營運安全

- 門禁管制
  - 出入口常由警衛或接待員管制
  - 警衛或接待員是門禁管制的最佳選擇，他們人性化、機動、並且判斷合理，遠優於任何科技防禦設備
  - 若缺乏訓練、沒有紀律則會造成組織「錯誤的安全感(false sense of security)」，以為有保障而鬆懈，反而造成組織更加脆弱
  - 另一個問題是警衛或接待員常被同時指派其它工作，例如文書遞送、採購、甚至司機等，造成門禁管制的空窗時間

營運安全 (Cont.)

- 閉路監視設施 (closed circuit television, CCTV) 需要具備以下三種功能：
  - 偵測 (detection)：可以偵測到物件出現
  - 識別 (recognition)：可以識別那個物件是什麼東西
  - 指認 (identification)：可以指認物件的部分細節
  - 在裝置閉路監視系統時，應該消除盲點 (blind spots)
  - 較佳的閉路監視系統具備移動偵測功能 (motion detection)，當有物件在監視範圍內移動就會通知監視人員，同時開始儲存畫面

營運安全 (Cont.)

- 入侵感應設備
  - 裝設於圍牆上的入侵感應設備，許多出入口照明也具有移動偵測功能，有助於嚇阻及偵測
  - 入侵感應設備常因貓、鳥跨越而造成誤警報 (false alarm)，因此配合燈光照明與閉路監視系統使用，有助於正確地偵測與辨識
  - 入侵感應設備的種類
    - 常用於圍牆上，靠切割紅外線光束來感應
    - 被動式紅外線感應器可以感應體熱的輻射
    - 利用超音波反射，物件通過會改變反射距離
    - 使用微波感應或氣壓感應

營運安全 (Cont.)

- 火災偵測
  - 火災偵測設備要有效地全面覆蓋
  - 偵測器的種類
    - 離子型煙幕偵測器 (ionization-type smoke detectors)：火焰燃燒產生導電之離子，使接收器中的電流訊號增強
    - 光學偵測器 (optical detectors)：火焰燃燒所產生之煙幕會阻斷偵測器內部的光訊號
    - 溫度偵測器 (heat detectors)：火焰燃燒造成偵測器氣室中線圈的溫度改變，並產生電阻與電壓的變化

營運安全 (Cont.)

- 備份與備援
  - 「備份」通常指資料的一個靜態副本
  - 「備援」則指動態的、系統持續運作中的救援措施
  - 用備份 / 備援來保護資料時，可考慮以下的層次
    - 資料備份：定期備份資料，為求備份完整，會複製整個磁碟
    - 磁碟陣列容錯：在運算中維護資料的完整性與可用性
    - 遠端即時備份：透過網際網路或專線，即時的在遠端建立備份。一旦系統需要復原的話，遠端所儲存的是最新的備份

營運安全 (Cont.)

- 備援伺服器：不只備份資料，還有相同的伺服器做故障復原 (failover)
- 備援服務：整個系統完整複製（可能在另一個地方），一旦主機房主機房因故無法運作，備援服務能在幾分鐘內啟動

緊急應變計畫

- 災難造成的影響
  - **財產損失**：未妥善備份、備援的資訊資產也無法恢復的直接損失
  - **客戶失去信心**：設想一家專業的網路資料中心(IDC) 被火災燒毀，即使事後獲得保險理賠，也可能因失去客戶而倒閉
  - **災害復原成本過大**：就算災難後沒有立即的財務缺口，企業未必能支付持續的復原與重建的成本
  - **失去關鍵技術或生產能力**：資訊資產被毀，可能會失去智慧財產。若組織只備份「結果」卻沒有「過程」，會造成技術無法複製

緊急應變計畫 (Cont.)

- **失去主要領導人或技術擁有者**：人員傷亡也可能造成企業無法彌補的傷害，有些企業規定主要經理人不可搭乘同一交通工具
- 緊急應變計畫與**風險管理**
  - 從緊急應變計畫的角度看，風險管理有兩大功能
    - 識別威脅與弱點，並建置適當的防禦手段來避免事件的發生或降低它造成的衝擊
    - 識別殘餘風險，讓緊急應變計畫來處理

備份方法

- 備份方法
  - 緊急應變政策應該對組織的備份頻率與方式做規範。備份可分**完整式**與**增加式** (每次只備份變更過的部分)；存放可分**本地**與**異地**
  - 以專業的資料中心做異地備份是個好選擇；可以在自己機房將資料備份在磁帶、磁碟或光碟上，再送到異地資料中心存放
  - 選擇異地備份地點時應考慮以下原則
    - 應仔細評估該地點的安全性，與管理人員的素質
    - 存放環境必須符合規範，包括溫度、濕度控制以及消防設備等

備份方法 (Cont.)

- 該地點與主機房之間的距離如果太近，有可能受到同一個災難衝擊
- 要考慮地點的方便性，包括來回存取資料備份媒體所需要花費的交通時間，與該地點的開放時間是否適當
- 最後，存放與復原成本也應列入考

- 異地備援
- 雖然造成長期資訊服務中斷的災難很少發生，但卻是緊急應變計畫的重點之一，因此這個計畫需要包括在異地復原系統運作的策略。該地點及設施可以是組織所擁有或是租用專業的資料中心 (IDC)

備份方法 (Cont.)

- 異地備援分以下幾種
  - **冷備援** (cold sites)：具備足夠的基礎設施，如機房、水、電、及辦公室空間；但是沒有軟硬體設備或電話、傳真等辦公設備。受災害衝擊的單位進駐後才重新建立系統，需要數周的時間復原資訊服務
  - **暖備援** (warm sites)：有部分資訊與辦公室設備；平時這個地點及設備可能做為它用，當緊急應變計畫啟動，受災害衝擊的單位進駐後，會在現有設備上重建系統，需要幾天到數周的時間復原資訊服務

備份方法 (Cont.)

- **熱備援** (hot sites)：隨時軟硬體及人員準備妥當，一旦緊急應變計畫啟動，可在幾小時內復原資訊服務
- **全備援** (mirrored sites)：平時就與主機房完全同步備援，系統完全相同且資訊即時備份。一旦主機房服務中斷，備援系統立即啟動。

建立緊急應變計畫

- 緊急應變協調人有足夠的資訊將整個緊急應變計畫制訂出來。計畫應包含三個階段
  - **通知與啟動階段** (notification/ activation phase)：當災難發生時應按程序通知上級和相關人員；經過損失評估後若有必要，就可以依照程序啟動緊急應變計畫
  - **復原階段** (recovery phase)：災難發生後，短期的重點是如何快速地復原資訊服務；這一階段說明復原活動的順序與標準作業程序
  - **重建階段** (reconstitution phase)：災難結束後就要重建原地點，當系統重裝或修復並通過測試後，就可以停止備援系統並結束緊急應變計畫

建立緊急應變計畫 (Cont.)

- 計畫啟動
  - 災難發生後應先通知**損失評估小組** (Damage Assessment Team)，評估完系統所受的衝擊後，將結果及應採取的措施通知相關部門及個人
  - 若損失達到一個或多個**啟動條件** (activation criteria)，緊急應變協調人或資訊長就該啟動緊急應變計畫。組織可依據以下狀況來訂定啟動條件，並記載於緊急應變計畫文件中
    - 人員傷亡以及設施的損失程度
    - 系統遭受損失的程度
    - 遭受損失的系統對組織運作的重要性
    - 預計服務中斷的時間長度