個資侵害事故之緊急應變教育訓練

2012.10.11
16

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

2012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」計畫於2012.10 上路

案例：內部員工竊取個資

匯豐銀行員工竊取2萬4000名客戶資料

案例說明：

匯豐控股公司(HSBC)，旗下瑞士私人銀行分行的帳戶資料遭離職員工竊取，可能影響多達2.4萬名客戶。該竊案可能重創滙豐的商譽，且可能導致許多客戶成為母國查緝逃漏稅的對象。匯豐表示其離職員工法契亞尼，竊取這些來自全球各地客戶資料，包括1.5萬名開設瑞士帳戶的客戶，和已關閉的9,000個帳戶。該竊案還可能引發國際糾紛。瑞士政府已告訴法國，不會協助追查涉及的客戶逃漏稅，因為這些資料並非合法取得。但瑞士與德法兩國政府曾因類似事件起糾紛，德國財長說已準備付錢購買瑞士某家銀行遭竊的資料，裡面可能有逃漏稅的資訊。滙豐指出法契亞尼在公司資訊科技部門任職多年，深受信賴，在一次資料遷移的過程中接觸到這些機密資料。滙豐聲稱，法契亞尼把資料轉存到個人裝置上，然後設法對黎巴嫩數家銀行兜售這些資料。先前也有報導指出，他曾企圖把這些資料以250萬歐元（339萬美元）賣給德國；稅務調查界人士估計，德國可能從這些資料追回1億歐元稅金。

資安事故原因分析

1.未控管機敏資料傳輸
2.未控管員工個人資訊設備之使用

預防措施

1.制訂資料存取與資訊設備之管控程序
2.對機敏資料進行加密與權責區分

新聞來源：經濟日報

案例：麥當勞委外廠商遭入侵 客戶資料外洩

* 根據外電報導，連鎖速食業者麥當勞也傳出客戶資料外洩。美國麥當勞總部透過電子郵件及其官方網站發布訊息，指出其行銷服務合作夥伴Arc Worldwide所委託管理麥當勞客戶資料的電子郵件公司，系統遭到入侵，包括姓名、電話號碼、電子郵件、地址等客戶資料很可能被未經授權的第三方存取。
* 一直以來，麥當勞委託行銷公司Arc Worldwide——知名廣告公司李奧貝納（Leo Burnett）旗下互動行銷子公司進行宣傳、行銷活動，包括電子郵件促銷訊息的開發設計，而Arc則再委由另一家電子郵件發送公司負責管理麥當勞客戶資料。而這次遭到駭客攻擊的正是此電子郵件公司的系統。
* 在專業分工時代，許多企業會將非核心業務委外處理，然而一旦委外項目與個人資料有關時，例如此例中的電子郵件名單，企業就須特別注意。根據新版個人資料保護法第四條規定：『受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。』因此，業者必須特別注意委外廠商對於客戶資料的處理過程及系統 是否安全。由於委外廠商對於個人資料管理所應付的責任視同委託機關，因此業者必須特別留意在相關業務委外的合約上是否註明清楚的權利、義務。
* 個資法第四條對於委外機構有清楚的規範，法務部曾表示，將來若有個人資料外洩，業者必須直接面對消費者負起所有責任，而後續與委外廠商之間的對價賠償關係則是業者與委外廠商的事，與民眾無關。因此，企業在進行委外業務時，必須特別注意。

資安事故原因分析

未有資料保護及相關法律責任之警覺，導致違法情事

預防措施

1. 提高個資保護認知
2. 委外相關安全控管

新聞來源：資安人

案例：個人隱私於網站外洩

勞工局甄試竟洩漏個資 北市：處理有疏失

案例說明：

台北市勞工局辦理「數位就業服務營運中心試辦計畫」，甄試業務促進員，不過甄試結束後竟然發現北市勞工局將甄試人員的身份證字號、電話、學歷、地址等個人資料，全被登錄上網，儘管勞工局已經立即將網頁移除，不過現在於Google網站上，依然可以找到暫存檔，台北市勞工局長表示，勞工局在處理上的確有疏失，已經發文給Google，希望將資料移除。

資安事故原因分析

資料管理人員未考量個人資料之敏感性，即公告於公開網站，遭搜尋引擎列入查詢

預防措施

1.提高人員個資保護認知
2.必要公布之敏感資料應加密保護，並利用電子憑證等認證方式限制存取權限
3.審視機關個人資料保護之規範，制訂控制措施

新聞來源：中廣新聞

案例：販售民眾隱私

盜取名人個料轉售 北檢起訴熊x芬等8人

案例說明：

女子熊x芬為首的集團涉嫌以每筆1500元至28000元代價，透過不肖警察取得特定人的個人資料後，再轉售給徵信業者作為跟監、討債及捉姦使用。台北地檢署依涉貪污、洩密、違反電腦處理個人資料保護法等罪嫌起訴熊女等8人。
檢調發動搜索時，還傳出包括藝人楊x緯、隋x、王x凌，及一些政商名流個資都曾遭轉售，其受託取得的資料五花八門，包括車籍資料、電話號碼、前科表、不動產資料、婚姻狀況、入出境資料、通聯紀錄，及戶籍資料等。有徵信社要求查詢特定人的健保資料，熊女也能透過友人想辦法由健保局的公務電腦取得。

資安事故原因分析

人員未有個人資料保護及相關法律責任之警覺，利用公務系統存取並販售個人資料導致違法情事

預防措施

1.提高人員個資保護認知
2.建立權限區隔機制，並留存紀錄及進行適當稽核

新聞來源：自由時報

案例：水利署外洩個資

水利署外洩個資 跨機關資料調閱問題大

* 民眾向立委及市議員爆料指出，經濟部水利署網站傳出將民眾個人資料外洩事件。任何人只要下載「台北市XXX水災保全計畫」，就可看到台北市士林、北投、文山區部份易發生水災地區的住戶個人資料，包括姓名、地址、出生年月日、身分證字號、聯絡電話等個資，約400多筆。由於事涉地方(台北市水利處)及中央(經濟部水利署)，立委要求主管機關徹查失職原因。

資安事故原因分析

未有資料保護及相關法律責任之警覺，導致違法情事

預防措施

跨機關資料調閱應明定資料使用目的及保管權責

新聞來源：資安人

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

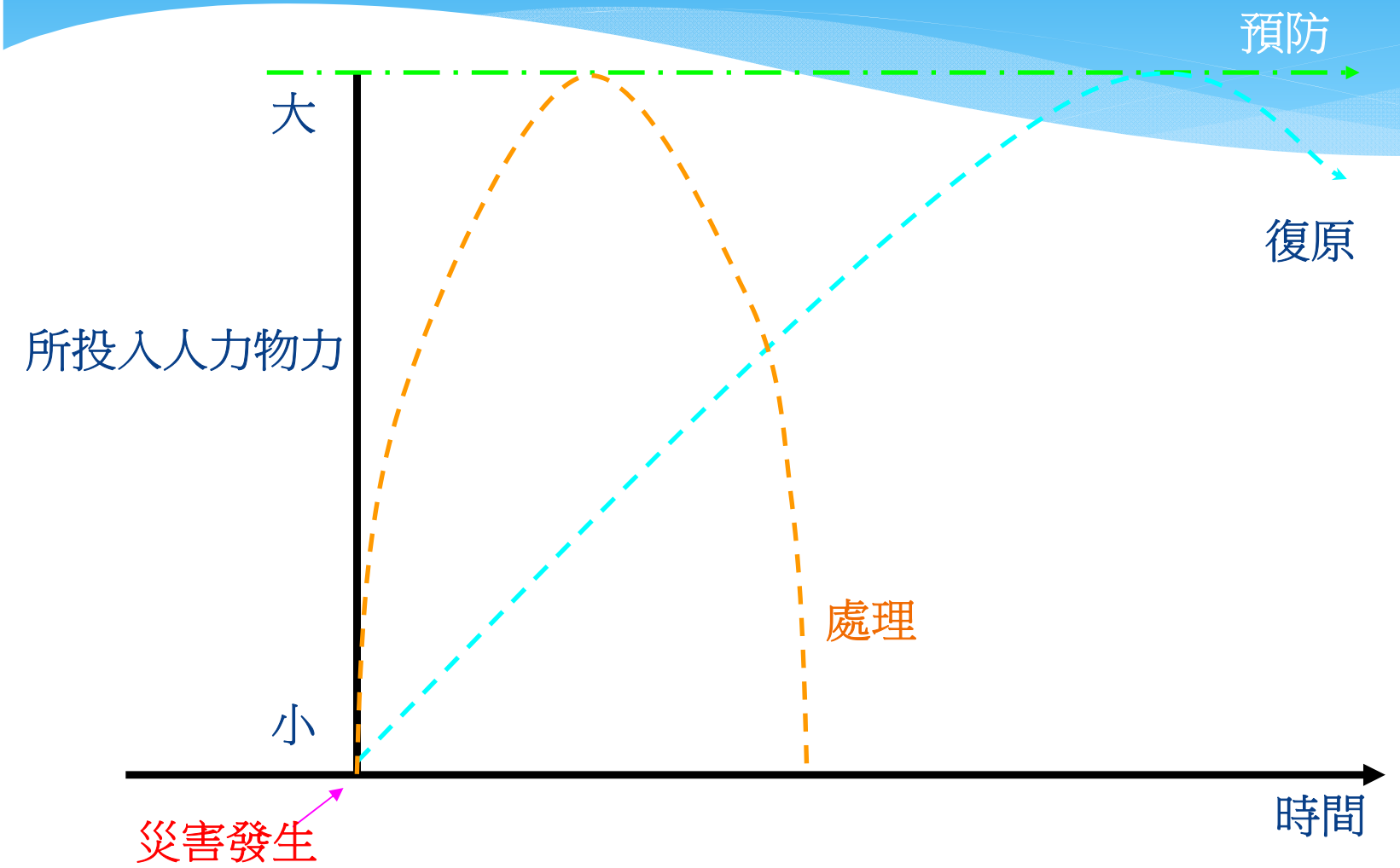
危機預防階段
* 危機偵測
* 危機防範
* 研擬各種應變計畫

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

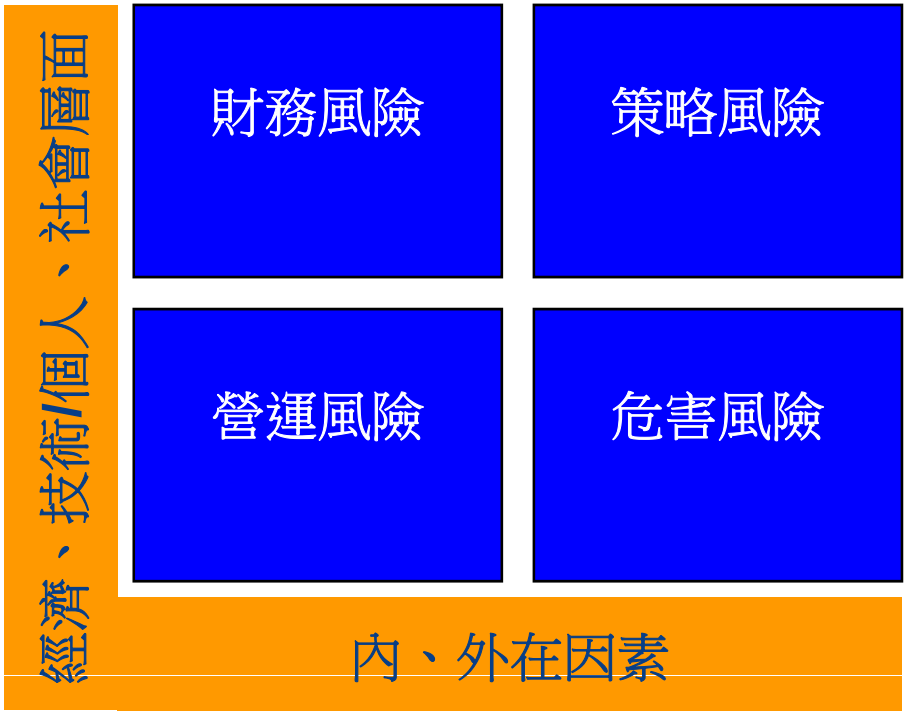
* 組織資產
* 組織達成目標的能力
* 組織運作能力
* 組織商譽與形象
* 客戶基礎及市場佔有率
* 組織獲利能力

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

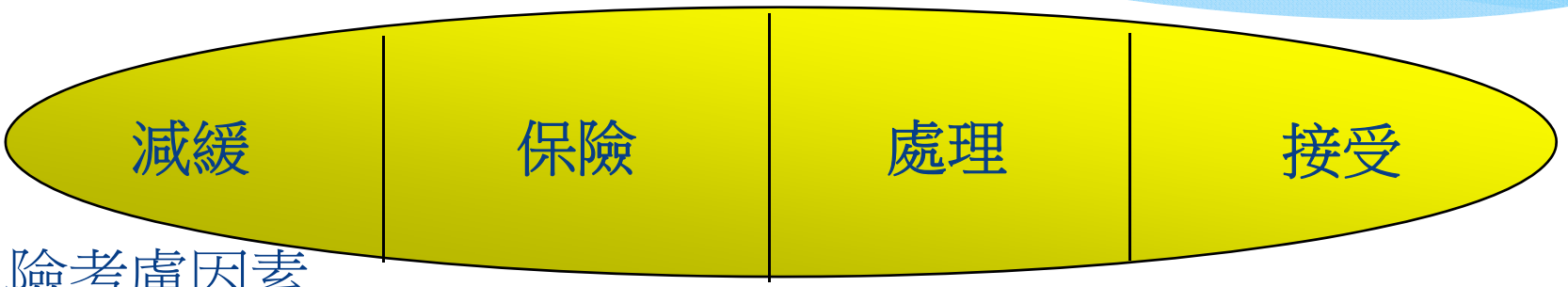
風險定義與分類

* 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

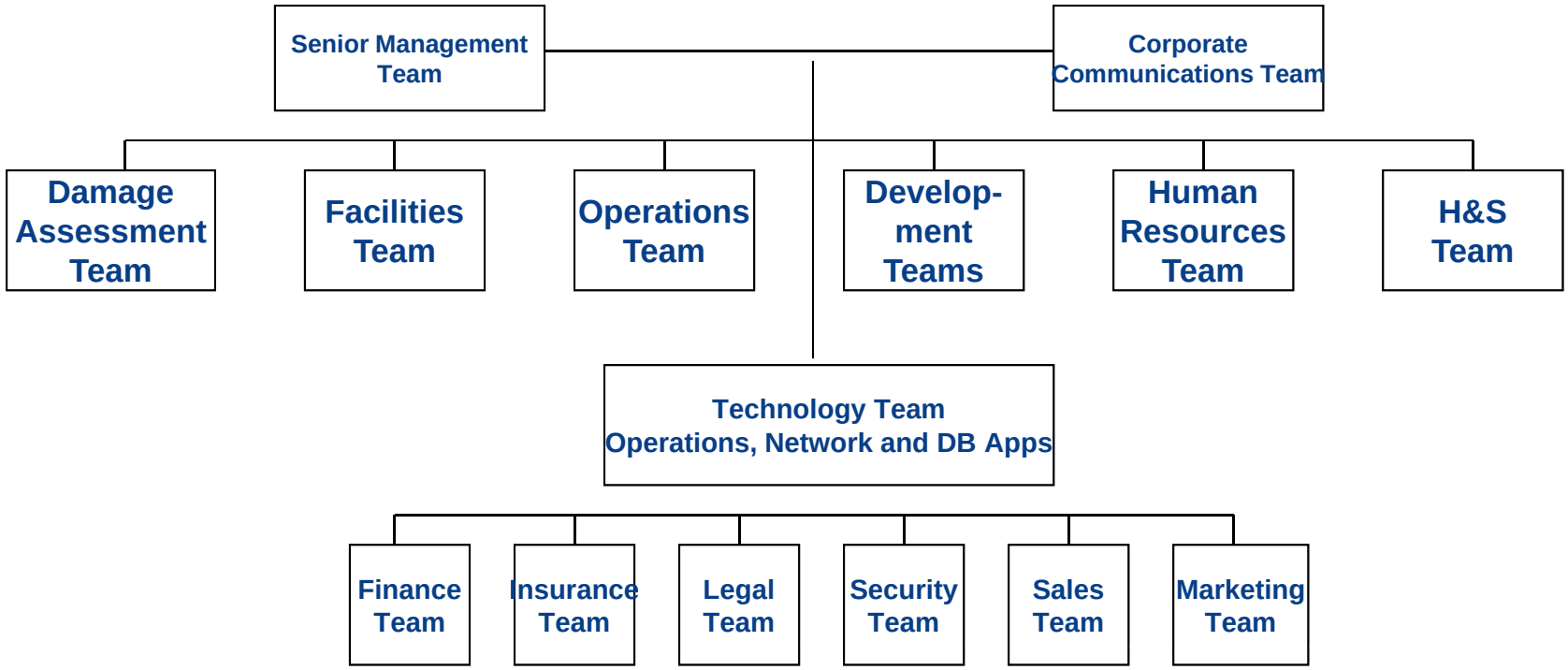
面對風險有四種處理的方式



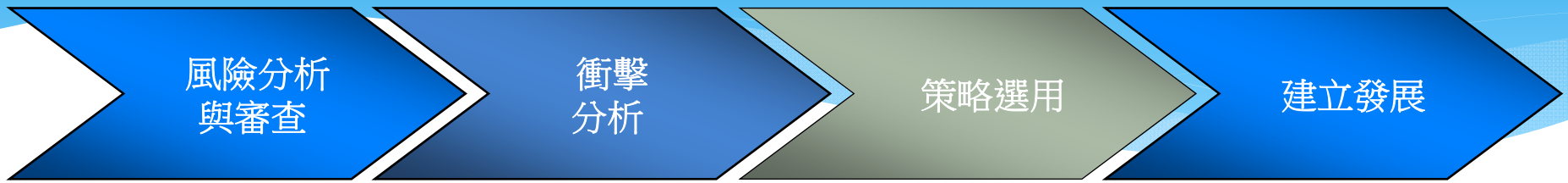
風險考慮因素

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