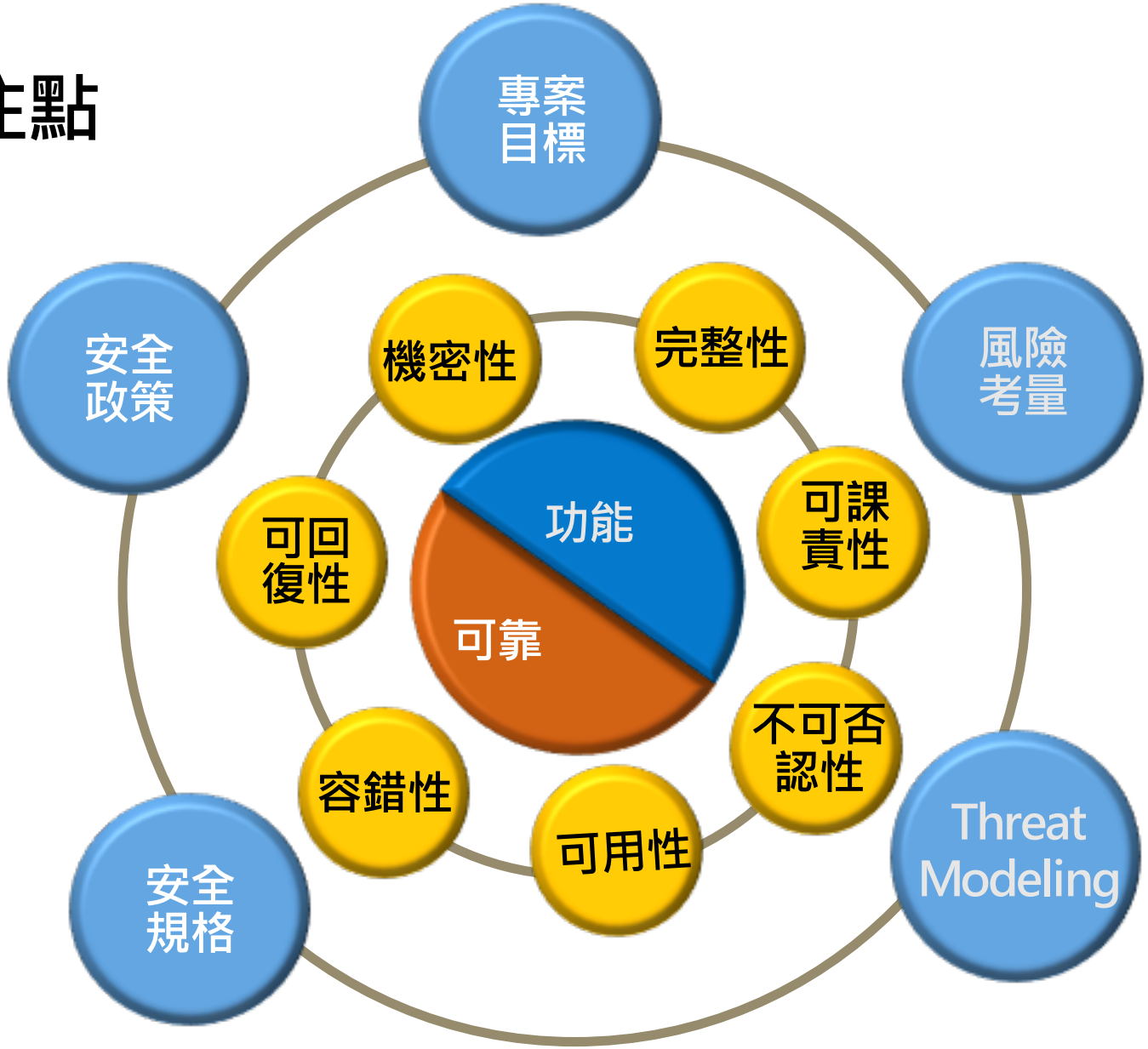
Natural Surveillance

人行道,自行車道,座椅,開放空間,矮牆矮樹

Natural Territorial Reinforcement

燈光,公司特色裝飾,圍籬...

程式與開發安全-關注點



績效評估,查核與審查-為何而做？

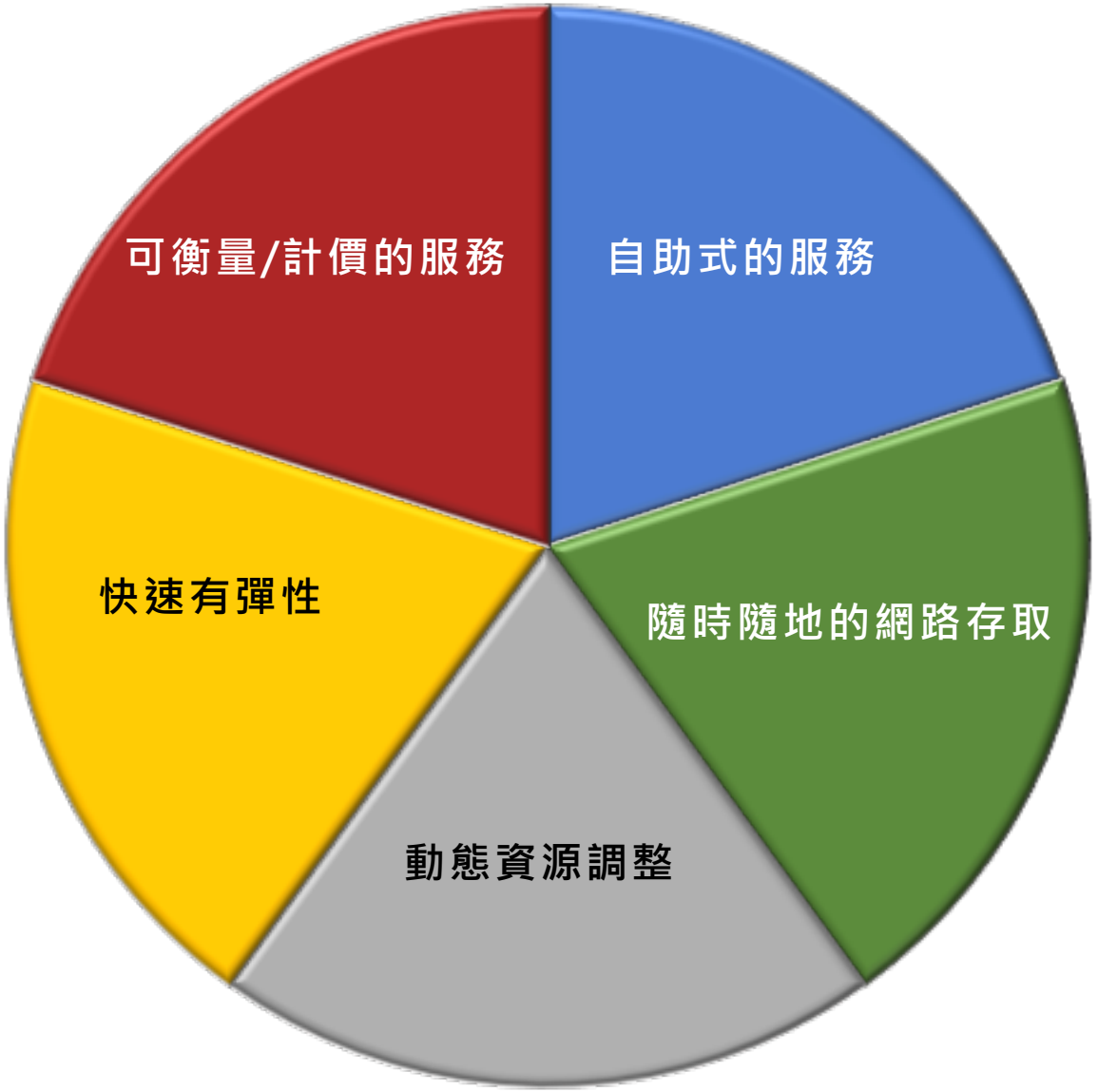
- 確認流程與控制的有效性
- 確認日常維運是否依據規範進行
- 找出問題與改善機會

績效評估-如何做？指標如何訂？

- KPI -> Key performance indicator
  - ✓衡量control/process是否有效
- KRI -> Key Risk Indicator
  - ✓Forecast 特定的風險情境是否達到threshold->事先預警
- KCI->Key control indicator (兩者搭配使用)
  - ✓SMART原則
  - ✓多不一定好
  - ✓藉此明確宣示管理階層對於控制的要求與風險容忍水準

Cloud computing的特性

- ✓On demand self-service
- ✓Broad network access
- ✓Resource pooling
- ✓Rapid Elasticity
- ✓Measured service



Cloud Service Categories