一般人員教育訓練
資訊安全認知與相關法規

課程大綱

1. 資訊安全簡介
2. 資訊安全威脅
3. 高階主管應扮演之角色
4. 案例探討
5. 資安教戰手冊
6. 通資安全法令

資訊安全簡介

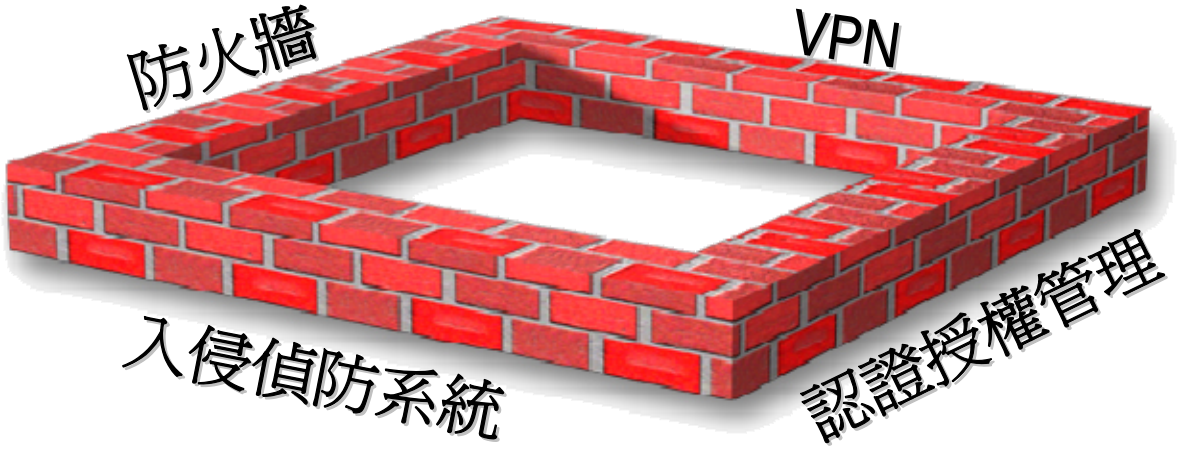
資訊安控的問題點

- 大多已購買資安設備
- 大多已作過系統安全修補購買防火牆
- 大多已購買入侵偵測
- 大多已購買防毒程式

No Management, No Security

一般都會注意…

- 建立安全的周邊環境…



結果是…

據統計有80%的資料遺失, 是因為內部人員有意或無意之下所造成的結果

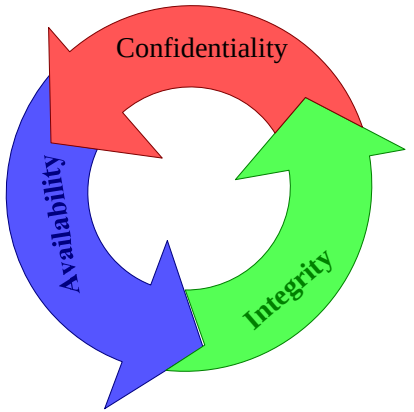
何謂資訊安全管理制度(ISMS)

- （Information security management system）

ISMS目的在於保護資訊資產的機密性、可用性與完整性。

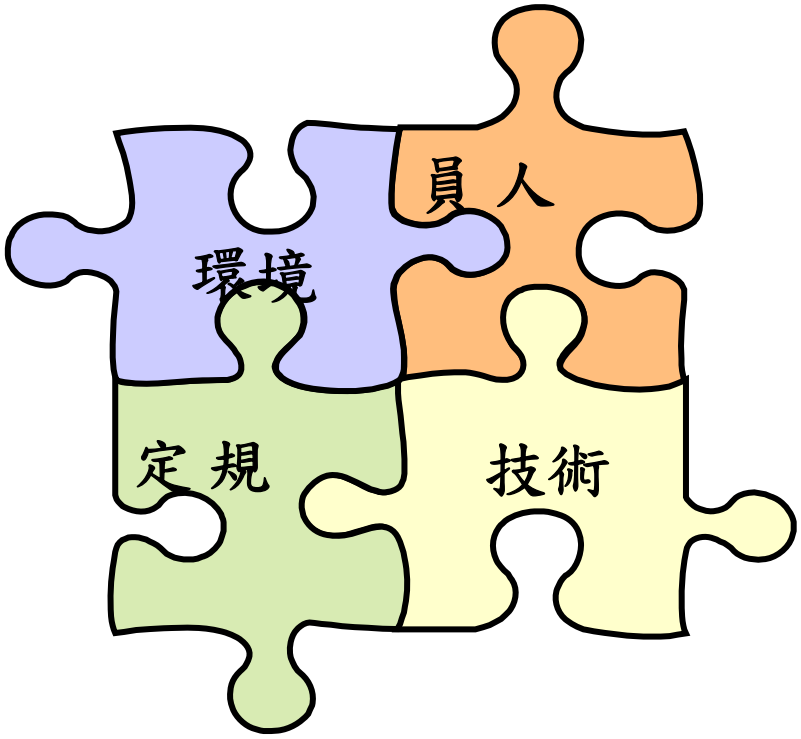
資訊安全三要素

- 機密性，Confidentiality
  - 保護資訊不被非法存取或揭露
- 完整性，Integrity
  - 確保資訊在任何階段沒有不適當的修改或損毀
- 可用性，Availability
  - 經授權的使用者能適時的存取所需資訊

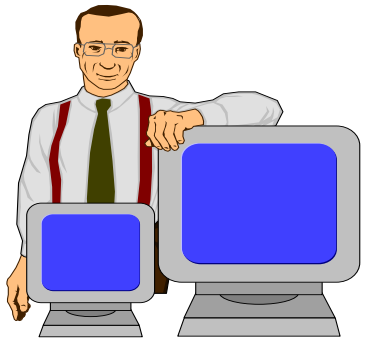


資訊安全的範圍

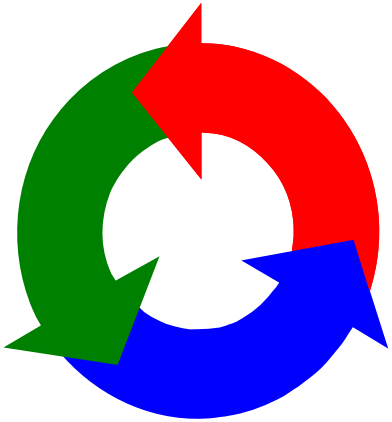
- 資訊使用之『環境』
- 資訊使用之『技術』
- 資訊使用之『規定』
- 資訊使用之『人員』

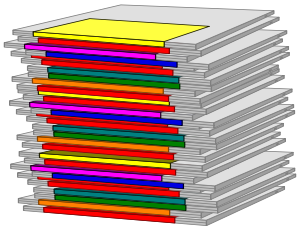


資訊安全管理重點

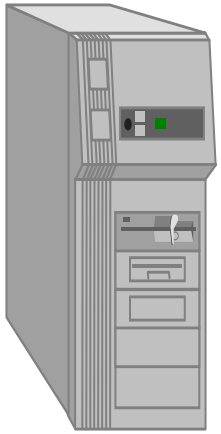


People



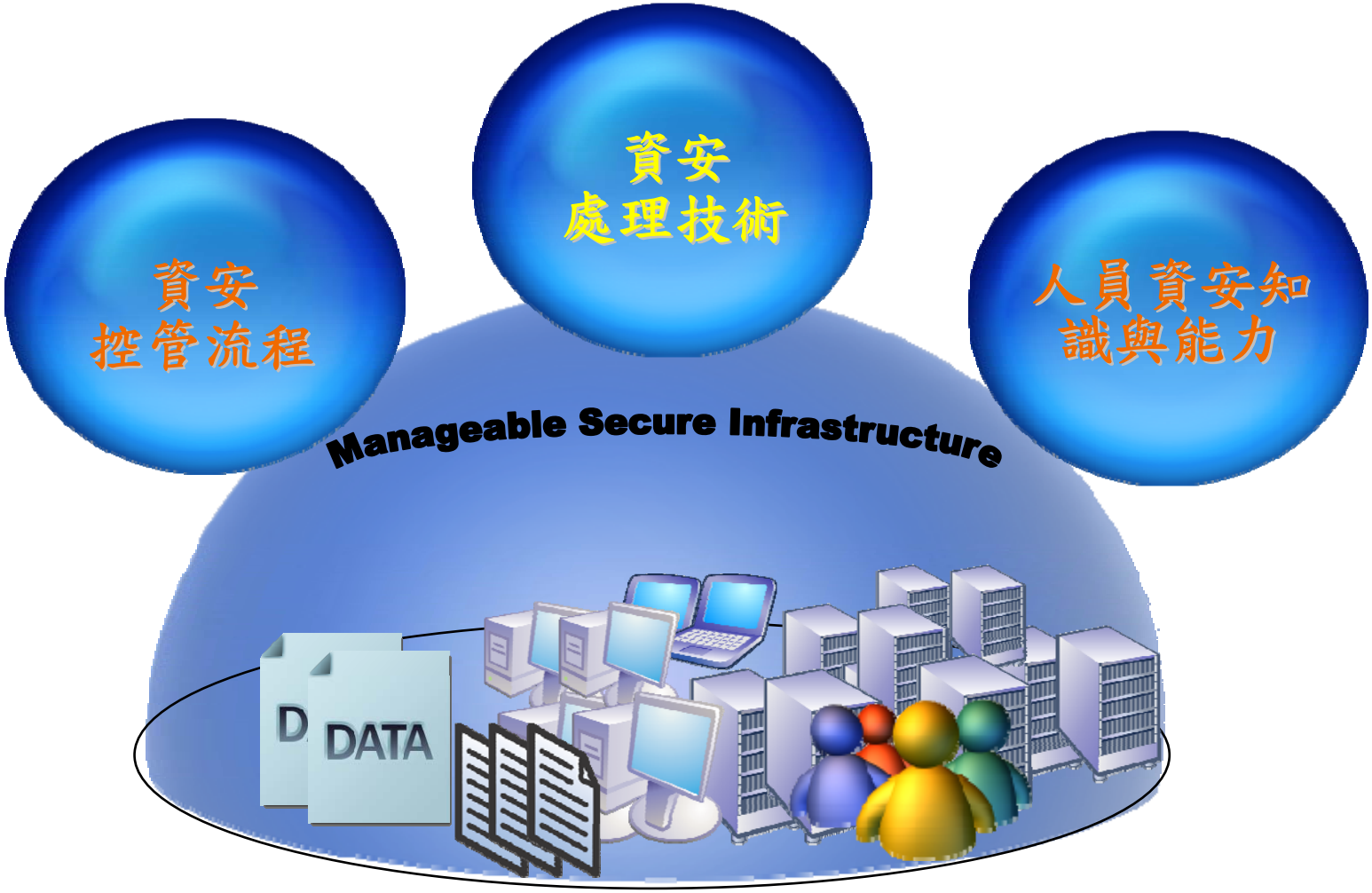


Process



Technology

資訊安全管理重點


資安
處理技術
資安
控管流程
人員資安知
識與能力
Manageable Secure Infrastructure
DATA

資訊安全事件定義

- 資訊安全事件指的是任何違反常軌的異常行為，其可能造成資訊系統及網路的安全威脅。
- 經證明可能導致資訊系統運作錯誤事件或事故之情形及其後續所產生之故障效應等。
- 從設備故障、人員差錯、人為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資安事件範疇內的事件案例。

資訊安全事件等級

- 依據91年06月06日行政院資通安全會報，第二次修訂之「建立我國通資訊基礎建設安全機制計畫」，資通安全事件等級概分為四級

  - **A 級**：影響公共安全、社會秩序、人民生命財產
  - **B 級**：系統停頓，業務無法運作
  - **C 級**：業務中斷，影響系統效率
  - **D 級**：業務短暫停頓，可立即修復

資安事件的類型

- 內部事件
  - 遭人為惡意破壞毀損、作業不慎等危安事件。
  - 設備故障
    - 能直接或間接影響機房安全資訊系統的各個設備的故障可視爲資通事件。
  - 人員差錯
    - 錯誤或不良的維護、錯誤設定和操作員的其他錯誤行為等。
  - 其他內部事件
    - 內部原因所引起的火災、爆炸等對機房安全可能產生重要之影響 。

資安事件的類型

- 外部事件
  - 因外部事件或自然事件所引起某一安全重要系統、元件或建築物故障的可能性，可經由設計和建造中所採取的因應措施，將其風險降低至可接受的程度
    - 病毒感染事件
    - 駭客攻擊（或非法入侵）事件
- 自然事件
  - 天然災害：颱風、水災、地震
  - 重大突發事件：火災、爆炸、核子事故

資訊安全威脅

資訊安全威脅與來源

好奇人士

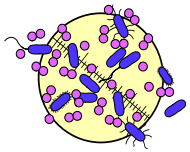
內部員工

預謀犯罪的歹徒

間諜

組織型駭客

好奇的人士可能剛學會入侵電腦的方法，
就應用書本上寫的方法當起駭客



病毒

蠕蟲

木馬

社交工程

資訊安全威脅與來源


好奇人士

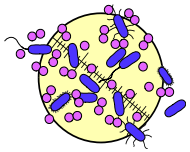

內部員工


預謀犯罪的歹徒


間諜


組織型駭客

內部員工也<u>有可能</u>是潛在的威脅，尤其對單位有不滿情緒及抱怨的人


病毒


蠕蟲


木馬


社交工程

資訊安全威脅與來源


好奇人士

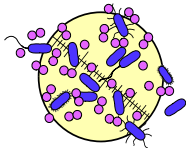

內部員工


預謀犯罪的歹徒


間諜


組織型駭客

預謀犯罪的歹徒是大家最熟悉的，會透過各種方式竊取單位機密、牟取暴利，如：販賣個人資料


病毒


蠕蟲


木馬


社交工程

資訊安全威脅與來源

好奇人士

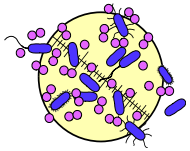
內部員工

預謀犯罪的歹徒

間諜

組織型駭客

間諜也是資安威脅的一種，因為商業上或政治上的因素，以各種滲透入侵技術，取得企業機密文件



病毒

蠕蟲

木馬

社交工程

資訊安全威脅與來源


好奇人士

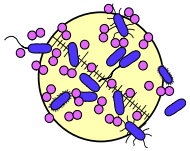

內部員工


預謀犯罪的歹徒


間諜


組織型駭客

組織型駭客一般都扮演入侵者的角色，主要以竊取或破壞單位內部電腦機敏檔案資料為主，是以刺探、布建、竊取為目的


病毒


蠕蟲


木馬


社交工程

風險來自

- 電腦環境的潛在風險

風險的類型	範例
天災與實體	火災、水災、風災、地震 停電
非蓄意	未被告知的員工 未被告知的客戶
蓄意	駭客、恐怖份子、工業間諜、政府、惡意的程式

風險來自

- 電腦環境的潛在弱點

風險的類型	範例
實體	門未鎖
天然	消防系統失效
硬體與軟體	軟體版本過期、韌體過舊
媒體	電子干擾
通訊	沒有加密傳輸
人為因素	疏失

來自網路的威脅

- 有線網路
  - 利用線路找尋設備資訊，封包加密較完整，若有人自線路中竊取資訊，至少還有軌跡可尋，無論是管理、安全、記錄資訊等較為方便。
- 無線網路
  - 安全問題最令組織擔心，由於無線電波透過空氣傳遞訊號，只要在無線基地台訊號範圍內，都能擷取訊號資訊，故而管理無線網路資訊安全比有線網路更為困難。

無線基地台(AP)

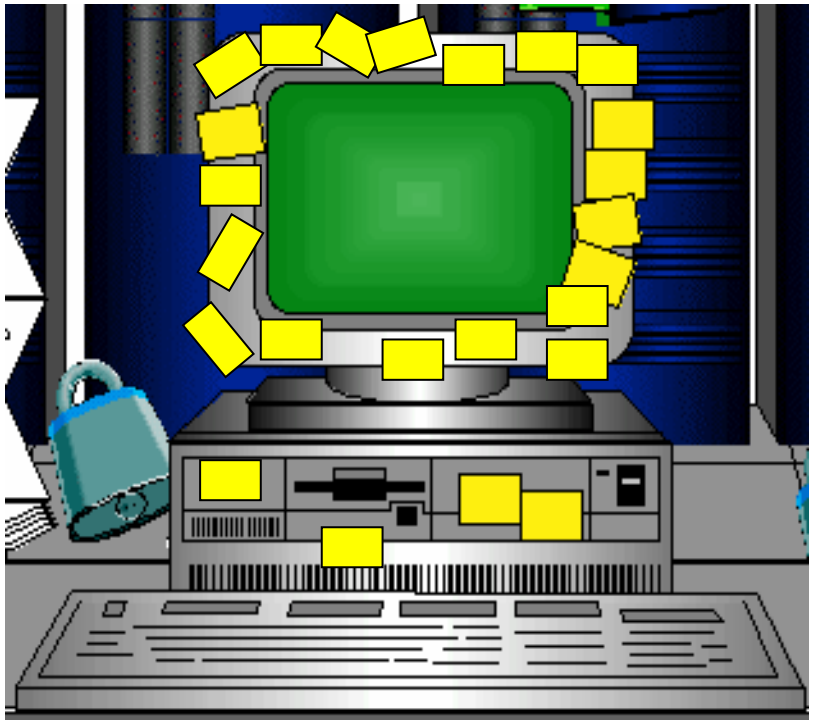
來自離職員工的威脅

衛豐運鈔車遭劫　警政署開罰百萬　撤銷其「優良」資格

來自內部粗心員工的威脅

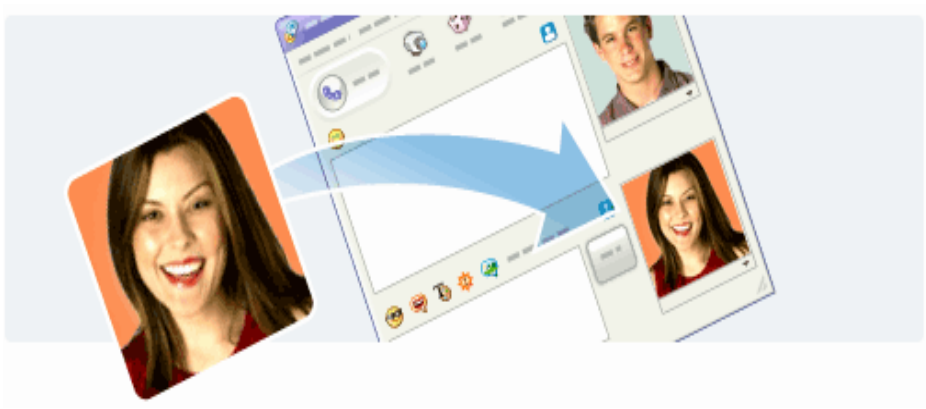
- 不規避旁人，如重要資料或密碼輸入
- 不隨手關機
- 隨時討論業務機密
- 使用者帳號隨便借給他人
- 印出的報表隨手亂放
- 檔案資料未事先分類
- 硬碟存放私人資料
- …

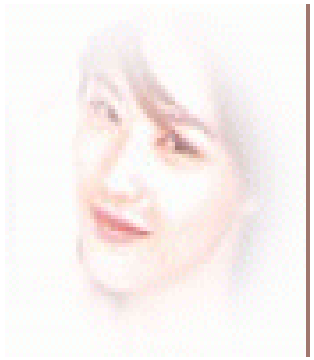
密碼輸入？ 明碼張貼!!



即時通軟體的安全隱憂

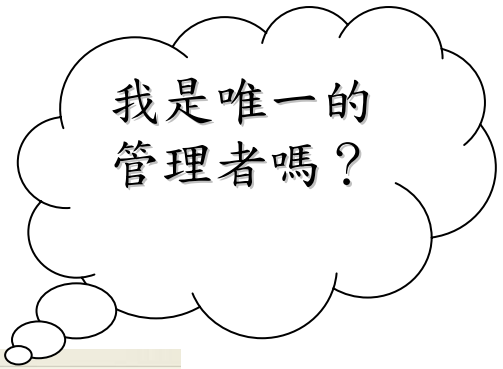
- 台灣常見的即時通軟體





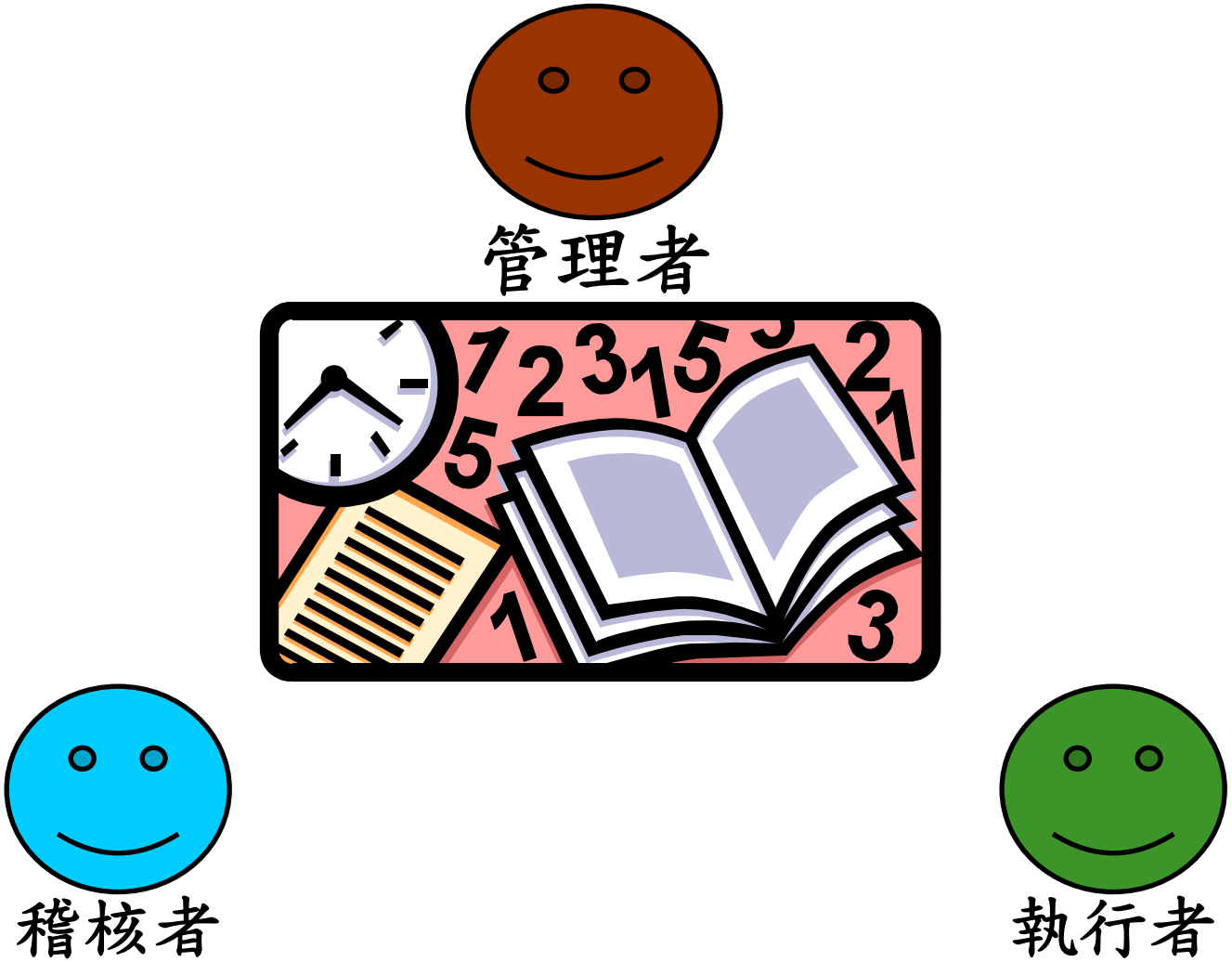
免費的網路資源

- 免費的電子郵件空間，高達2G
- 免費的網站空間，100M



高階主管應扮演之角色

權責分工



人員定位


專業顧問
risk management
Specialist staff who provide independent opinions on the status of risk management
Top management
High-level steering group
Driving force
Local coordinators
(eg. BCP champions, business unit specific)
'Owners, user, keeper' of business critical information resources
最高管理階層負責企業整體資訊安全之成敗，並決定風險忍受等級和資源之分配
負責跨部門協調及政策推動
（部門主管，IT，風險管理部門）
資訊安全任務推動者
資訊安全任務之執行者及部門內協調者
組織重要資訊資產擁有著、使用者、保管者

基本觀念

- 資通安全絕不是僅僅是資訊人員之責任。
- 資通安全絕對是組織全體之責任。
- 資通安全絕對需要長官的大力支持。
- 資通安全之推動絕對不是專案形式。
- 組織每位成員都可能成為資安漏洞。

ISMS之管理責任(1)

- 管理階層應提供承諾建立、完成、監督、檢視、維護及改善ISMS之承諾：
  - –建立資訊安全政策。
  - –建立資訊安全目標及計畫。
  - –建立資訊安全之角色及責任。
  - –跨部門溝通及協調。
  - –提供足夠資源。
  - –決定可接受風險值。
  - –確認ISMS內部稽核之執行。
  - –執行ISMS管理階層檢視。

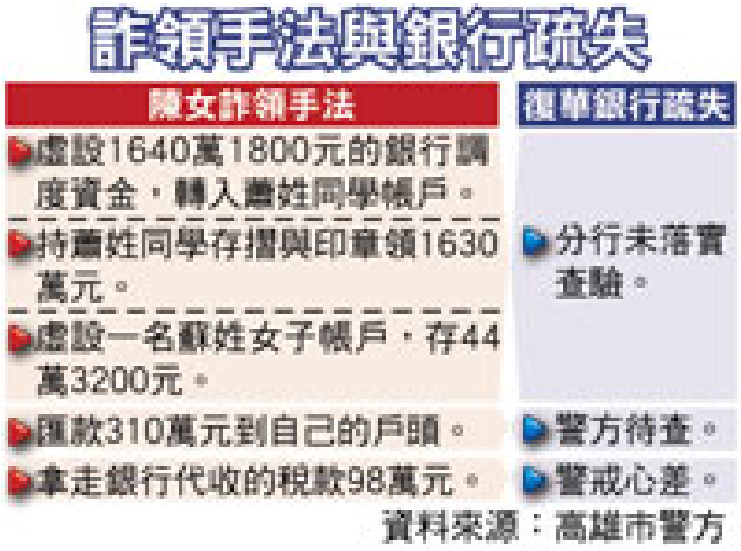
ISMS之管理責任(2)

- **資源管理**，管理階層應決定並供應資源給下列需求：
  - –提供開發、建置、運作、維持及改善ISMS所需之足夠資源。
  - –確保資訊安全程序可支持業務需求。
  - –辨識及確認法令及規範之要求、履行合約之義務。
  - –藉由正確運用所有建置的控制以維持適當的安全。
  - –執行檢視作業，並適當地回應檢視之結果。
  - –持續改善ISMS。

案例探討

女行員盜銀行鉅款2千萬，同事還代開車門

- 復華銀行高雄市三民分行一名女會計行員，疑因負債四、五百萬元，利用職務之便竄改電腦紀錄，共詐領二千零九十二萬五千元銀行帳款，得手後於昨早搭澳門航空班機赴澳離台。銀行稍早發現該行員未到班、清查發現遭詐領後報案。警方調查發現因該分行便宜行事、未落實內部安全管控，才會讓行員輕鬆詐領二千多萬元逃逸。陳女依涉嫌詐欺、背信、《洗錢防制法》等罪嫌起訴。



資安觀點:

1. 虛設幽靈數位帳號很容易。
2. 轉帳授權密碼隨意借。
3. 員工對系統與流程安全無意識。
4. 危機處理未及時。
5. 深知系統漏洞的最大駭客，常是內部不肖人員。

臍帶血業者競爭 報告書變對手文宣

- 民眾儲存臍帶血，資料卻遭外洩，淪為業者競爭下的犧牲者！有消費者到訊聯生物科技儲存臍帶血，但相關報告書卻被訊聯對手生寶生物科技刊登在廣告文宣上，還被批評這份報告書不夠專業，兩家業者卻不願道歉，讓消費者氣炸。訊聯說，資料不可能外漏，生寶則不願回應。律師表示，兩家業者的做法已侵害個人隱私，消費者可向業者提告求償。

民眾保護個人資料應注意事項：

1.簽約內容應有保密條款，明定保密內容，如：個人資料等。
2.民眾可自行訂定違約條款。
3.發生個人資料遭盜用時，須保留證據，如：廣告單及契約正本等。

資安觀點:

1.客戶資訊保護不周毀了商譽(訊聯)。
2.行銷資訊引用疏忽傷了利益(生寶)。

台彩大烏龍 當機兼派錯獎金

- 由中國信託商業銀行接手的公益彩券昨天開賣，但狀況百出，各地投注站電腦大當機、久久無法連線，有民眾排了三小時還買不到彩券，有經銷商因此整個上午一張都沒賣出去，民眾與經銷商昨罵聲不斷。負責中信銀彩券業務的台灣彩券表示，無法連線與當機問題應是網路塞車造成。
- 台灣彩券公司再度擺烏龍，昨晚開獎的樂透彩，本期各獎項獎金總額原本為五千三百十萬餘元，卻誤植為七千五百卅七萬餘元，台彩公司在深夜十一時四十分緊急通知更正。

資安觀點:

1. 資安的範圍，除了資訊的機密性外，亦涵蓋了可用性與完整性。即使重要資料沒有洩漏，但系統無法提供服務，或未達預期服務水準，以及資料錯誤或誤用，都必須視為資訊使用的風險，亦需提出矯正預防措施來改善。
2. 除了健全的資訊系統外，系統的維護人員及使用人員的訓練，也是降低資訊風險不可或缺的一環。

盜用他人帳號 遭函送

- 某科技大學助理教授，遭檢舉涉嫌盜用校內教授帳號及密碼，在網路上行使國科會產學計劃共同主持人的同意權，企圖讓自己成為計劃共同主持人，經學校舉報檢調依違反「電腦處理個人資料保護法」函送法辦。

妨害電腦使用罪 刑法第３５８條：
「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

資安觀點:

1.密碼除了保障資訊的"機密性"與"完整性"外，對於資訊作業的"可歸責性"維持亦是相當的重要。

2.使用他人的帳號密碼非但違反個資法，若情節重大，還有可能違反刑法第３５８條。

假銀行網站－竊個資盜存款

假銀行網站 竊個資盜存款

Focus 焦點提要

B1

鎮代開淫窟 逼越女賣淫

B2

今彩539 第096028期開獎號碼 本期頭獎中獎數：2注

7 11 23 32 35

24星彩 第096028期 開獎號碼 本期獎號正彩注數：17注 4 1 9 4

3星彩 第096028期 開獎號碼 本期獎號正彩注數：80注 6 1 9

（記者黃敦硯／台北報導）喜歡透過網路交易的網友可得當心了！在敲下鍵盤進行交易的同時，對岸的中國廈門正有犯罪集團以遠端遙控功能及鍵盤側錄程式（Keylogger），側錄你上網時所輸入的帳號密碼，他們還會在你電腦植入木馬程式，搜尋你電腦所有磁碟的憑證檔案，接著便可任意轉帳或盜取你的個人資料，讓你被看光光、盜光光。

掌握多名中國可疑共犯

刑事警察局說，近來有一個由兩岸駭客組成的詐騙集團，專門購買網路關鍵字廣告服務，再架設冒充銀行、航空公司的假官方網站，一旦網友連結，便會遭到詐騙集團以「網路釣魚」方式植入木馬程式，經連日追查，刑事局已掌握多名可疑中國共犯身分，正透過管道請中國公安代為追查，而因損害情形仍持續擴大，刑事局昨緊急提出警告，請網友提高警覺。

竊取數十萬筆個資行騙

刑事局表示，駭客集團架設包括土地銀行等十家銀行的網路銀行、華航與長榮等兩家航空公司、一〇四人力銀行、四家旅行社、四家電腦科技公司與數個理財網等，初步清查已逾五十個假網站，警方初步估計該集團可能已取得數十萬筆個人資料，民眾遭盜轉金額近千萬。

警方發現，這個詐騙集團是由兩岸人士組成，平常都在中國廈門一帶活動，除了有駭客負責操作「釣魚網頁」外，還僱用多名中國籍人士擔任「資料蒐集員」、「資料操作員」，將蒐集到的個人資料分門別類，若有銀行金融資料，則加以冒貸、預借現金，若是身分資料，便打電話行騙。

警方說，該犯罪集團的手法是先設立一個與正牌網站相似度極高的假網站，然後再到各大入口網站購買關鍵字廣告服務，這些假網站的網址與正牌網站的網址極易混淆，例如英文字母小寫「l」與阿拉伯數字「1」，或者「o」與「u」、「n」與「h」等很像的字母，讓上網民眾難以辨別而掉入陷阱。

網站魚目混珠側錄密碼

據了解，這個詐騙集團一開始是鎖定航空公司的會員資料，架設假網站，取走會員累積的搭機里程數，再上網販賣，經刑事局調查，至少有上百名會員，上千萬公里的里程數被取走，警方戲稱，「這些被偷走的里程數都可繞地球好幾圈了！」

警方指出，該集團從去年底將目標轉向網路銀行、人力銀行、旅行社等可能取得大量客戶資料的目標。令警方驚訝的是，該集團甚至會整理出被害人之間的親屬關係，研判可能做為「假親綁架、真詐財」之用。

（相關新聞刊B1）

網路下餌釣魚

駭客詐騙集團利用關鍵字搜尋，架設假網站，搜尋「土地銀行landbank」網站的網址，英文「land」應是小寫的「l」（圖左下），仔細看可發現變成阿拉伯數字的「1」，一旦網友連結，便會遭到詐騙集團以「網路釣魚」方式植入木馬程式，即可任意轉帳或盜取你的個人資料 。（記者黃敦硯翻攝）

TANet 網路中心導入資訊安全管理制度及資訊安全專業人才培訓計畫

資安教戰手冊

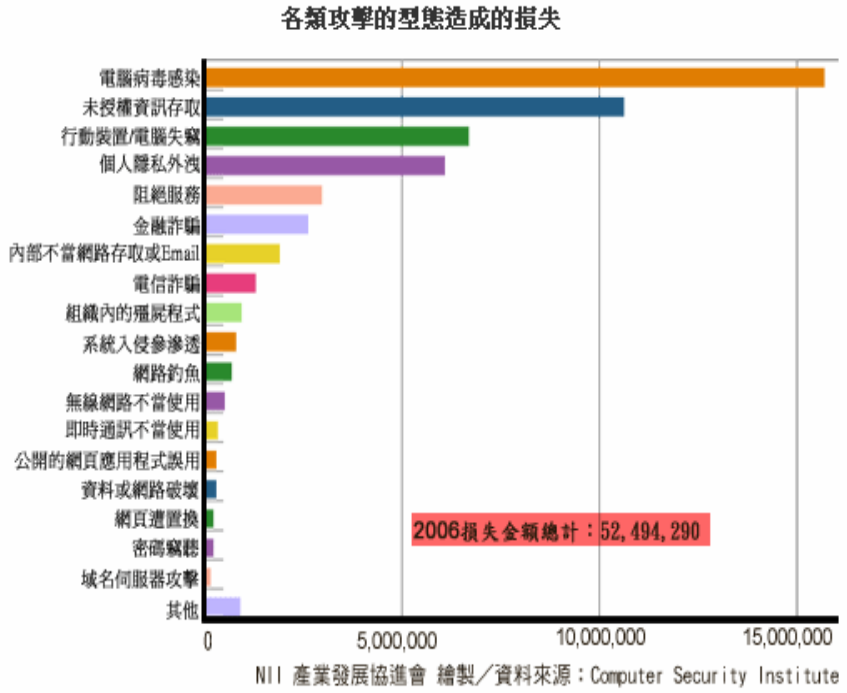
資訊安全損失

- 美國企業2006年資安損失約達5千萬美元

CSI/FBI 2006 Computer Crime and Security Survey：美國企業2006年資安損失約達5千萬美元

資料來源：Computer Security Institute
公布日期： 2006年

根據CSI/FBI 2006 Computer Crime and Security Survey，針對美國企業、政府、金融、醫療、學校等單位資訊安全從業人員調查「各類攻擊的型態造成的損失」，前三名分別是電腦病毒感染、未授權資訊存取、行動裝置/電腦失竊。



使用者責任

- 使用者的態度，對於有效防止非法的使用者存取，以保障安全的工作非常重要。
- 目標：防止未經授權的使用者存取資訊與資訊處理設施，以及使其避免遭受破壞或竊盜。
  - 通行碼的使用。
  - 無人看管的使用者設備。
  - 桌面淨空與螢幕淨空政策。

通行碼的使用—密碼管理

- 定期更新密碼
- 定期檢查密碼
- 設定優質密碼
  - 避免使用重複數字、單位簡稱、詞語、生日
  - 數字字母符號穿插且不過於複雜。
  - 避免重複使用密碼。
- 不告訴他人密碼或寫下密碼
- 懷疑密碼外洩立即更新

無人看管的使用者設備

- 使用者應確保無人看守的設備獲得適當保護
- 安裝在公共區域的設備（如公用主機、印表機或伺服器），應有具體的保護
  - 在活動完成時應終止對話，結束畫面。
  - 螢幕保護程式需設定密碼保護。
  - 活動結束時登出系統或主機，再關閉電腦。
  - PC或設備不用時，應使用密鑰鎖或其他安全控制措施，以防止他人非法使用。

桌面淨空與螢幕淨空政策

- 桌面淨空
  - 重要、機密文件不置於桌上。
  - 重要、機密文件下班或離開辦公室前應鎖入安全空間。
- 螢幕淨空
  - 設定螢幕保護程式。
  - 設定保護密碼。
  - 離開座位或暫時不使用時鎖定螢幕。

處理公務時的安全防護

- 處理公文時須離線作業。
- 人員勿從網路下載與公務無關之不明程式。
- 公文系統均要求在內部網路處理。
- 不得將與公務有關之內容上傳至網際網路個人儲存空間。

要注意什麼？

- 考慮以下狀況
  - 攜帶型資訊設備之使用安全(如:隨身碟)。
  - 列印文件或使用傳真之安全。
  - 桌上型 PC的帳號密碼及螢幕保護密碼。
  - 使用E-mail的安全。
  - 防範個人電腦病毒。

要注意什麼？(續)

- 考慮以下狀況
  - 個人資料備份。
  - 辦公室、機房進出管制。
  - 非法軟體使用管制。
  - 資訊安全事件的通報。
  - 使用資訊系統的存取權限設定與主管覆核。
  - 人員離調職的帳號異動管理。

防範資料外洩

- 防範機密資料洩露方法
  - 減少在公共場所討論。
  - 離開座位，使用螢幕保護程式。
  - 在不使用或下班後將機密文件收妥。
  - 機密文件不遺留傳真機或影印機。
  - 傳真前通知對方領取。
  - 機密文件以碎紙機銷毀。
  - 機密檔案櫃或房間上鎖。
  - 會議室文件帶走及白板擦拭乾淨。
  - 儲存媒體報廢清除內容。

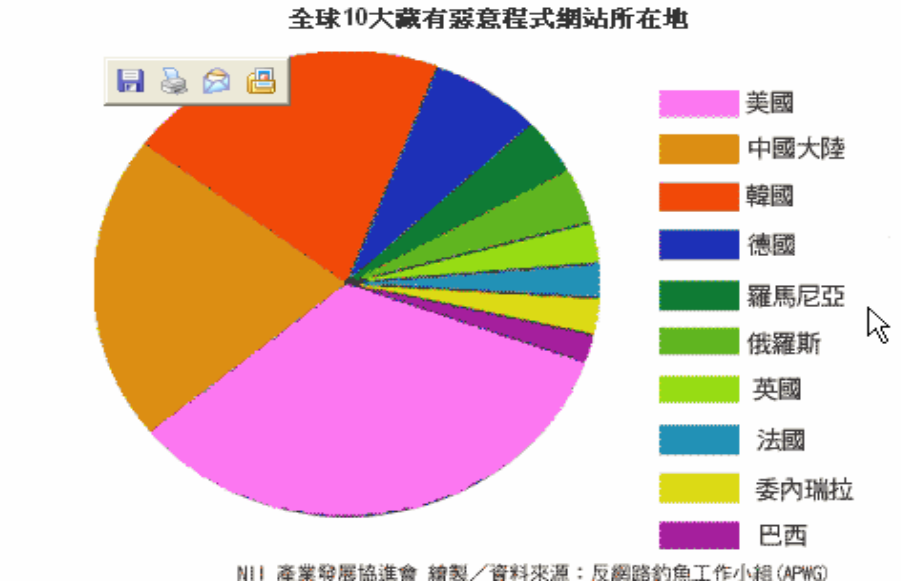
惡意程式網站

- 每十個網站就有一個是惡意網站

APWG: 全球藏有惡意程式網站的前三名國家
2006年11月：美國、中國大陸、韓國，委內瑞拉首次入榜
資料來源：反網路釣魚工作小組(APWG)
公布日期： 2007年1月

反網路釣魚工作小組（Anti-Phishing Working Group） 2006年11月全球網路釣魚調查報告：

全球藏有惡意程式的網站前十名分別在美國(24.2%),中國大陸(15.42%),韓國(14.88%),德國(5.27%),羅馬尼亞(2.84%),俄羅斯 (2.64%), 英國(2.04%), 法國 (1.83%),委內瑞拉(1.81%), 巴西(1.43%)。



網路釣魚攻擊

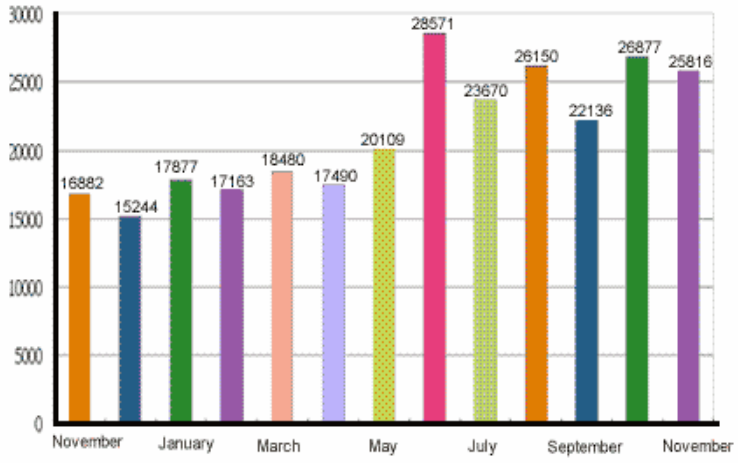
- 全球120個企業品牌被駭客用來透過電子郵件進行網路釣魚詐騙活動。
- 英國2006年約350萬人遭網路詐騙。

2006年11月全球網路釣魚攻擊通報數量超過25,816個

資料來源：反網路釣魚工作小組(APWG)
公布日期： 2007年1月

反網路釣魚工作小組（Anti-Phishing Working Group）2006年11月全球網路釣魚調查報告：

- 全球釣魚網站數量達到37,439個
- 全球網路釣魚攻擊通報數量約25,816件
- 全球總計有120個企業品牌被駭客用來透過電子郵件進行網路釣魚詐騙活動

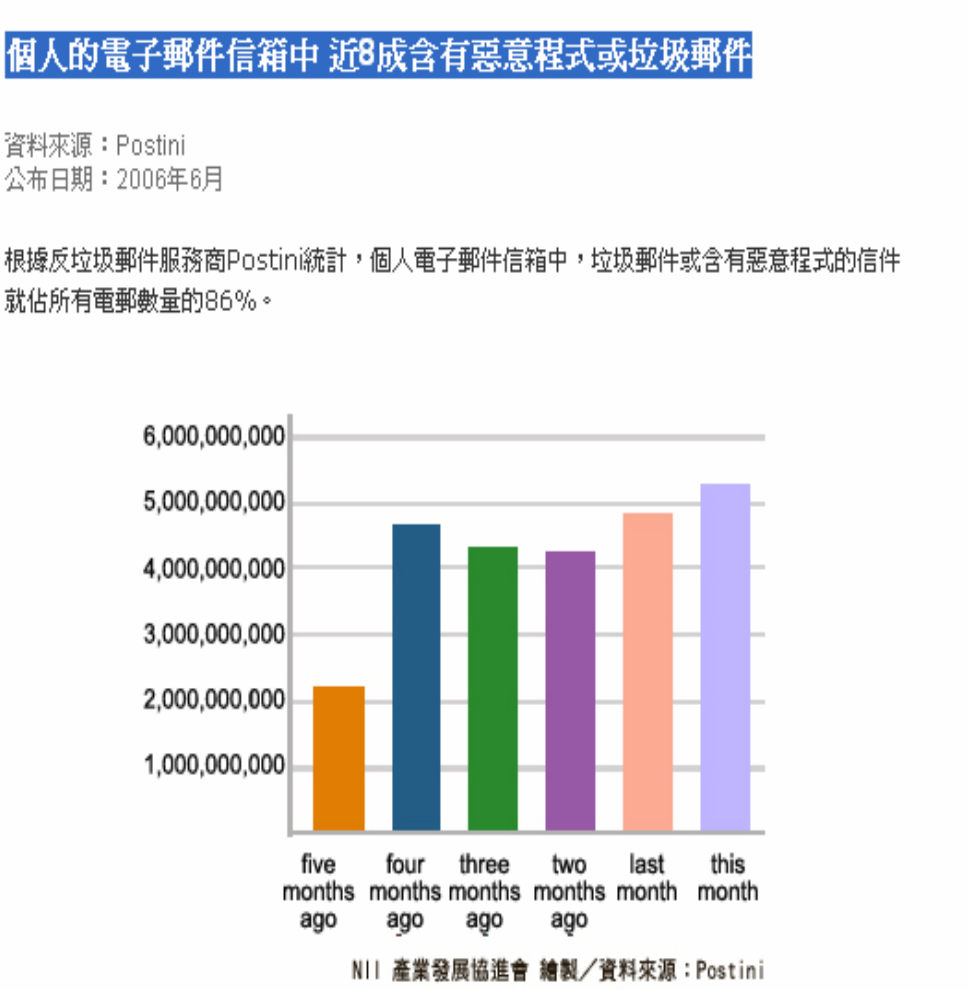


網路使用安全

- 確保網頁瀏覽器使用安全
  - 設定網頁瀏覽器安全性、隱私權。
  - 設定信任的網站。
- 遠離網路釣魚犯罪陷阱與騙局
  - 不回應不明公司、技術部門要求提供個人隱私或安全資訊。
  - 不點選來路不明郵件的網頁連結。
  - 不利用企業網路轉寄垃圾郵件。

電子郵件風險

- 國內30.7%網路人口一天收到10封垃圾郵件。
- 垃圾郵件讓美國企業一年損失達700億美金。
- 個人的電子郵件信箱中近8成含有惡意程式或垃圾郵件。



電子郵件的安全

- 安裝防毒軟體過濾郵件
- 不隨意開啟郵件附檔
- 防堵垃圾郵件
  - 絕對不回覆垃圾電子郵件訊息。
  - 不購買垃圾電子郵件的廣告商品。
  - 不轉寄串接式的電子郵件，(例如聲稱不轉寄給10 個人就會倒楣的電子郵件)。
  - 要寄送同一訊息給許多收件者時，可採用「密件副本」方式來進行。
  - 刪除寄件者為空白的電子郵件。
  - 使用垃圾電子郵件過濾軟體。
- 垃圾郵件過濾簡易設定
  - 在**Web** 郵件上設定過濾垃圾郵件寄件者。
  - 利用常見關鍵字過濾郵件。

即時通訊軟體的風險

- 存在的風險
  - 病毒威脅。
  - 垃圾訊息。
  - 檔案交換。
  - 洩密。
  - 工作效率的影響。
- 常犯之錯誤
  - 盲目的檔案分享。
  - 花費過多時間於私人聊天。
  - 將個人帳號資訊以儲存密碼方式設定儲存。
  - 任意將個人之連絡者清單給他人。

即時通訊軟體使用安全

- 登入密碼最好不要用「儲存密碼」記錄於系統內
- 不任意傳遞與分享公司重要資訊或檔案。
- 不任意接收來路不明之分享檔案。
- 使用者必須秉持以公事使用之目的使用企業即時訊息。
- 隨時更新使用端程式。

電腦作業威脅—電腦病毒

- 電腦中毒徵兆
  - 電腦系統運行速度異常緩慢。
  - 上網速度越來越遲緩。
  - 異常的系統訊息通知。
  - 螢幕顯示異常，例如畫面突然一片空白。
  - 來自防毒軟體的警告訊息。
  - 電腦無故自動關機或不斷重新開機。
  - 瀏覽器自動出現產品廣告或色情網頁。
  - 網路流量異常，例如沒有使用網路服務或收發電子郵件，但網路的連線燈號卻一直閃爍。

電腦作業威脅—電腦病毒

- 電腦病毒的防範
  - 確認防毒軟體隨時運作。
  - 勿隨意安裝未經許可的電腦軟體。
  - 確保軟體在最新更新狀態。
  - 使用有問題立即反應。

電腦作業威脅—廣告、間諜軟體

- 廣告或間諜軟體的症狀
  - 沒有上網卻還是一直看見廣告視窗。
  - 網路速度時快時慢。
  - 首頁被更改成奇怪的網站。
  - 視窗下方的工具列出現許多原本沒有的工具
  - 瀏覽器多出沒有安裝過的工具列、搜尋工具，而且無法移除。
  - 電腦處理速度變慢或當機頻率增加。

電腦作業威脅—廣告/間諜軟體

- 廣告或間諜軟體的防範
  - 使用防火牆阻擋。
  - 關閉網路瀏覽器的ActiveX 功能。
  - 安裝封鎖彈跳視窗功能的工具。
  - 下載免費軟體前仔細閱讀所有相關資訊。
  - 學習資料備份基本技巧。

電腦作業威脅—駭客入侵

- 駭客入侵的徵兆
  - 檔案及資料庫內容遭到竊取或篡改。
  - 不知名的IP來源與電腦連線。
  - 系統中異常的服務程式。
  - 異常通訊埠開啟。
  - 稽核紀錄及檔案中的異常事件。
  - 系統帳號的異常增加。
  - 系統異常的訊息或行為。

電腦作業威脅—駭客入侵

- 駭客入侵的簡易處理
  - 定期系統備份。
  - 針對可能入侵途徑系統作隔離。
  - 蒐集入侵紀錄、檔案等軌跡。
  - 追查駭客IP來源。
  - 分析資料找出入侵方式並改善。
  - 報告相關單位。
  - 適時尋求協助。

電腦作業威脅—駭客入侵

- 駭客入侵的防範
  - 即時更新修正檔。
  - 檢視權限設定。
  - 日常備份作業。
  - 紀錄及檢視稽核軌跡。
  - 設定自動時間校正作業。

資料備份

- 不論是紙本或電子檔的重要資料，皆應：
  - 定期備份。
  - 存放在不同地方(異地備份)。
- 資料備份原則
  - 資料價值較高時應優先備份。
  - 擇適合之儲存媒介進行資料備份工作。
  - 按所欲備份的資料型態，選擇方法進行備份(如：完全備份、選擇性備份、漸進式(增量)備份)。
  - 備份的資料需定期做資料回復測試，以確認備份資料的可用性。

資訊儲存媒體的管理

- 儲存媒體的管理
  - 制訂儲存媒體(如：磁帶、磁片、光碟以及列印報告)的管理方法。
  - 明確記錄所有的管理步驟和授權級別。
- 儲存媒體的報廢
  - 具敏感資訊的媒體應該進行安全保險的保存和處置。
  - 安全收集和報廢所有媒體。
  - 謹選具有經驗及技術的合格合約商。
  - 儘可能記錄敏感資料的報廢，並保留稽核追蹤。
- 儲存媒體的運送安全
  - 使用可靠的傳輸工具或投遞人。
  - 包裝應可保護不受運輸過程中事故造成損壞。
  - 依需要採取特殊的控制措施以保護敏感資料免遭非法公開或修改。

資通安全法令

資通安全相關法令

- 國家機密保護法
- 電子簽章法
- 刑法(防駭條款)
- 電腦處理個人資料保護法
- 檔案法
- 著作權法
- 行政院及所屬各機關資訊安全管理要點
- 機關公文電子交換作業辦法
- 智慧財產權 Intellectual Property Rights (IPR)

案例一

- **案例描述** (資料來源:教育部網站)
- 王小浩是上一波「網路泡沫化」的犧牲者，在網路幻夢破滅後，王小浩在一夕之間成了無業遊民。
- 由於沉重的經濟壓力，王小浩被迫鋌而走險，他在網路上架設一個與國內知名的A銀行網站首頁完全相同的網頁，並以該銀行名義，發出數十萬封偽造的電子郵件，該郵件標題為「銀行系統轉換，重新登錄」，要求該銀行的網路銀行用戶，點選該郵件上的網頁鏈結，進行網路銀行帳戶號碼與個人密碼的重新確認。
- 黎小芬是上述A銀行網路銀行的用戶，她收到上述的電子郵件就依照其上的指示進行，發現所鏈結的網頁確實是與A銀行的網站首頁一模一樣，因此不疑有他，便在該網頁上登錄了自己的銀行帳戶號碼與個人密碼，王小浩利用騙得的帳號與密碼，將黎小芬的帳戶餘額10萬元，轉帳至自己所設的一個銀行人頭帳戶中。隔天黎小芬發現後，她馬上打電話與該銀行聯繫，並且向警方報案處理。

- 適用法條
  - 在網路上架設與A銀行網站首頁完全相同的網頁，並以該銀行的名義，發出偽造的電子郵件，已觸犯刑法第210條之「**偽造私文書罪**」。
  - 利用騙得的網路銀行帳戶號碼與個人密碼，入侵受害者在A銀行的網路銀行帳戶，已觸犯刑法第358條之「**無故入侵電腦罪**」。
  - 將受害者帳戶存款轉走之行為觸犯刑法第339-3條之「**電腦詐欺罪**」

案例二

- **案例描述** (資料來源:2007/02/10 工商時報)
- 國內多家金融投資顧問公司，**遭駭客入侵破解通行碼**，將客戶個資及投顧研究分析結果竊走，業者近一年來損失超過三億元。刑事局偵九隊昨偵破此一地下投顧犯罪集團，將主嫌陳慶興逮捕到案，刑事局呼籲金融、證券公司應加強電腦資安，特別是**系統帳號、密碼不宜明文儲存於網路主機，以防駭客入侵**，損害客戶及公司權益。

- 適用法條
  - 觸犯刑法第358條「**無故入侵電腦罪**」。
  - 觸犯刑法第359條「**無故取得、刪除或變更他人電磁紀錄罪**」。
  - 違反證券投資信託及顧問法。

案例三

- **案例描述** (資料來源:2007/08/18 蘋果日報)
- 小米今年十九歲，是剛要升大二的女生，最喜歡的休閒活動就是看韓劇，因為電視播的進度太慢，乾脆去夜市買整套ＤＶＤ回來看。
  由於正版太貴，便選擇便宜的盜版片，買回家後才一個禮拜便看完了，意猶未盡的我，前後買了六部韓劇，我靈機一動，想把看過的ＤＶＤ上網拍賣，就可以再去買新的。 於是，我以買來的七折價網拍，並標明可面交，三天後有買家出價競標，三部韓劇全由同一買家買下，我們約在捷運站出口交易，交易當天，我依約到達。十分鐘後，一名中年男子前來和我攀談，問我是不是韓劇ＤＶＤ賣家，我點頭示意後，他便表明警察身分，旁邊也出現另名穿制服警員，表示有人檢舉我在**網路販賣盜版光碟**，依法須將我帶回做筆錄，這時我才知自己犯法，但已來不及了。
- 適用法條
  - 賣家行為已違反「著作權法」可處3年以下有期徒刑、拘役，或併科50萬元以下罰金。

妨害電腦使用罪簡介

- 隨著資訊科技快速發展，網際網路應用日益普及與多元，除了帶給我們許多生活上的便利，但也衍生一些資通安全問題，特別是網路犯罪行為已有增多趨勢。
- 網路犯罪行為大約可歸類下列三種
  - 以網路作為犯罪工具–網路詐欺、網路恐嚇等
  - 以網路作為攻擊標的–竄改檔案、阻斷式服務攻擊、駭客入侵、電腦病毒等。
  - 以網路作為犯罪場所－如色情、誹謗、賭博等
- 為避免電腦犯罪與維護網路秩序，特於刑法中設立相關法令條文以為管理-**刑法第36章**「妨害電腦使用罪」章。

妨害電腦使用罪主要內容

- **第358條 無故入侵電腦罪**
  - 無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
  - 本條主要目的為遏止駭客入侵行為。
- **第359條 無故取得、刪除或變更他人電磁紀錄罪**
  - 無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
  - 本條主要目的為確保電腦內部電磁紀錄安全。
- **第360條 無故干擾電腦系統罪**
  - 無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
  - 本條主要目的為維護電腦及網路運作正常。

妨害電腦使用罪主要內容

- **第361條 對公務機關犯罪之加重**
  - 對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
  - 本條主要目的為確保國家安全。
- **第362條 製作供犯罪程式罪**
  - 製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
  - 本條主要目的為防止犯罪工具之利用與擴散。
- **第363條 告訴乃論**
  - 第三百五十八條至第三百六十條之罪，須告訴乃論。
  - 本條主要目的為集中司法資源對抗重大犯罪。

電腦處理個人資料保護法說明(1)

- 立法目的
  - 對公務與非公務機關蒐集、處理、與利用個人資料的情形，加以明文規範。
  - 避免個人**人格權**（隱私權）遭受侵害，促進個人資料之合理利用，特此制定電腦處理個人資料保護法。
- 保護客體
  - 本法保護客體限於**經電腦處理的個人資料**。
  - 受本法保護之個人資料以**現仍生存之自然人為限**，已死亡之自然人與法人，不受本法之規範。
  - 個人資料包含:自然人之姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社交活動、及其他**足以識別該個人之資料**。

電腦處理個人資料保護法說明(2)

- **適用主體**
  - 本法規範的對象有公務機關及非公務機關。
  - 公務機關係指依法行使公權力之中央或地方機關。
  - 非公務機關係指以下所列之事業、團體或個人。
    - 徵信業、以蒐集或電腦處理個人資料為主要業務之團體或個人
    - 醫院、學校、電信業、金融業、證券業、保險業、大眾傳播業
    - 其他經法務部會同中央目的事業主管機關指定之事業、團體或個人
  - 受公務機關或非公務機關委託處理資料之團體或個人，於本法適用範圍內，其處理資料之人，**視同委託機關之人**。

電腦處理個人資料保護法說明(3)

- 機關對個人資料之蒐集或利用的原則
  - 應尊重當事人之權益，依誠實及信用方法為之。
  - 不得逾越特定目的之必要範圍，以確保當事人權益，避免人格權受到侵害。
- 揭露個人資料，當事人是主要關鍵人物，當事人本身需審慎決定何者為提供給公務與非公務機關的必要個人資料。

電腦處理個人資料保護法修訂草案

- 修法背景
  - 法務部為因應急速變遷之社會環境，特別彙整國內學界與實務界的相關修法建議，並參考其他國家之個人資料保護相關法令來針對本法進行修訂。
- 修訂草案共有55條，並將本法名稱修訂為「個人資料保護法」。
- 草案修正方向
  - 擴大保護客體
  - 普遍適用主體
  - 增修行為規範
  - 強化行政監督
  - 妥適調整罰則
  - 促進民眾參與

電腦處理個人資料保護法修訂草案

- **修法重點說明**
  - **將買賣個人資料行為從告訴乃論罪修改為公訴罪，並提高刑責，最高為五年有期徒刑。**
    - 寄廣告信、垃圾郵件將觸法，未經個人同意，網路公司或個體戶大舉販賣蒐集的大筆電子郵件信箱供寄發垃圾郵件等行為，均將觸犯本法，檢警接獲檢舉後必須主動追查。
    - 若是公務員涉案，依法得加重其刑二分之一，最重可處七年半徒刑，與刑責已接近涉及貪瀆案。
- **重罰意圖營利而違法的行為**，修訂草案大幅加重「意圖營利而違法蒐集、利用或盜賣個人資料者」的刑責，由原本二年以下徒刑，提高為五年以下徒刑，且併科由原先四萬元大幅提高為五百萬元罰金。

簡報完畢，敬請指教。