國立中興大學

個資侵害事故之緊急應變教育訓練

2013.4

大綱

個資侵害事故回顧與討論

危機處理概念

緊急應變管理思維與責任

個案討論

個資侵害事故回顧與討論

2013年個資管理新挑戰

來源	過去情形	現階段挑戰
惡意駭客	資訊系統破壞或入侵知識僅由少數駭客掌握，相關技術具有進入門檻	攻擊工具垂手可得，人人都可是駭客，24小時進行主動、無時差攻擊
民眾	僅注重服務的效率與品質	開始具備個人資料保護與資訊安全意識，並重視個人資料安全
媒體	未關注個資保護議題	媒體爆料文化盛行，監督企業或政府機關的資訊保護作為
法律規範	電腦處理個人資料保護法(84年公布)	「個資法」2012.10 公佈施行

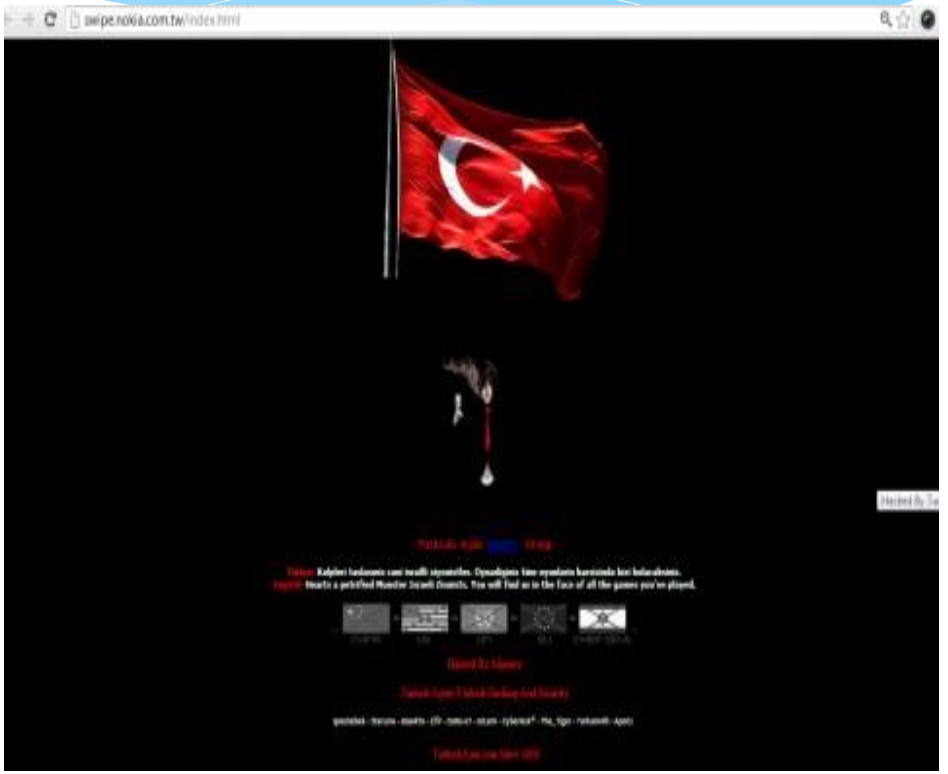
個資外洩管道

- 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**

台灣Nokia行銷網站被駭，150萬個資可能外洩

* Nokia委外經營的5個台灣行銷網站遭駭客入侵，目前駭客已公佈17萬筆資料，由於缺乏證據證實駭客取得的資料數量，Nokia估計約150萬筆資料可能被竊。
* Nokia發生重大資安事件，台灣委外經營的5個行銷活動網站被駭客入侵，約150萬筆消費者個資可能被竊，Nokia已關閉這些網站，同時通知用戶防範。
* 台灣Nokia對外發出聲明，表示該公司委託網路行銷公司Agenda經營的5個台灣行銷活動網站遭駭客入侵，駭客已公佈17萬筆資料，經過調查後，Nokia可能有150萬筆先前在台灣舉辦行銷活動的消費者個人資料外洩，Nokia已採取因應措施，關閉網站、修復伺服器漏洞，移除資料庫，同時以電子郵件、簡訊通知客戶。



資料來源：isecurity

Evernote遭駭，要求近五千萬用戶改密碼

* 如果你是雲端筆記服務Evernote的愛用者，可能要注意一下這則新聞了。Evernote近五千萬名用戶發出修改密碼的通知函，理由是遭到駭客攻擊，導致大量用戶的帳號、電子郵件地址和密碼疑似外露。這也是繼Twitter和Facebook等社交網站遭遇駭客攻擊後，再一次有知名網站遇駭。
* Evernote透過官方部落格表示，用戶在Evernote中所記錄的各項內容並未被擷取，但為了小心起見，還是建議用戶儘快設定新密碼，以保障資訊安全。
* Evernote指出，該公司最初於2月28日發現了非比尋常的可能性惡意活動。有些人用了不正當手法獲取了Evernote的帳號名稱、電子郵件和密碼。隨後，Evernote立即對該公司各平台的應用軟體進行升級，並協助所有用戶重新設定一組新密碼。
* Evernote執行長菲爾.李賓（Phil Libin）相當重視這起事件，他表示：「我們沒有儲存任何有關用戶的支付訊息，因此不會有與支付相關的資訊外露狀況。」

資料來源：isecurity

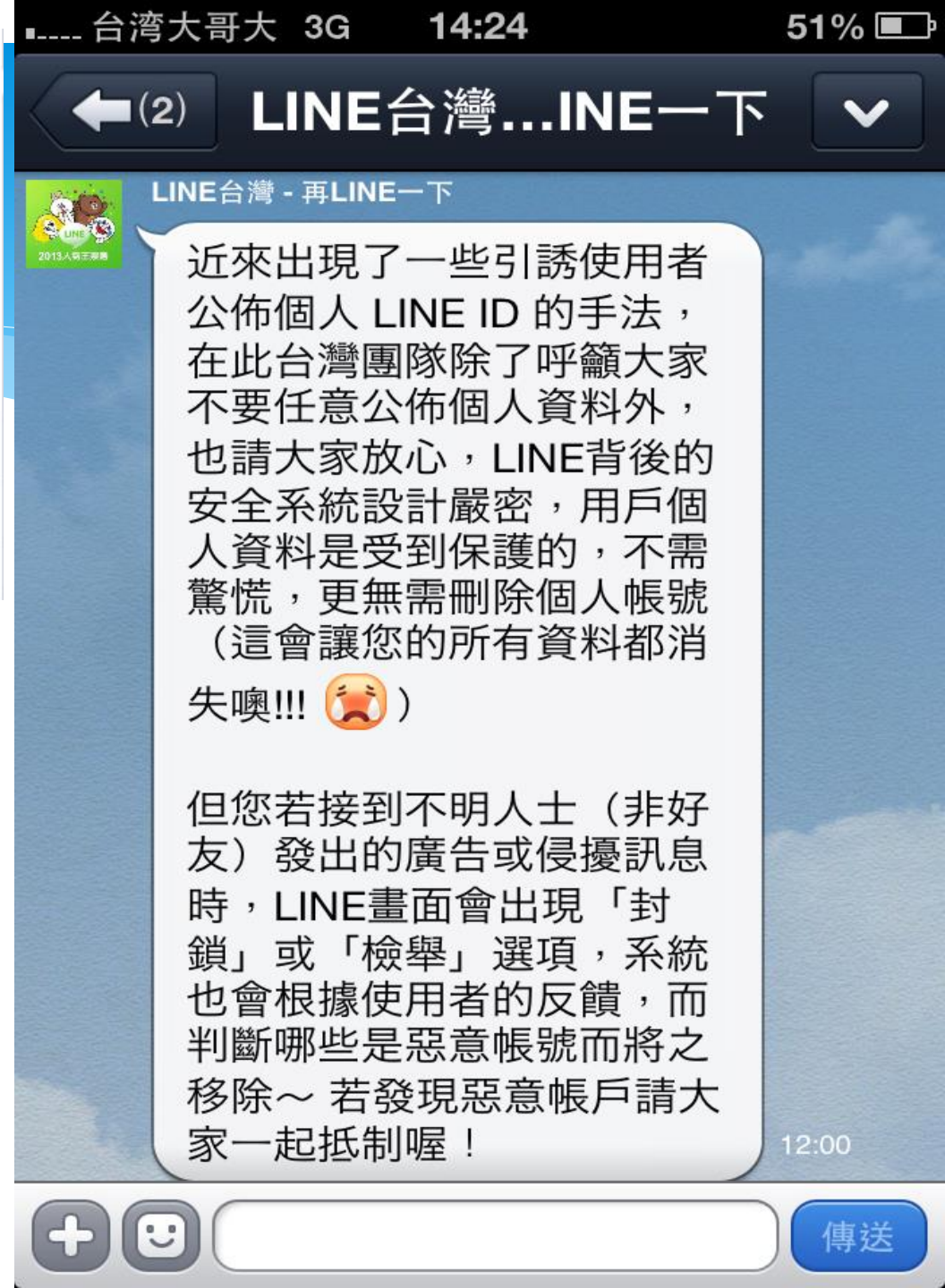
LINE Taiwan- 再Line一下
2小時前來自手機

[官方聲明] 最近在網上有一些聲稱留下個人LINE ID就免費贈送付費貼圖的網站，建議用戶不要輕易相信，LINE官方從未跟任何一家公司或團體在該方面進行合作，並請留意勿洩露個人訊息。
祝各位朋友 假期愉快~

讚 · 留言 · 分享 16,614

16,651 個人都說讚。

顯示先前的留言 771則中的2則



危機處理概念

事故定義

* 從設備故障、人員差錯、人爲事件或自然事件之類的單一事件到各種事件的複雜組合均屬於事故範疇內的案例。

事故的類型(1)

內部

* 員工惡意行為
  * 遭人為惡意破壞毀損、作業不慎等
* 設備故障
  * 能直接或間接影響的各個設備的故障
* 員工差錯
  * 錯誤的或不良的維護、錯誤設定和操縱員的其他錯誤行為
* 其他內部事件
  * 內部原因引起的

事故的類型(2)

外部

* 自然或外部引起某一安全重要系統、元件和建築物故障的可能性，通過設計和建造中所採取的措施可降低到可接受的程度
  * 病毒感染事件
  * 駭客攻擊（或非法入侵）
* 自然
  * 天然災害：颱風、水災、地震
  * 重大突發：火災、爆炸、核子事故

事故處理

依據「國家資通安全會報技術服務中心緊急應變作業方式」，處理分三色警戒狀況

* 「紅色警戒」：於機關單位通報「A」等級事件(將影響政府服務、公共安全、社會秩序、人民生命財產之緊急狀況)
* 「黃色警戒」：於平時如元旦、五二O與十月慶典等重點期間，國家資通安全可能遭受威脅
* 「藍色警戒」：平時經收集情報研判電腦網路駭客可能有入侵舉動之異常狀況，以及電腦病毒可能蔓延全國之重大疫情

演變為危機的特徵

* 意外
* 訊息混亂
* 事件影響逐漸升高
* 失去控制
* 來自內部/外部嚴重關切
* 開始產生精神折磨
* 恐慌
* 需要公開化解疑慮

危機處理方式

* 制訂處理機制，事先找出潛在的問題，避免事件擴大成危機
* 在事件發生之初，投入適當的資源，以有效管理
* 儘量控制或減少對單位的風險
* 適當的處理各種抱怨

處理考慮的優先順序

* 保護客戶的權益
* 組織、單位的形象
* 永續營運

第一要務

* 第一優先 — 『人員生命安全』
* 在任何情形下絕對不要讓員工冒風險，當重大風險發生立即疏散員工

對外說明原則

* 只有授權的發言人，才可對外說明
* 強調首要目標為保護客戶權益
* 說明時必須快速與所有聽眾有目光接觸
* 說明時必須平衡本單位事件處理方式與可能的法律問題
* 說實話，避免回答假設性的問題或缺乏事實根據的話
* 報告主管機關（不要透過媒體）
* 儘快提供最新的資訊，以滿足與引導媒體
* 由最高主管作對外危機說明

說明方式

誰該說明

* 只有授權的發言人，才可對外說明

說明什麼

* 只能說明事先經過核准的事實

哪些不該說

* 未經核准的資訊不能說
* 不要傳播謠言或推測的話
* 不要指責或歪曲事實

危機管理

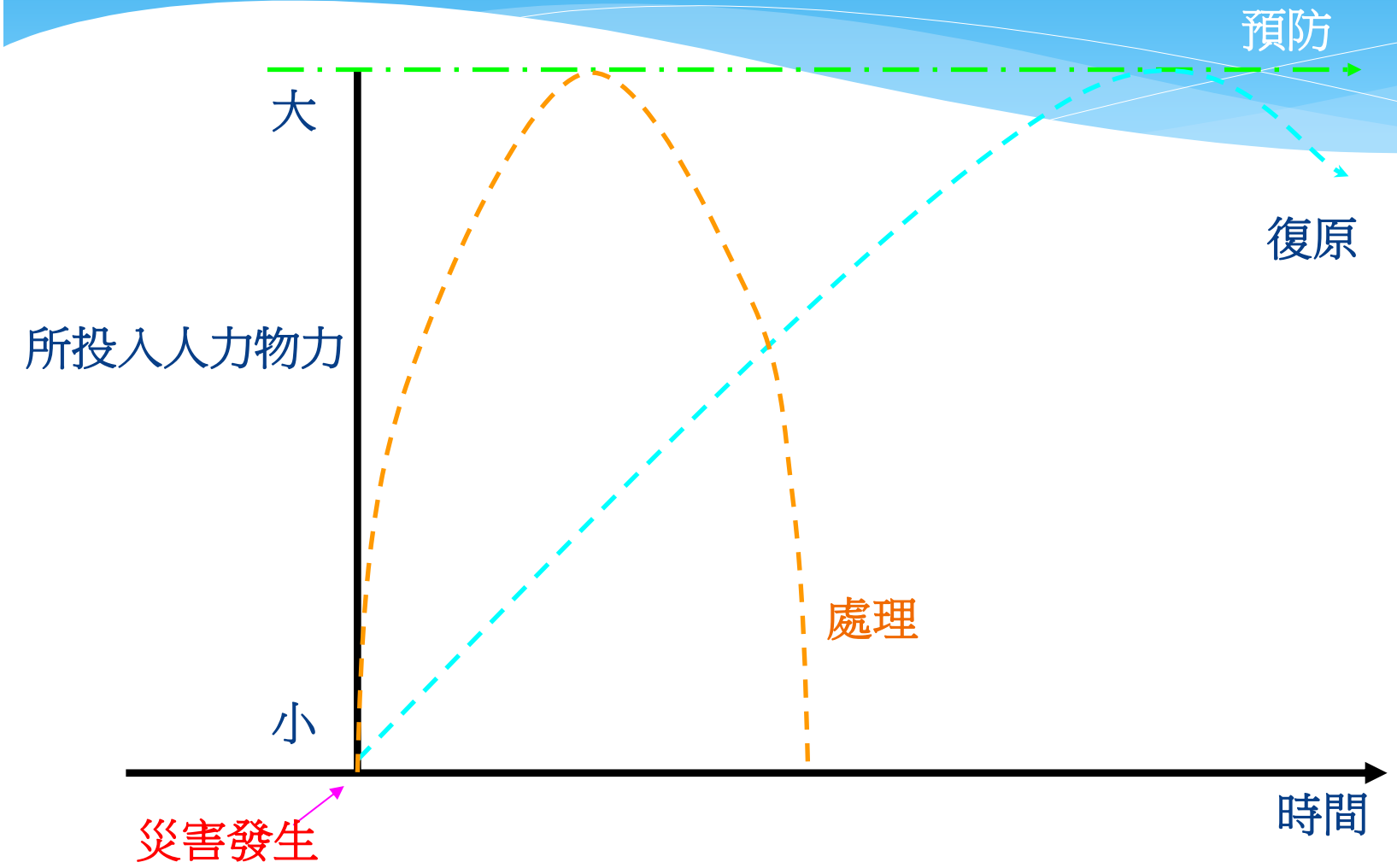
危機預防階段
* 危機偵測
* 危機防範
* 研擬各種應變計畫

危機處理階段
* 判定危機本質
* 設立危機處理目標
* 執行危機處理計畫

復原階段
* 擬訂重建復原計畫
* 召開檢討會議
* 回到危機預防階段

摘自：中國時報-前國安局秘書長

危機處理與時間關係



緊急應變管理思維與責任

Case Study(1)

情境討論

目的

確保組織重要業務具有充分緊急替代能力，當發生災害時減少損失，將衝擊降至最低，確保

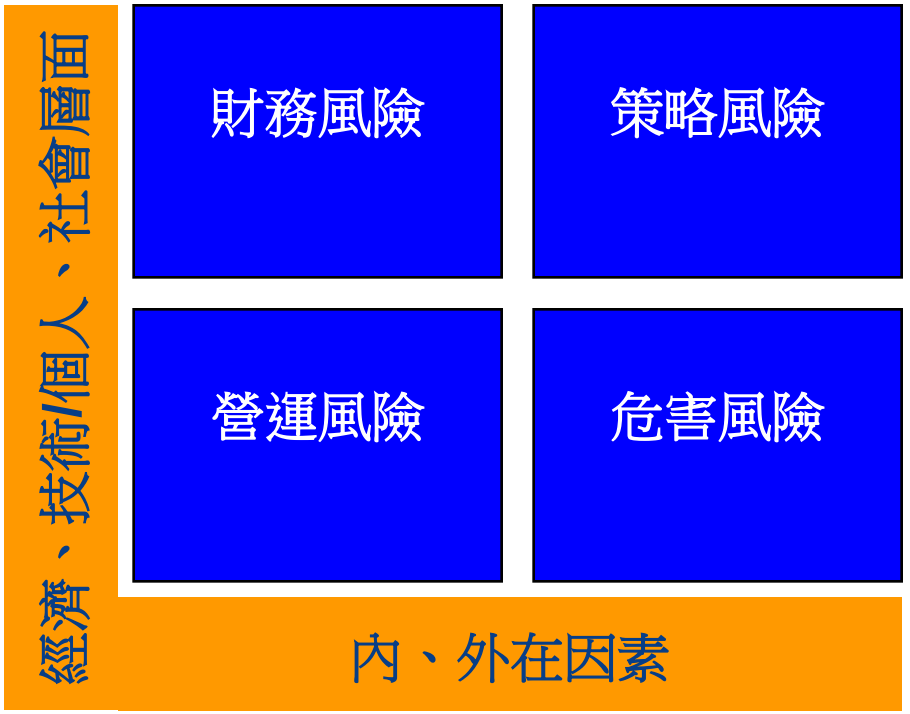
* 組織資產
* 組織達成目標的能力
* 組織運作能力
* 組織商譽與形象
* 客戶基礎及市場佔有率
* 組織獲利能力

影響的種類

* 財務
* 客戶或供應商
* 公共關係/商譽
* 法律
* 法規/合約要求
* 環境
* 營運
* 人員
* 主管機關

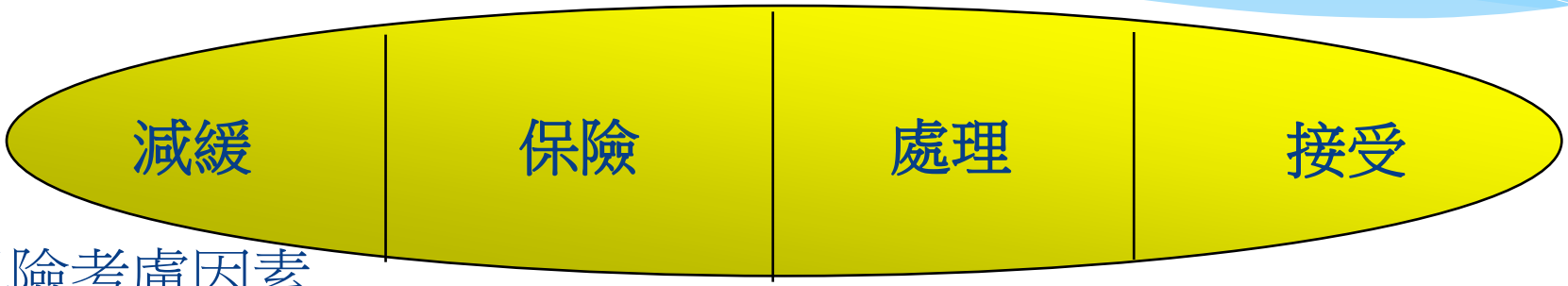
風險定義與分類

* 風險環境調查
* 營運風險辨識
* 風險影響分類
* 風險頻率分類
* 風險分析
* 風險評估
* 營運風險分析
* 營運風險改善彙整



風險管理方式

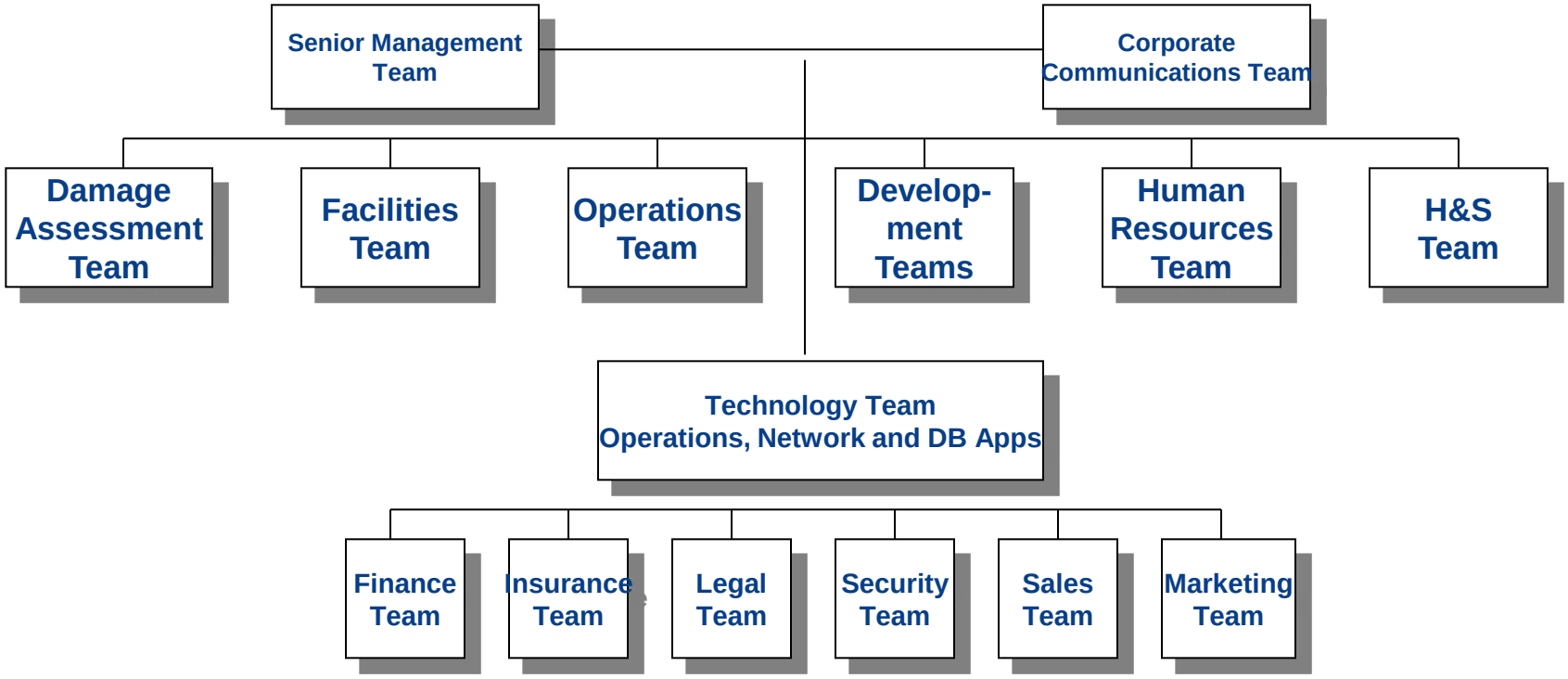
面對風險有四種處理的方式



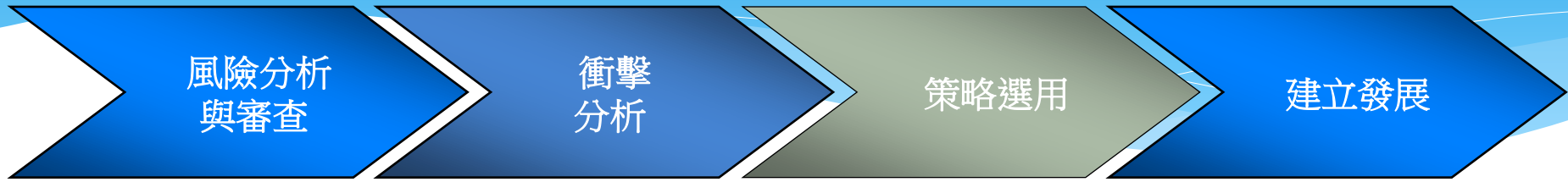
風險考慮因素

遵循性	財務	營運	策略	技術
合約	*損失或延緩營收*	*人員*	*市佔率*	*網路犯罪*
法規	*機會*	*產品*	*夥伴關係*	*電子商務*
服務水準	*股東權益*	*供應鏈*	*商譽*	*基礎設施損毀*

緊急應變管理小組(建議)


Senior Management Team
Corporate Communications Team
Damage Assessment Team
Facilities Team
Operations Team
Develop-ment Teams
Human Resources Team
H&S Team
Technology Team Operations, Network and DB Apps
Finance Team
Insurance Team
Legal Team
Security Team
Sales Team
Marketing Team

危機管理小組(範例)



Coordination Team

Facilities Team | Operations Team | H&S Team

Develop-ment Teams | Human Resources Team | Marketing Team | Sales Team

Finance Team | Insurance Team | Legal Team | Security Team

TOP Management

Finance Team | Sales Team | Marketing Team

Facilities Team | Operations Team | H&S Team

Develop-ment Teams | Human Resources Team | Sales Team

Finance Team | Insurance Team | Legal Team | Security Team

開發應變計畫

「危機管理計畫」(Crisis Management Plan, CMP)

* CMP 是指用於事故發生時被清楚定義之行動計畫，通常其涵蓋了實施事故管理流程所需的主要人員、資源、服務及行動；這個部份包括行動清單、媒體回應流程、以及股東管理流程。

管理計畫的定義與理論

當主要業務發生中斷情形，組織並須立即採取措施減緩損失。危機管理計畫 Crisis Management Plan (CMP) 將協助組織處理、回應與復原主要業務

* CMP應包含:
  * 危機管理小組架構、角色與職責
  * 管理階層、員工、媒體等溝通計畫
  * 危機服務;角色與職責
  * 危機因應程序與檢查表,
  * 危機處理活動程序與檢查表;
  * 復原程序與檢查表
  * 指揮中心架構

應變計畫(個案範例)

個資外洩應變計畫

演練類型與方法

複雜性	演練類型	程序	頻率
低	書面審查	計畫內容審查	至少年度
中	局部計畫演練	挑戰內容	年度
中	模擬	運用情境驗證	年度或半年
中	關鍵活動演練	啟動可控制之情境，不為及營運作業	年度或低於
高	完整演練	大範圍演練	年度或低於

個案討論

Case Study(2)

危機總動員

Q&A 問題與討論