國立中央大學電子計算機中心
「資訊安全管理系統顧問服務暨驗證範圍擴大案」

資安法令宣導及案例分析

專案經理：吳昭儀 經理

財團法人中華民國國家資訊基本建設產業發展協進會

課程大綱

- 資訊安全之概念說明
- ISMS/ISO27001簡介
- 資訊安全相關法律與安全倫理
- 案例說明與案例檢討
- 資安相關注意事項

課程大綱

- 資訊安全之概念說明
- ISMS/ISO27001簡介
- 資訊安全相關法律與安全倫理
- 案例說明與案例檢討
- 資安相關注意事項

資訊安全的最大威脅??→人員安全

- 根據Datapro Research Corporation的資安調查，約有5成的資安事件是由人為失誤所造成，加上離職員工或內部犯罪所佔1成，人為因素造成資安事件所佔的比例高達6成

資料來源:資安人 2006/9/8

什麼是資訊？

- 資訊對組織而言就是一種資產，和其他重要的營運資產一樣有價值，因此需要持續給予妥善保護
- 資產就是組織直接賦予價值，且需要受到保護的人、事、物

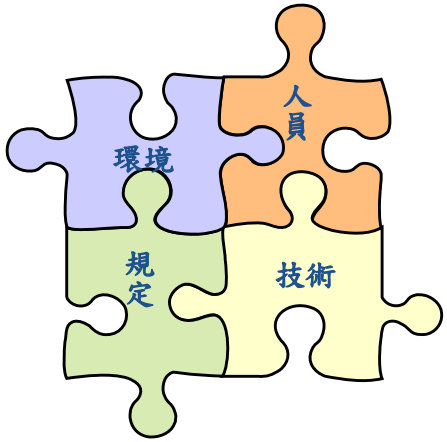
資訊安全管理制度為何

- 資訊安全管理制度 (Information Security Management System, ISMS)

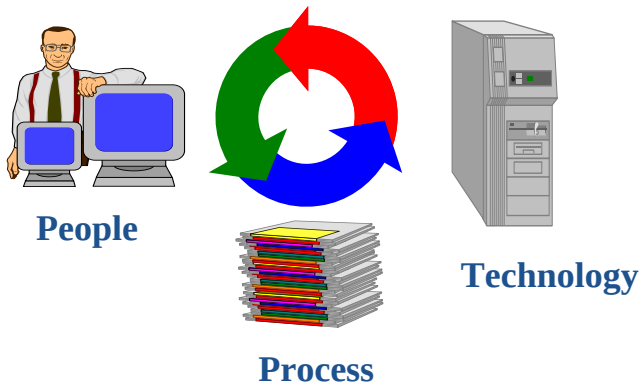
"The Information security management system is that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, maintain and improve information security"

資訊安全範圍

- 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『人員』



資訊安全管理重點



資訊安全三大原則

- 機密性(Confidentiality)：
  確保只有經授權的人才可以取得資訊，避免資訊洩露。
- 完整性(Integrity)：
  確保資訊不受未經授權的竄改與資訊處理方法的正確性。
- 可用性(Availability)：
  確保經授權的使用者，在需要時可以取得資訊，並使用相關資產。

課程大綱

- 資訊安全之概念說明
- ISMS/ISO27001簡介
- 資訊安全相關法律與安全倫理
- 案例說明與案例檢討
- 資安相關注意事項

ISO27001過去與現在

1995年發生了什麼大事?

- **BS7799標準更新之歷史：**
  - 1995:英國公佈BS7799 Part I
  - 1998:英國公佈BS7799 Part II
  - 1999:英國公佈新版BS7799 Part I、Part II
  - 2000:ISO通過成為ISO/IEC 17799 Part I
  - 2002:BS7799:2-2002 -資訊安全管理系統驗證規範
  - 2005: ISO/IEC 17799:2005
  - 2005: ISO27001
- **BS7799:2-2005在10月15日成為國際標準 ISO27001**

ISO27001驗證全球推廣狀況

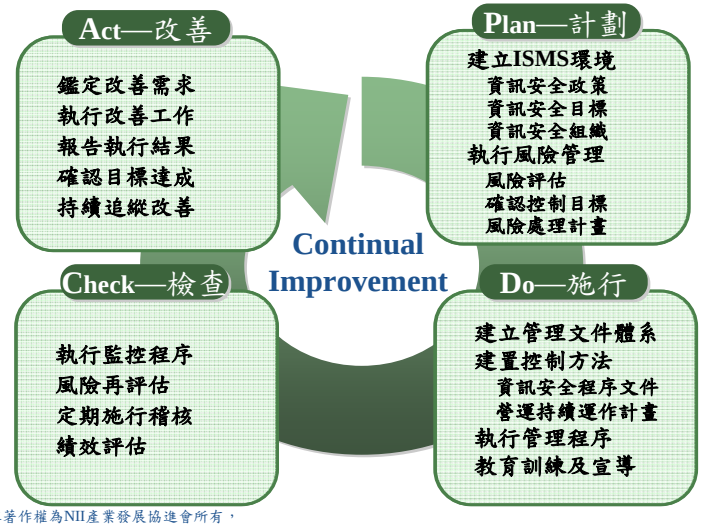
- 在政府帶動下，許多電信、金融與資訊服務，為能取得客戶信任，紛紛推動ISMS的建置
- 在法規要求以及客戶期望下，推行資訊安全管理制度已成為組織永續經營之必要工作

Top 10

日本	3273 *
印度	477
英國	401
臺灣	331
中國	205
德國	120
韓國	102
美國	95
捷克	82
匈牙利	65
Total	**5822**

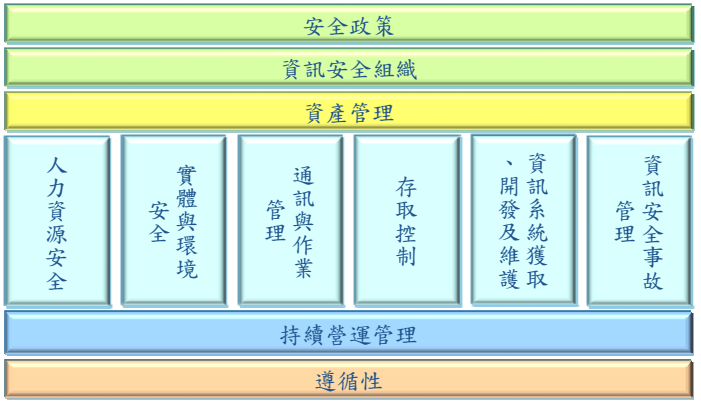
資料來源：http://www.iso27001certificates.com/ As of 2009/11

PDCA模型之應用



ISO27001涵蓋之內容

11 個領域、 39 個控制目標、 133 個控制要點



課程大綱

- 資訊安全之概念說明
- ISMS/ISO27001簡介
- 資訊安全相關法律與安全倫理
- 案例說明與案例檢討
- 資安相關注意事項

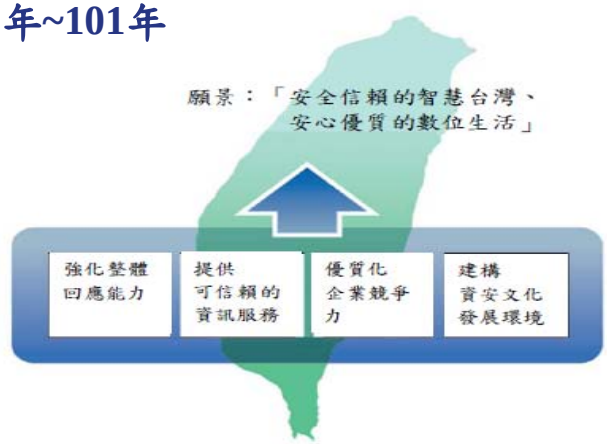
政府機關(構)資訊安全責任等級分級作業施行計畫 —各類資安系統等級應執行之工作事項

作業名稱 / 內容 / 等級	防護縱深	ISMS 推動作業	稽核方式	資安教育訓練(一般主管、資訊人員、資安人員、一般使用者)	專業證照	檢測機關網站安全弱點
A 級	NSOC 直接防護/自建 SOC、IDS、防火牆、防毒	通過第三者認証	每年至少執行二次內稽	每年至少（3,6,18,3 小時）	維持至少 2 張資安專業證照	每年兩次
B 級	SOC (Optional)、IDS、防火牆防毒、郵件過濾裝置	通過第三者認証(100 年)	每年至少執行一次內稽	每年至少(3,6,16,3 小時)	維持至少 1 張資安專業證照	每年一次
C 級	防火牆、防毒、郵件過濾裝置	自行成立推動小組規劃作業	自我檢視	每年至少(2,6,12,3 小時)	資安專業訓練	每年一次
D 級	防火牆、防毒、郵件過濾裝置	推動 ISMS 觀念宣導	自我檢視	每年至少(1,4,8,2 小時)	資安專業訓練	每年一次

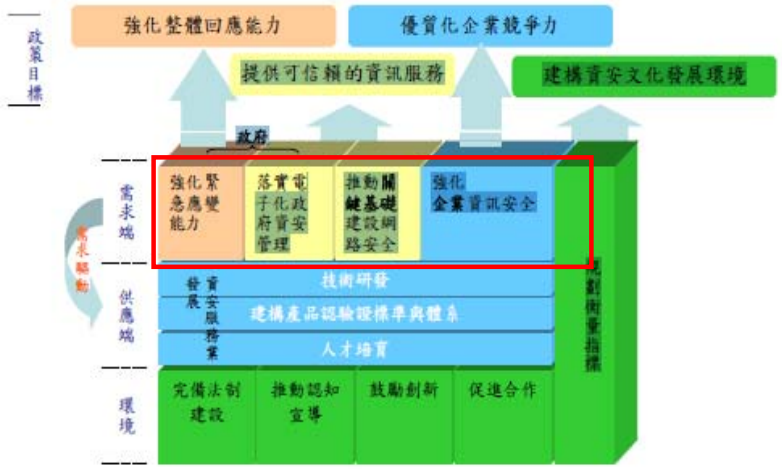
中央大學

98~101資通安全推動計劃

98年~101年



資通安全推動計劃－發展藍圖



98~101資通安全推動計劃－目標

1. 強化整體回應能力
   當重大資安事件發生時，必須具備能在有限的時間內，採取緊急應變行動的能力，方能使災害損失降至可接受的程度，並確保核心業務的持續運作。
2. 提供可信賴的資訊服務
   高度資訊化社會，民眾對於政府與關鍵基礎建設的最基本期待在於兩者所提供的資訊服務是可以讓人安心且可信賴的。
3. 優質化企業競爭力
   透過資安來為組織的核心業務創造價值，並協助企業達成未來的競爭優勢，亦　為推動本方案的目標之一。
4. 建構資安文化發展環境
   a.推動「個人資料保護法」儘速完成立法
   b.提升全民資安認知
   c.資安關鍵指標的量化資訊、定性分析，可概略瞭解我國資安政策發展狀況、實施成效及趨勢。

資通安全相關法規

- 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
- 機關公文電子交換作業辦法
- 智慧財產權 Intellectual Property Rights (IPR)

很多法令在法規資料庫可循!!~

電腦犯罪

- 電腦犯罪向來有廣義與狹義二者的分別，廣義的電腦犯罪指凡犯罪之工具或過程牽涉到電腦或網路，即為電腦犯罪，狹義之電腦犯罪則專指以電腦或網路為攻擊對象之犯罪。由於廣義的電腦犯罪，我國刑法原本即有相關處罰之規定，無須重複規範，但就刑法原本並無規範之狹義的電腦犯罪，便於 民國九十二年六月二十五日 修正我國刑法，新增刑法第三十六章「妨害電腦使用罪」，本犯罪所保護者，除個人之法益外，尚包括社會安全法益。
- 內政部警政署刑事警察局下設偵查第九隊，是國內電腦犯罪的主要偵防單位，該隊前身為電腦犯罪偵防小組，自民國八十五年成立以來，該隊所查獲的案件已逾百件，綜觀電腦犯罪案件，有以下的特性：
  - 散布迅速：網際網路具有無遠弗居、迅速廣泛散布的特性，其影響力與破壞力極大。
  - 身分易藏：網際網路的來源網址可以假造，網路犯罪者經常假冒他人身份，因此極難追查其真實身份。
  - 證據有限：電腦犯罪沒有現場、兇刀、血跡、槍彈、血衣等實体的證據，網路犯罪留下的僅有電磁紀錄，並非如指紋、DNA等有個化性證據，如何提升電磁紀錄的證明力，實為一大挑戰。
  - 毀證容易：網路犯罪非但證據有限，而且這些證據十分容易毀滅。例如，電腦內部帳冊、名冊等不法資料，只要輕按刪除鍵或執行格式化指令，即能於瞬間毀滅。
  - 修法困難：民國八十六年十月立法院曾經針對電腦犯罪通過修正刑法條文計八條。然而電腦科技日新月異，已不敷防制各種新興電腦犯罪之所需，網路科技帶來的新問題，往往令立法者追趕不及，故於 民國九十二年六月二十五日 再次修正我國刑法，新增刑法第三十六章「妨害電腦使用罪」。
  - 跨國管轄：網路世界無國界，網路犯罪的來源經常發生在國外，這也造成偵辦網路犯罪，具有跨國管轄的特性。
  - 偵查不易：以上幾個特性，致使網路犯罪不易偵查。同時，各國法律與實務對於某些行為是否違法的判斷標準不同，例如賭博或色情的認定，也使得跨國性網站的非法行為，在偵查上更增困擾不易偵辦。

網路犯罪

- 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
  - 以網路作為犯罪場所–如色情、誹謗、賭博等
  - 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
- 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-刑法第三六章妨害電腦使用罪章

妨害電腦使用罪章主要內容

- **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**

妨害電腦使用罪章主要內容(續)

- **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**

其他相關法令

❑網路色情：（如登載色情圖片）可能觸犯的法律

刑法：第二百三十五條(散佈猥褻文書罪)

- ◆散布、播送或販賣猥褻之文字、圖畫、聲音、影像或其他物品，或公然陳列，或以他法供人觀覽、聽聞者，處二年以下有期徒刑、拘役或科或併科三萬元以下罰金。
- ◆意圖散布、播送、販賣而製造、持有前項文字、圖畫、聲音、影像及其附著物或其他物品者，亦同。

刑法：第二百三十一條

- ◆意圖使男女與他人為性交或猥褻之行為，而引誘、容留或媒介以營利者，處五年以下有期徒刑，得併科十萬元以下罰金。以詐術犯之者，亦同。

兒童及少年性交易防制條例：第二十三條（雛妓）

- ◆引誘、容留、媒介、協助、或以他法，使未滿十八歲之人為性交易者，處一年以上七年以下有期徒刑，得併科新臺幣一百萬元以下罰金。
- ◆意圖營利而犯前項之罪者，處三年以上十年以下有期徒刑，應併科新臺幣五百萬元以下罰金。

其他相關法令(續)

❑網路恐嚇：（如以Email寄發恐嚇信）可能觸犯的法律

刑法：第三百四十六條（恐嚇罪）

❑網路毀謗：（如在網站的網頁、留言版或BBS站上，公布或張貼足以妨害他人名譽的行為）可能觸犯的法律

刑法：第三百零九條、第三百一十條(公然侮辱罪、毀謗罪)

- ◆ 第三百零九條：公然侮辱人者，處拘役或三百元以下罰金。以強暴犯前項之罪者，處一年以下有期徒刑、拘役或五百元以下罰金。
- ◆ 第三百一十條：
  - ◆意圖散布於眾，而指摘或傳述足以毀損他人名譽之事者，為誹謗罪，處一年以下有期徒刑、拘役或五百元以下罰金。
  - ◆散布文字、圖畫犯前項之罪者，處二年以下有期徒刑、拘役或一千元以下罰金。
  - ◆對於所誹謗之事，能證明其為真實者，不罰。但涉於私德而與公共利益無關者，不在此限。

其他相關法令(續)

刑法第315條

❑ 竊視竊聽竊錄罪

無故利用工具或設備窺視、竊聽他人非公開之活動、言論或談話者

無故以錄音、照相、錄影或電磁記錄竊錄他人非公開之活動、言論或談話者

三年以下有期徒刑

❑ 便利竊視竊聽竊錄罪

意圖營利供給場所、工具或設備，便利他人為前項之行為者

意圖散布、播送、販賣而有竊錄等行為

明知為竊錄內容而製造、散步、播送或販賣

處罰未遂之五年以下有期徒刑

❑ 洩漏電腦或相關設備秘密罪

無故洩漏因利用電腦或其他相關設備知悉或持有他人之秘密者

二年以下有期徒刑

電腦處理個人資料保護法修訂草案

- 名稱將修訂為「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

現行法與修正草案對照表 (1/3)

項　　目	現 行 法	修正草案
增修行為規範 (書面同意)	無規範	特定目的外利用個資需當事人書面同意方式
增修行為規範 (拒絕接受行銷權利)	無特別規定	首次行銷應免費提供當事人表示拒絕之方式
強化行政監督	無規範	中央目的事業主管機關或直轄市、縣(市)政府，發現違反本法規定時，得派員進入檢查，並採取必要處分
妥適調整罰則 (刑罰規定)	僅處罰意圖營利侵害個資隱私權益者，刑期最高2年以下	違反規定雖未意圖營利，刑期最高2年以下 意圖營利者加重其刑最高5年以下

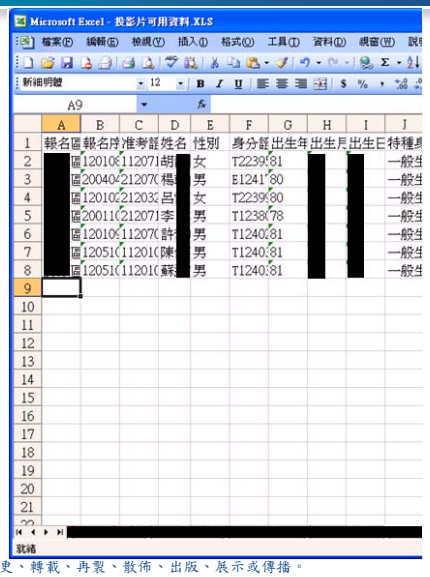
現行法與修正草案對照表 (2/3)

項　　目	現 行 法	修正草案
增修行為規範 (書面同意)	無規範	特定目的外利用個資需當事人書面同意方式
增修行為規範 (拒絕接受行銷權利)	無特別規定	首次行銷應免費提供當事人表示拒絕之方式
強化行政監督	無規範	中央目的事業主管機關或直轄市、縣(市)政府，發現違反本法規定時，得派員進入檢查，並採取必要處分
妥適調整罰則 (刑罰規定)	僅處罰意圖營利侵害個資隱私權益者，刑期最高2年以下	違反規定雖未意圖營利，刑期最高2年以下 意圖營利者加重其刑最高5年以下

現行法與修正草案對照表 (2/3)

項　　目	現 行 法	修正草案
妥適調整罰則 (民事損害賠償)	每人每一事件2 萬元以上，10萬元以下同一原因事實最高2000萬元	每人每一事件5000元以上，10萬元以下同一原因事實最高5000萬元(待定)
妥適調整罰則 (機關代表人同受罰則)	無規範	企業代表人、管理人對違反規定之行為，除能證明已盡防止義務外，應受同一額度罰鍰之處罰
妥適調整罰則 (主動通知安全責任)	無規範	當蒐集之個資有被竊取、洩漏、竄改或侵害時，應迅速通知當事人，隱匿不報者，除限期改正外，按次罰以2萬元以上，20萬元以下
促進民眾參與	無規範	符合規定之公益團體可代替當事人提起團體訴訟

提醒您，您是否真的沒有外洩個資？



個人資料管理重點(一)

- ◆蒐集
  - ✓蒐集個人資料之理由、方法與告知義務
  - ✓確認個人資料之正確性及內容是否為法律定義之「得以直接或間接方式識別該個人之資料」
- ◆使用
  - ✓符合法律之使用規範
  - ✓符合組織政策之內部使用規範(例如：交叉行銷)
- ◆存取
  - ✓存取個人資料之權限管理
  - ✓委外或外包廠商之資訊安全管理

個人資料管理重點(二)

- ◆傳輸
  - ✓個人資料傳輸過程中之安全(加密或安全網路)
- ◆儲存
- ◆清除
  - ✓個人資料新增及修改之作業程序
  - ✓存放個人資料場所及設備之安全管理
  - ✓備份或歸檔後之資料安全
  - ✓個人資料刪除或報廢之安全處理程序
- ◆其它
  - ✓客訴、法律糾紛、懲處程序

保護個人資料小提醒

- ■員工資料亦受法律保護
- ■所有調閱活動應依照標準作業程序進行
- ■不在電話裡隨便透露個人資料
- ■非信任之網站，勿隨意留下個人資料
- ■以碎紙機銷毀各式帳單、收據、信件、藥單等
- ■不點選不明人士傳送的網址
- ■提防偽裝之網頁、電子報與信件
- ■不委託他人代辦貸款及信用卡
- ■影印文件交付時註明用途(表示不適用於其他用途)

其他網路常見犯罪類型

- 妨害風化
- 網路竊盜
- 網路詐欺
- 偽造文書
- 公然侮辱、誹謗
- 煽惑他人犯罪

妨害風化

- 網路援交
  - 刊登網路援助交際訊息
  - 違反兒童及少年性交易防制條例第29條之「以電腦網路散布使人為性交易訊息罪」，最重可處有期徒刑五年
- 貼圖、以電子郵件散布色情圖片
  - 圖片若為未滿十八歲之人：兒童及少年性交易防制條例第28條之「散布未滿十八歲之人性交或猥褻圖片罪」，最重可處有期徒刑三年
  - 圖片若已滿十八歲之人：刑法第235條第一項：散布猥褻圖片罪，最重可處有期徒刑二年
- 販賣色情光碟
  - 同刑法第235條

網路竊盜及詐欺

- 線上遊戲寶物、天幣竊盜案件，以竊盜罪移送。
  - 刑法第359條：「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」最重可處有期徒刑五年
- 網路拍賣交易詐欺：刑法第339條，最重可處有期徒刑五年
- 不正當利用電腦取財：以不正當方法製作財產之變更，而取得他人財產者，刑法第339條之三第一項，最重可處有期徒刑七年

偽造文書

- 冒用他人名義刊登援交訊息：為偽造文書，刑法第210條，最重可處有期徒刑五年
- 上網竄改他人資料：電腦處理個人資料保護法第34條，最重可處有期徒刑三年

公然侮辱、誹謗

- 意圖散布於公眾，足以毀損他人名譽之事者：刑法第309條之公然侮辱罪與第310條之誹謗罪，公然侮辱罪可處拘役或三百元以下罰金，如果以暴力公然侮辱人者，可處一年以下有期徒刑、拘役或五百元以下罰金
  - 政大學生在 BBS 上罵老師事件
  - 某大學生因為不滿某教授之教學及考試方式，在校園的網際網路上指責某甲教授如何抄襲學生的研究報告

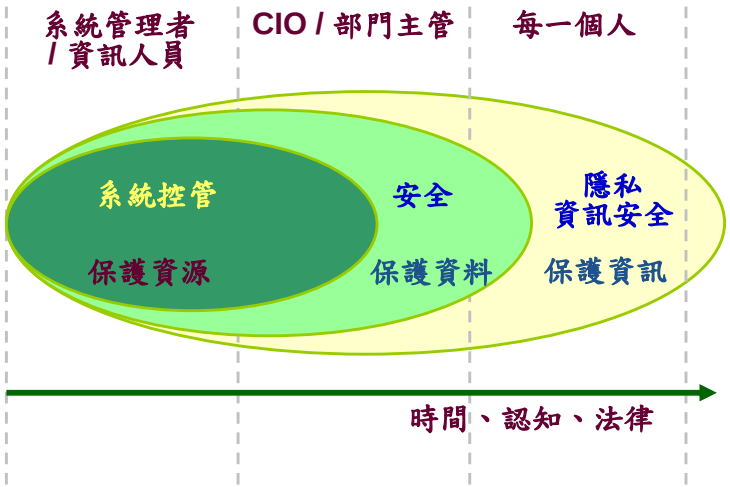
更新日期:2008/03/20 04:34 陳佳鑫台北報導 **在網拍評價意見欄留言「不要臉」遭起訴…**

網路買賣評價留言要注意！吳姓男子向網路王姓買家購買商品後互留負面評價結惡，吳遂在王的露天拍賣網站內評價意見欄內留下「你真的很不要臉」等文字。檢方認為已足以減損王某商譽，昨天依妨害名譽罪起訴王某。

煽惑他人犯罪

- 刑法第153條第一款之「以文字煽惑他人犯罪」罪，最重可處有期徒刑二年
  - 「軍火教父」網站以文字及圖片內容介紹「貝瑞塔」槍枝廠牌、規格、性能、配件、裝填子彈數、相片及販賣價格、訂購方法、劃撥帳號、交槍時間及交槍方法等資訊。經台北地院以被告涉嫌煽惑他人違背我國之槍砲彈藥刀械管理條例法律，造成網路使用者有進而透過該管道取得槍枝而觸法之虞，予以判刑

資訊安全　人人有責



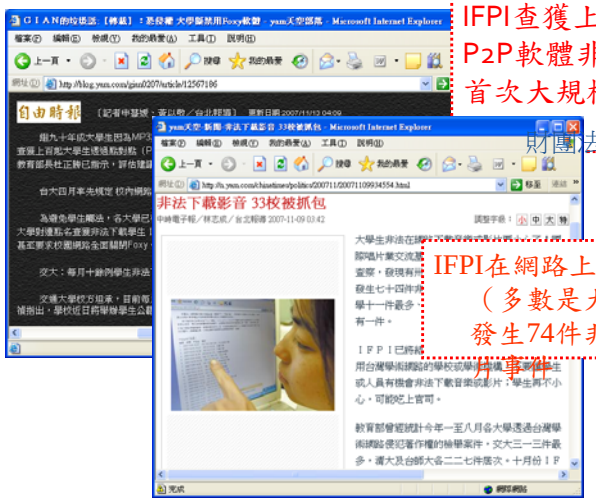
課程大綱

- 資訊安全之概念說明
- ISMS/ISO27001簡介
- 資訊安全相關法律與安全倫理
- 案例說明與案例檢討
- 資安相關注意事項

- 拷貝正版光碟…？
- 提供MP3下載…？
- 複製他人著作…？

您確定也沒有下列行為嗎？

P2P軟體下載音樂、影音

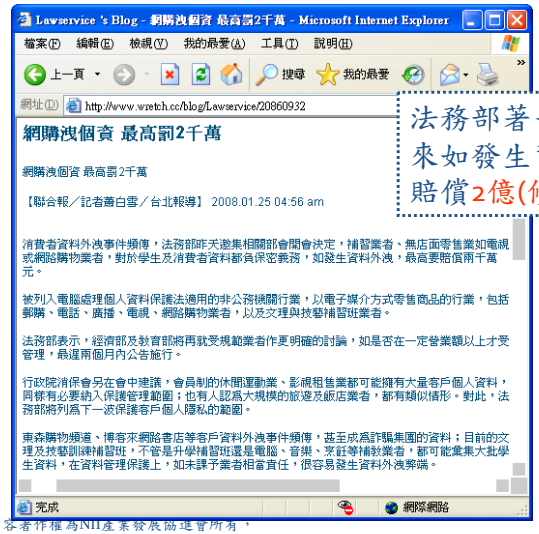


IFPI查獲上百位大學生透過P2P軟體非法下載音樂，可能首次大規模對學生提告開

財團法人國際唱片業交流基金會

IFPI在網路上查察，發現有33校（多數是大學）、學術機構發生74件非法下載音樂或影片事件

洩個人資料將重罰2億(新法修訂中)



法務部著手修法(個資法)，未來如發生資料外洩，最高要賠償2億(修法中)！

案例：業界的個資外洩

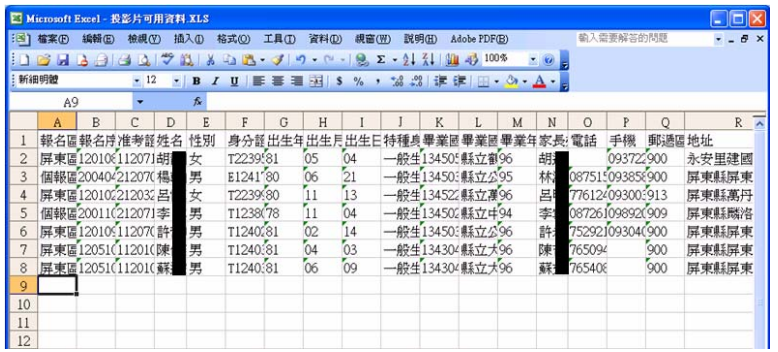
遭罰200萬；
停卡處分至少損失5,000多萬。

提醒您，真的沒有外洩個資？

搜尋網路上的公開個資

在入口網站上使用某些關鍵字搜尋…

詳細的各項個人與家庭資料



課程大綱

- 資安相關注意事項

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。
  - 使用密碼保護的螢幕保護程式。
  - 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

網際網路管理要求

- 與網路服務的連接如果不安全，就會影響整個組織。
- 在敏感或重要業務應用或與處於高風險區域（如無法管理與控制的公共或外部區域）使用網路連接時，安全控制措施非常重要。
- 制定網路服務的使用政策要包含：
  - 允許存取的網路和網路服務。
  - 確定存取網路和哪種網路服務的授權程序。
  - 保護網路連接和服務存取的管理控制措施和程序。
  - 與存取控制政策取得一致性

公共區域無線上網安全性

- 選擇有加密功能的無線基地台
- 使用認證機制對使用人員做好身份管理
- 牽涉到高度機密之相關資訊，避免使用無線傳輸。

(資料來源：i-security-輕鬆學資安/資安小撇步 http://www.i-security.tw)

公共電腦使用安全

- 登入網路服務動作的保護
  - 使用公共電腦時，尤其要注意避免勾選任何的記住帳號或密碼的功能
- 使用公共電腦後，關閉網頁瀏覽器，清除個人相關資料
  - 清除網頁瀏覽記錄/網站上所留下的個人資料/電腦中的**cookie**/隱私權記錄/密碼記錄
- 盡量避免利用公共電腦上網處理重要或私密事務
- 特別注意坐在或站在你旁邊的人
- 更換密碼的頻率要更高

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

- 使用者
  - 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

- 電腦病毒簡易處理步驟
  - 將中毒電腦離線網路作業
  - 設法使防毒軟體運作：
  - 以防毒軟體執行病毒的掃瞄與清除
  - 若防毒軟體無法正常執行，則執行以下替代方案：
    - 手動掃毒：
    - 使用未受病毒感染健康的電腦之防毒軟體來進行問題硬碟掃毒作業。
    - 透過免費線上掃毒資源，在不危害狀況下連線網路進行。

    http://housecall.trendmicro.com/
    http://www.symantec.com.tw/
  - 受感染的檔案並執行隔離或刪除動作
  - 未知病毒的處理方式：
    - 電腦病毒事件的通報，尋求資源協助。
    - 聯絡病毒軟體廠商協助。

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

- 間諜或廣告軟體的防範
  - 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， 例如Google Toolbar 。
  - 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
  - 使用反間諜軟體

刑事警察局惡意程式清除軟體「GK 1.0」
http://www.cib.gov.tw/news/news02_2.aspx?no=343

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
- 駭客入侵的簡易處理
  - 系統備份
  - 可能入侵途徑系統隔離
  - 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
  - 報告相關單位
  - 適時尋求協助

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

可攜式設備之安全管理要求

- 使用可攜式設備（如筆記型電腦、掌上型電腦、膝上型電腦和行動電話）時，應確保業務資訊不受損壞。
- 訂定可攜式設備連接網路的規則和公共場所中使用的指導說明，並提供適當保護連接網路的設施。
- 使用可攜式設備進行遠端存取時，必須先成功地進行身份識別和驗證並採用適當的存取控制機制。
- 在公共場所使用可攜式設備時應採用一定的保護措施，並防範被窺視，以避免儲存和處理的資訊遭到非法存取或洩密。
- 制定並即時更新用於防範惡意性軟體的程式。
- 準備對資訊備份的必要設施，並適當地保護備份的資訊，避免被盜或遺失。
- 應防止可攜式電腦化設備被盜，尤其是比如丟在汽車等其他交通工具、旅館、會議中心以及聚會場所內。
- 內含重要、敏感和/或關鍵業務資訊的設備不應無人看管。如果可能，應上鎖。應使用專用鎖來保障設備的安全。
- 進行可攜式設備的資安訓練，提高他們對可攜式設備可能帶來額外風險的防範意識，以及因應措施的認識。

資料備份

- 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 Ex.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

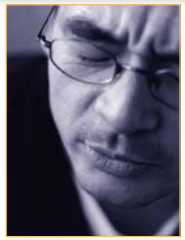
資訊儲存媒體的管理

- 儲存媒體的管理
  - 制定儲存媒體（如磁帶、磁片、盒式磁帶以及列印報告）的管理方法
  - 應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。
  - 包裝應該可以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保護敏感資料免遭非法公開或修改。

軟體管理

- 安全要求分析與規格
- 系統文件管理
- 系統測試資料的保護
- 程式源碼的存取控制與集中管理、版本控制
- 測試資料的保護
- 軟體變更控制程序
- 委外的軟體開發管理
- 技術脆弱性控制，如：Code review、滲透測試
- Shareware 與 freeware 管理

問題與討論



&