個人資料保護安全管理

個人資料隱私衝擊分析與風險評鑑

課程綱要

- 風險管理新挑戰
- 風險評鑑暨控管原則
- 風險管理作業
- 實作討論

課程綱要

- 風險管理新挑戰

資料來源：爽報

2014 年個資安全威脅回顧綜覽

課程綱要

- 風險評鑑暨控管原則

何謂風險

- 風險是具有破壞某種事物發生的可能性
- 風險管理是識別、評估風險，並將這種風險減小到一個可以接受的程度
  - 物理損壞。
  - 人為錯誤。
  - 設備故障。
  - 內部和外部攻擊。
  - 資訊誤用。
  - 資料遺失。
  - 應用程式出錯。

個資風險(外洩管道)

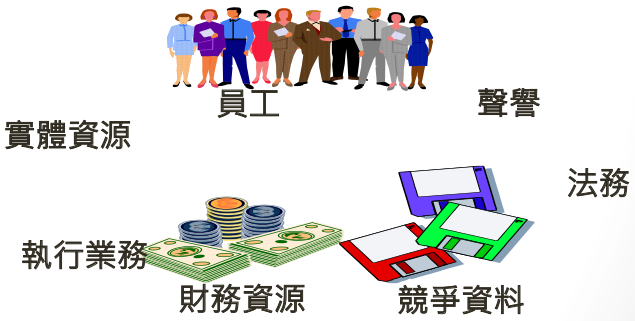
- 問卷
- 電話客服中心
- 網購
- **掛馬網站、設計不良的網站**
- **駭客入侵**
- **社群網站**
- **P2P軟體使用**
- 銀行申請單
- 會員手冊
- 信用卡
- 內部人員
- 補習班
- 電子謄本系統
- 直銷公司
- 盜版光碟
- **即時通訊軟體(IM)**
- 無個資保護認知
- **釣魚網站**
- 委外廠商

風險評鑑及風險管理

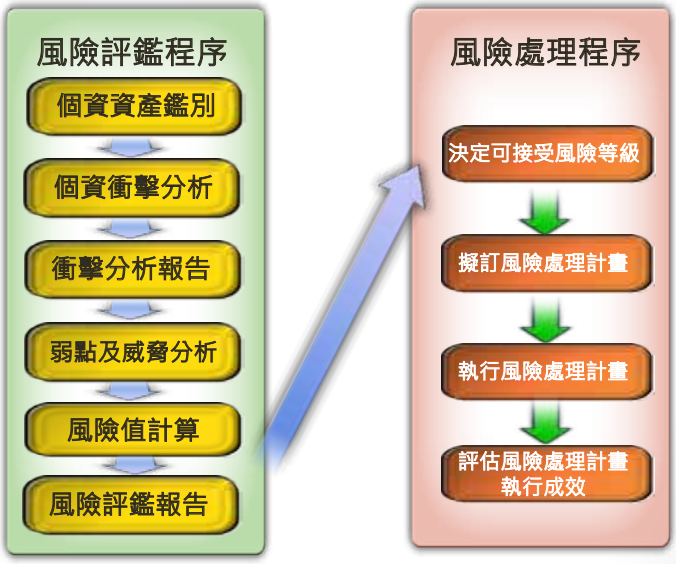
- 風險評鑑
  - 找出可能會造成組織損失的事件，並加以評估的一種方法。
- 風險管理
  - 如何降低該事件至可接受程度，並導入適當方法以維持所有風險皆在可忍受之範圍內。

風險評鑑及風險管理所帶來的效益

- **Identify assets** 識別個資資產– 我需要保護什麼?
- **Identify threats** 識別威脅–我需要採取何種對策?
- **Calculating risks**計算風險–需要多少時間、人力、或成本來保護重要資產?



風險評鑑與處理程序

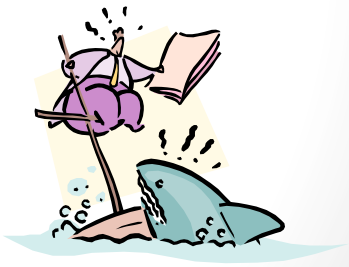


威脅分析

- 威脅為外部足以造成資產危害之狀況或事件
- 可分為意外的及蓄意的安全威脅
- 可能的安全威脅
  - **天然災害：颱風、地震、水災及停電等**
    - 地震可能威脅到個資資產的可用性及完整性。
  - **人為因素：非法存取資料、偷竊及竄改資料等**
    - 偷竊可能威脅到個資資產的可用性及機密性。

弱點分析

- 弱點存在於資產本身或內在，若被威脅利用，可能會造成危害
- 可能的安全弱點
  - 識別與認證機制的不足。
  - 存取權限授與不當。
  - 儲存媒介內之資料沒有適當刪除就丟棄或重覆使用。
  - 未保護儲存文件。
  - 人員評選程序不夠嚴謹。
  - 人員教育訓練不足。
  - 缺乏安全警覺。



有下列症狀的同仁請注意了

- 太有正義感
- 太有愛心
- 好奇寶寶
- 太容易被唬

不用打:
0800XXX000

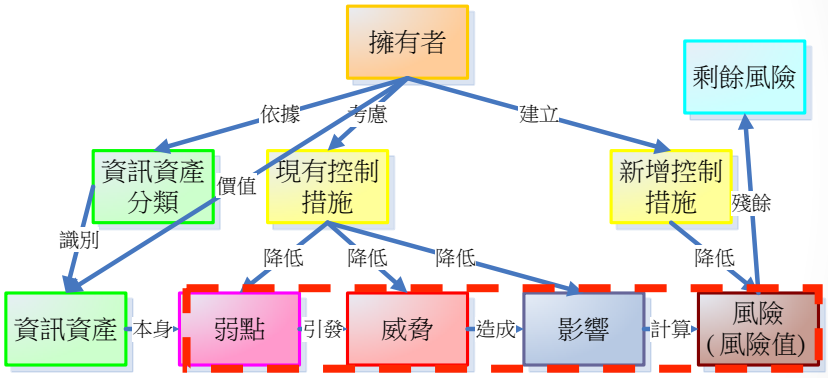
威脅、弱點、風險之間的關係

- 威脅利用弱點而對個資資產在不同的構面所造成傷害
- 風險= *f*【個資衝擊值 × 威脅與弱點在不同的構面等級】

風險管理名稱彙總

- 資產(Asset)-是一種資源(實體或邏輯)，對組織是有價值的。
- 威脅(Threat)-是一種事件，可能會對系統或組織及其資產造成傷害，威脅必須利用資產的弱點才能對資產造成傷害。
- 威脅來源(Threat Agent)-引發潛在威脅的源頭。
- 暴露(Exposure)-弱點誘發威脅的情況。
- 弱點(Vulnerability)-指單一或一系列會讓威脅有機可趁而造成資產損害的狀況。資產的脆弱點本身並不會造成傷害。
- 控制措施(Safeguards) -降低潛在風險的機制。
- 風險(Risk)-有害事件發生的可能性。
- 剩餘風險(Residual Risk)-剩餘的部份風險。

風險管理原則



風險評鑑的分析方式

定量分析

- 試圖去分配獨立的數量化價值物件(例如財務價值)作為風險評鑑的要素及潛在損失的評估。
- 當全部要素(資產價值、影響、威脅頻率、防護效果、防護成本、不確定性及可能性)是定量化處理，則表示完全定量的考慮。

定性分析

- 以情節為導向。
- 資產價值、弱點及威脅的重要等級。

風險分析實務

- 組織執行的方式
  - 由評鑑人員進行專業判斷(主觀判斷)。
  - 以會議的方式進行討論(較為客觀)。

- 顧問常用的方式：
  - 觀察-觀察實體環境、作業流程。
  - 訪談-詢問資產負責人或管理人。
  - 檢視-相關文件(事件的報告、系統稽核及安全檢查的結果)。
  - 測試及驗證-針對控制或作業的程序及結果進行正確性確認。
  - 問卷-透過問卷瞭解眾人的意向。
  - 其他-外部安全事故的經驗、事件通報、相關論壇。

  (以ISO 31000、27005為基礎)

風險處理程序

風險處理(Risk Treatment) - 選擇與實施各項控制措施，以降低風險影響程度。

可接受風險值的決定

↓

擬訂風險處理計畫

↓

執行風險處理計畫

↓

評估風險處理計畫執行成效

風險控管原則

- 在符合法令要求下，決定組織可接受之風險值
- 高於可接受風險值者，優先控管或處理

實務 - 風險接受度

- 風險接受度應該用組織可接受或不可接受來分類。
- 不可接受的風險乃經再三考量可能不被容許存在的。
- 管理者要決定是否因為不願花費額外且昂貴的保護措施來降低不可接受的風險，進而選擇接受這些風險。

可接受風險值的決定

- **資源有限**
- **決定因素**
  - 風險嚴重(衝擊)程度(例如：財務、聲譽…)
  - 風險處理急迫性。
  - 可分配的資源(例如：人力、時間、金錢)
- **決定方式**
  - 80/20法則(排序百分比法)
  - 基本統計(平均數、中位數)
  - 高階統計分析(變異與標準差、常態分配)
  - 檢視法。
- **高於可接受風險值的資產，應依據識別的弱點、威脅進行風險處理計畫的擬訂。**
- **新增控制措施，降低弱點、威脅的發生機率。**
- **將資產的風險值降低至可接受風險值以下。**

例外原則:
擬訂風險處理計畫時，仍檢視可接受風險值下的資產，是否仍有較高的潛在風險。

課程綱要

- 風險管理作業

風險管理作業

- 確認、控制及降低安全風險至可接受程度所採取的程序管理作業
  - 訂定風險可接受等級。
  - 檢視安全威脅及弱點。
  - 檢視目前使用之控制措施。
  - 加強其他控制措施。
  - 訂定相關個人隱私保護政策及作業程序。

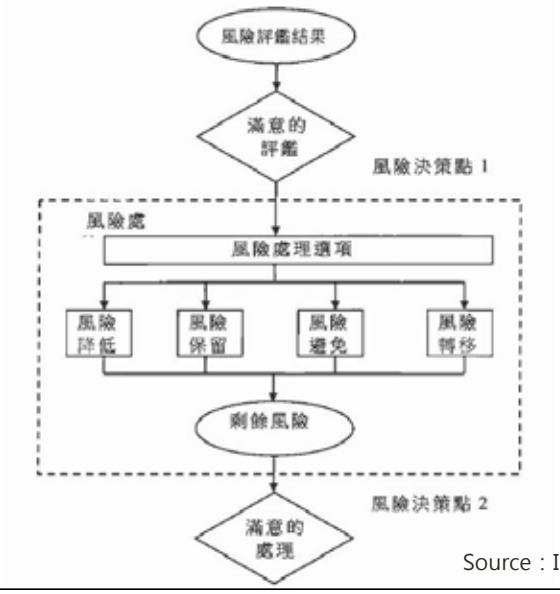
選擇控制措施

- 考慮因素
  - 需要的風險接受等級。
  - 所需費用是否合理。
  - 安全風險所造成之影響。
  - 是否容易執行。
  - 需花費多少時間。
  - 與現有環境及技術之整合是否可行。
  - 符合法令規定。
  - 相關契約規定。

控制風險策略

- 避免風險
  - 修改作業方式或採用技術以避開風險。
  - 經由政策或標準以禁止從事高風險交易或活動。
- 轉移風險
  - 轉移相關之營運風險至他者，例如：承保商、供應商。
- 保留風險
  - 符合組織的政策與風險接受準則，則知悉且客觀地接受風險。
- 降低風險
  - 參考標準選擇適當之控制措施以降低風險。
  - 藉由加強各項作業之內控以降低風險發生之機會。

風險處理活動



Source：ISO 27005

控制措施說明

- 預防性控制
  - 藉由「事前」的控制，形成一道屏障來防止特別交易的不當進行或阻止錯誤的發生。例如：承保前之風險評估、對銷貨客戶之徵信、使用經核准之供應商名單。
- 偵查性控制
  - 利用某些程序來偵測已發生之錯誤或不當交易。例如：編製銀行調節表、存貨盤點、與銷貨客戶之定期對帳。
- 矯正性控制
  - 用來矯正偵查性控制所發現之問題或矯正交易之控制。例如：透過電腦對採購單之檢核可以偵測到未經核准之供應商號碼，進而追蹤其原因及時修正交易資料或防止向不適當供應商之採購。
- 補償性控制
  - 用來補償其他控制之不足，使得某些控制弱點不成為問題。例如：未有足夠之人力執行職能分工時，可透過由客戶或管理階層親自監督來彌補此一控制弱點。

控制措施的選擇考量

- 時效性
  - 控制執行時間及有效期限為何。
- 人力
  - 每年需要多少工時來監控和維護。
  - 負責執行、監控及維護控制的人員需要接受多少訓練。
  - 必須容易執行，了解對使用者造成多少程度不便。
- 成本
  - 是否有預算執行這項控制措施。
  - 控制的費用相對於資產價值而言合理嗎？ (成本)
  - 控制成本<資產價值<威脅損失。
- 法規或合約要求

風險處理

- 依據資產風險評鑑的結果，對於超出組織風險值可接受程度之風險，進行處理。
- 目的：降低風險發生機率及風險發生時產生之損害。
- 工具：風險處理計畫。

風險處理建議及規劃

- 系統使用之資料或傳輸加解密技術存在弱點，遭利用造成資訊不當揭露
- 預防性措施：
  - 制定委外服務安全管理程序，規範委外服務的安全管理方式。
  - 禁止服務提供者及其人員接觸任何與加解密有關的系統及傳輸之檔案。
  - 提出提升加解密安全性之需求。
  - 對委外廠商實施資訊安全宣導。
  - 制定委外服務廠商安全須知，並要求簽署。
  - 修定安全事件處理程序增加委外服務人員之安全事件處理準則，考量以下事項：
    - 證據保全
    - 合約及法律責任
    - 法務的參與

風險處理後

- 建立一套量測系統(例如：KPI指標)，協助控制目標的達成。
- 執行內部稽核，確保控制措施的有效性。
- 當有下列情況時，執行風險評鑑作業。
  - 每年定期執行。
  - 營運組織變更。
  - 作業流程改變。
  - 資產新增或變更。
  - 發生重大個資安全事件。

課程綱要

- 實作討論

Q&A 問題與討論