KPMG

INFORMATION TECHNOLOGY ADVISORY

台北市教育網路中心
資訊安全管理與個人資料保護宣導

安侯企業管理股份有限公司
中華民國98年12月

ADVISORY

AUDIT ▪ TAX ▪ ADVISORY

講師 – 謝昀澤（Jason Hsieh）

現職：
- 安侯企管KPMG 資訊科技諮詢服務部 協理
- 國立台灣科技大學 兼任講師
- 教育部TANet ISMS建置專案協同主持人
- 教育部96-99年提升校園資訊安全計畫協同主持人
- 教育部推動RFID校園安全計畫資安審議委員

專業資格：
- 國立交通大學資訊管理研究所碩士
- ISO 27001主導評審員訓練合格
- ISO 20000主導評審員訓練合格
- 國際認證電腦稽核師（CISA）
- 美國計算機技術協會（CompTIA）Security+認證合格
- Oracle 資料庫管理師（OCP）認證合格

資訊安全講授經驗 - 網路安全/防火牆安全系列課程兼任講座：
- 台灣大學 資管所
- 萬能科技大學資管所
- 人事行政局研習中心
- 金管會檢查局等5個單位

資訊安全講授經驗 - 資安技術訓練講師：
- 司法院
- 中央健保局
- 臺北市國稅局等18個單位

資訊安全講授經驗 - 網路安全研討會講師：
- CNET 、PCWEEK 、ITHOME 、IBM、資安人等30場

資訊安全實務經驗：
- ICBC、證交所、日月光集團、証券集保公司等18個單位 網路安全專案規劃與查核經驗
- 國家資通安全會報資訊安全專刊、 RUN PC雜誌資安診療室特約撰述
- 美商CA組合國際電腦公司 首席資訊安全顧問
- 荷商荷蘭銀行資訊管理部 副理

KPMG

課程大綱

- 網路應用的新機會
- 2010年校園資安管理的新挑戰
- 看新聞學資安-最新資安案例探討
- 個人電腦資安防護秘笈
- Q&A

資安迷思篇

網路應用的新機會

從圖書館，到親密互動的朋友

早期的網路，多數使用者僅能靜態點閱，被形容是一座「豐富的圖書館」

網路發表個人心得

現代的網路，多數使用者可以參與互動，被形容是一位「親密的朋友」

網路可以買美食

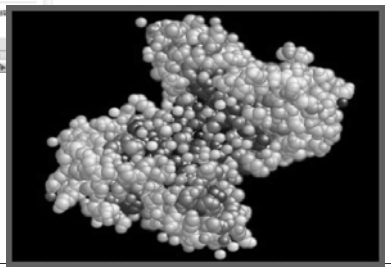
網路可以談戀愛

從英文到多國語言

從單機計算，到雲端運算

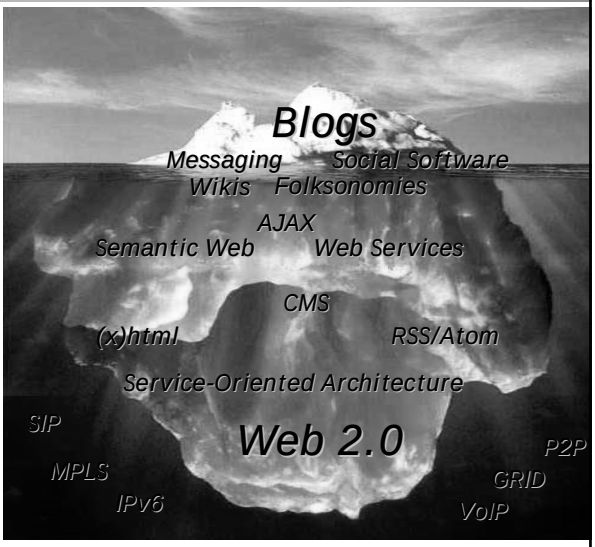
雲端運算範例: 利用你的空閒電腦研發抗癌藥物

絕大部分的電腦並沒有發揮它100%的效能. 即使你是上網打CS,處理影像, 上網找資料.而UD Agent即是一種軟體, 能使我們利用電腦閒置的時間,搜尋包圍癌細胞、並抑制其繁殖的分子,牛津大學化學系主任、國家癌症研究基金會英國辦公室主任理Graham Richards表示，分散式運算可能減少十幾年的新藥研發時間。



從觀看、參與互動到創造

性質	Web 1.0(從前)	Web 2.0(現在)
1.出發點	以資料為核心	以人為出發點
2.知識角度	將以前沒有放在網上的人類知識，通過商業的力量，放到網上去	將這些知識，通過每個用戶的瀏覽求知的力量，協同工作，把知識有機的組織起來，在這個過程中繼續將知識深化，並產生新的思想火花
3.內容產生者角度	主要以商業公司爲主體，將內容直接放置於網路上	以用戶爲主，以簡便隨意方式，通過blog/podcasting 方式把新內容往網上搬
4.交互性	•網站對用戶爲主	•加入P2P應用
5.技術上	進入門砍高	WEB用戶端化，各項技術越來越易用。



奉公守法夠了嗎?

2010年校園資安管理的新挑戰

傳統資安案例: 教育人員疑洩漏個人資料牟利

盜賣基測個資 主嫌求刑10年

2008/10/15【聯合報／記者楊濡嘉／高雄報導】

97年度國中基測學生資料遭盜賣案，多達496名被害學生提告，高雄地檢署檢察官劉河山昨天偵結，涉案的承包基測電腦作業的博暐公司實際負責人林正杰、許慧珠分別被求刑10年、9年；另有10名涉無償取得或提供學生資料的私立高中校長、主任、國中組長被處以緩起訴。

起訴書指出，林正杰（56歲）和許慧珠（47歲）是博暐圖書網路公司、大正資訊網路公司實際負責人，97年國立桃園高中受教育部指定辦理國中基測，由博暐得標負責基測各項電子作業，博掌握所有考生個資和測驗分數。

林、許與博暐公司人員呂錫恩、陳錫卿、葉適杰，今年4月複製學生個資和分數，分別以100萬元、180萬元、25萬元，賣學生個資給台北、高雄、桃園9家補習班，另依學校需求無償提供給桃園新興高中等7學校。林正杰在一名家長請託下，二度為參加基測的一名李姓學生更改分數，使這名男學生可以進入私立醒吾高中就讀，執行更改的博暐電腦工程師張煒翔（33歲）也被起訴。

檢警也查出案外案，以蒐集及販賣個人資料為業的男子吳茂德（59歲），利用擔任高雄縣田徑比賽裁判之便，與熟識的高雄縣前峰國中體育組長王逸森說好，更改前峰國中3名學生的田徑比賽成績，王則提供學校一年級學生資料給吳。王被處以緩起訴，吳被以背信、偽造文書起訴，檢察官求刑6年。間接向博暐購買到學生個資並轉賣的男子羅濟彰（43歲），被起訴且求刑5年。提供羅學生資料的新竹忠信高中一名黃姓主任則被緩起訴。

公務員借職務之便洩漏並販賣民眾資料可能觸犯之法條

（一）**貪污治罪條例第4條第1項第5款：**對於違背職務之行為，要求、期約或收受賄賂或其他不正利益者。處無期徒刑或十年以上有期徒刑，得併科新台幣一億元以下罰金。

（二）**貪污治罪條例第6條第1項第4款：**對於主管或監督之事務，明知違背法令，直接或間接圖自己或其他私人不法利益，因而獲得利益者。第5款：對於非主管或監督之事務，明知違背法令，利用職權機會或身分圖自己或其他私人不法利益，因而獲得利益者。處五年以上有期徒刑，得併科新臺幣三千萬元以下罰金。

（三）**刑法第132條（洩漏國防以外之密秘罪）：**公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處三年以下有期徒刑。因過失犯前項之罪者，處一年以下有期徒刑、拘役或三百元以下罰金。非公務員因職務或業務知悉或持有第一項之文書、圖畫、消息或物品，而洩漏或交付之者，處一年以下有期徒刑、拘役或三百元以下罰金。

（四）**電腦處理個人資料保護法第33條（意圖違反規定或限制命令罪）：**意圖營利違反第七條、第八條、第十八條、第十九條第一項、第二項、第二十三條之規定或依第二十四條所發布之限制命令，致生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣四萬元以下罰金。

公務員借職務之便洩漏並販賣民眾資料可能觸犯之法條(續)

（五）**電腦處理個人資料保護法第35條（公務員犯罪之加重處罰）：**公務員假借職務上之權力、機會或方法，犯前二條之罪者，加重其刑至二分之一。

（六）**公務員服務法第四條（保密義務）：**公務員有絕對保守政府機關機密之義務，對於機密事件無論是否主管事務，均不得洩漏，退職後亦同。

（七）**稅捐稽徵法第33條：**稅捐稽徵人員對於納稅義務人之財產、所得、營業及納稅等資料，除對下列人員及機關外，應絕對保守秘密，違者應予處分；觸犯刑法者，並應移送法院論罪：

一、納稅義務人本人或其繼承人。

二、納稅義務人授權代理人或辯護人。

三、稅捐稽徵機關。

四、監察機關。

五、受理有關稅務訴願、訴訟機關。

六、依法從事調查稅務案件之機關。

七、經財政部核定之機關與人員。

八、債權人已取得民事確定判決或其他執行名義者。

2010年校園機構資安管理的新挑戰

評比面向	AS IS	TO BE
個資法舉證責任	由受害者舉證資料持有機關之個人隱私保障缺失	由資料持有機關舉證已進行良善之民眾個資資料保護責任
個資法告訴乃論	告訴乃論	部分行為取消告訴乃論
個資法賠償內容	機關僅負有限的賠償責任	機關需承擔巨大的賠償責任
個資法範圍	公務機關等重要產業	所有行業都適用
資安通報	資料遺失沒有義務需通報	必須依據規定向主管機關與治安機關通報
惡意駭客	資訊系統破壞或入侵知識僅由少數駭客掌握	攻擊工具垂手可得，人人都可是駭客，24小時進行主動式無時差攻擊
民眾	僅注重教育的效率與品質	家長與師生皆開始具備個人資料保護與資訊安全意識，並非常重視個人資料安全
媒體	媒體暴料文化盛行	媒體針對教育機構的資訊保護作為，更加無孔不入的進行監視

誰在製造網路威脅

從顧客來的威脅

從網路狗仔隊來的威脅

隨處存在的網路攝影機

按一下影片開始播放

從賺外快者來的威脅

網路上的菸酒廣告近日成為網路駭客攻擊目標，駭客刪除廣告警語後，再向政府檢舉該則菸酒廣告未加註警語，藉機領取檢舉獎金，業者接到罰單後才驚覺網路廣告遭駭客入侵，轉向立委陳情。立委要求執法單位應先開勸導單再開罰，以免菸酒商無辜受罰。

從龜山島來的威脅

另類駭客-從龜山島轉進官網洩恨

一名女導遊，因屢次申請宜蘭龜山島觀光許可不成，竟入侵觀光局網站假官方名義，寄電郵取消其他業者登島資格；女子落網後表示，她入侵網站，發現幾乎是固定領隊和隊員申請通過，她懷疑觀光局包庇特定業者，才會心生不滿，取消同業許可出氣。

從空氣來的威脅

有線網路的設備可以利用線路找尋設備資訊，封包加密較完整，如果有人從線路中竊取資訊，至少還有軌跡可尋，無論是管理、安全、記錄資訊較為方便，然而無線網路的環境就複雜許多。

無線網路的安全問題是最令組織擔心的原因，由於無線電波摸不著，透過空氣傳遞訊號，只要架設發射訊號的儀器，無論在局內哪個節點，都能傳遞無線訊號，另外使用接收無線訊號的儀器，只要在訊號範圍內，就算在圍牆外，都能擷取訊號資訊，沒有線路可以依循，管理無線網路安全維護比有線網路更困難。

微型無線基地台(AP)

台灣政府機關面對的主要威脅來源

常見團體– 大陸

中國鷹盟ChinaEagle

http://www.chinaeagle.com/

最早成立之駭客團體

遍佈最廣

紅客聯盟CNHONKER

http://www.cnhonker.com/

中國紅客網路技術聯盟2000年成立

主導2001年5月1日中美駭客大戰

黑客聯盟CNHACKER

http://www.cnhacker.net/

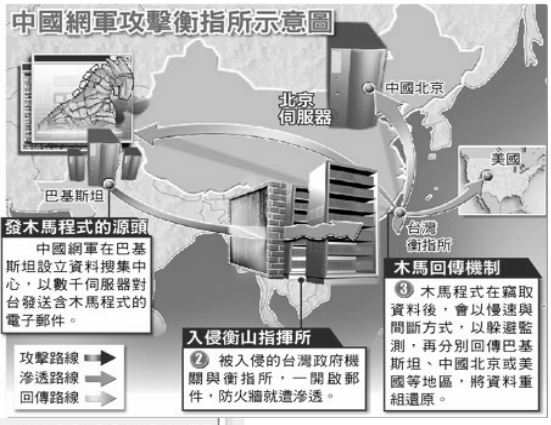
中國黑客聯盟2001年11月成立

中國網軍的最高機密

- **研發台灣政府專用的攻擊(惡意)程式**
- **惡意程式可以輕易閃躲防毒軟體**
- **惡意程式主要進行秘密的檔案竊取而非暴力破壞電腦**
- **台灣沒有真正的本土防毒軟體，病毒防治有空窗期**
- **利用人性弱點，誘騙台灣政府公務員「自願」被入侵**
  - 針對男性，利用情色、影片與破解程式軟體
  - 針對女性，利用HelloKitty等可愛程式
  - 針對公務員，利用國旅卡、養生等誘騙信件
  - 針對政黨機構，利用選舉內幕檔案等誘騙信件
- **建立網軍入侵捷徑1- 先入侵家用電腦，再感染辦公室(USB、家用電腦公用)**
- **建立網軍入侵捷徑2- 先入侵台商大陸廠房電腦，再……**

從對岸來的威脅

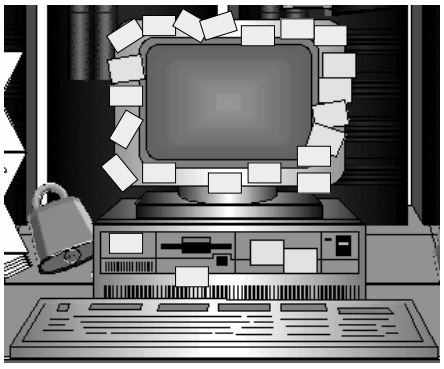
中國木馬破我軍中樞??? (2005/11/18)



從內部粗心員工來的威脅

- 不規避旁人，如重要資料或密碼的輸入。
- 不隨手關機。
- 隨時討論業務機密
- 使用者代碼隨便借給別人。
- 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!!



看新聞學資安(1)-
2006年的大學考試網站入侵事件

19歲駭客侵大考中心 盜百萬筆資料

案例分析

19歲駭客侵大考中心 盜百萬筆資料
警方偵破一起電腦駭客案，19歲的建中資優生蘇柏榕，不僅連續多年入侵大考中心、國中基測資料庫，盜拷上百萬筆考生資料，再以每次五到十五萬元的代價，賣給補習班，連總統府、台北悠遊卡系統等，都遭到他的入侵。

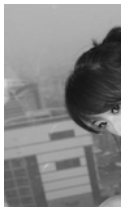
還好大考中心在清查後表示，考生的原始資料成績，沒有被篡改的跡象。(2005/4/26)

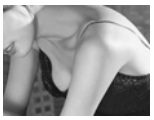
駭客的長相

被害苦主的長相

大考中心有三層的防火牆

使用規則匹配式演算





看新聞學資安(2)-

2007年CDC洩漏肺結核患者隱私事件

新便民系統上線?
肺結核患者病情，上Google免帳號即可查

二〇〇七年十一月十七日 星期六 農曆丁亥年十月初八日 A16·要聞

離譜疾管局 千人隱私曝光

開放性肺結核患者病情 上Google隨你查

肺結核患者隱私外洩狀況

洩漏時間	推估自今年9/1起，但衛生署說法為11/9日起，昨晚8時許已移除網頁
人數	推估全台25縣市，包括開放性肺結核患者（約1000多人）、多重抗藥性肺結核患者（約100多人）、超級抗藥性患者（不到10人）；截至昨晚計約1279人資料外洩
洩漏病患個人資訊內容	身分證字號、設籍縣市區域、最近就醫日、開護院所、病情資料（包括是否為多重抗藥性病人、是否參加都治計劃、衛生單位關懷天數、建檔日等）
洩漏方式	只要得知患者姓名上Google網站查詢，即可查到所有患者的個人及病情資料
協助管道	消基會（02）27001234；衛生署今天將公布協助專線

疾管局網站竟將全台千餘名開放性肺結核病患的個資公布。（翻攝網頁）

資料來源：衛生署疾病管制局、消基會

此

已觸《刑法》洩密罪

有心人利用難辭其咎

史上最劣

生病一千兩百七十九名患者的個人資料全部上網的離譜事！疾管局昨晚坦承將開放性肺結核病患的身分證字號、病情等全部公布上網，民眾只要透過98年度任何一名開放性肺結核病患姓名，即可查到全台灣所有患者的個人資料。學者專家批衛生署幫倒連法，「糟糕到難以置信」；消基會則呼籲所有必需與該會聯絡，將代患者打關說電話。

究竟是哪裡出了錯?

1. Google亂蒐集資料?
2. CDC沒有設防火牆?
3. CDC沒有弱點掃描?
4. 系統遭駭客入侵?

=>以上皆非

錯誤的程式設計+錯誤的資訊系統架構+未盡落實的上線流程

然後遇上強大的Google網頁扒取程式(Spider)

不巧又有個愛報料的記者

=>CDC Google Hacking

如何避免成為下一個Google Hacking 的受害者? (for 業務單位主管)

1. 分配少數人力經常在搜尋引擎(Google.Yahoo)上對業管相關系統進行檢索，檢查是否含有可能對系統造成危害的資訊。
2. 請確認在網頁上的敏感性資料存在之需求，考量要移除該目錄或使用密碼保護。
3. 若有需要，請對各業管系統維護廠商要求在網站根目錄建立搜尋引擎排除協定標準文字檔robot.txt，禁止Google的搜尋機器人「扒走」根目錄下的資料。
4. 如發現搜尋引擎所找到的內容是不適合出現的資訊，請透過線上表單通知Google，將該網頁的資訊從搜尋結果以及快取中移除。
5. 系統及網站上線或更新前，請確實檢查是否只有需要被公開的資訊能被看到。
6. 系統設計，請考量互動型態的必要性(查詢、論壇BBS、線上表單、留言版、上傳資料等)。一般而言，靜態與單向網頁，安全性高於多媒體互動式網頁。

更重要的是....

1. 注意! Google Hacking只是上千種網路威脅的一小類

2. 拒絕Google搜尋，並無法拒絕不懷好意的使用者造訪

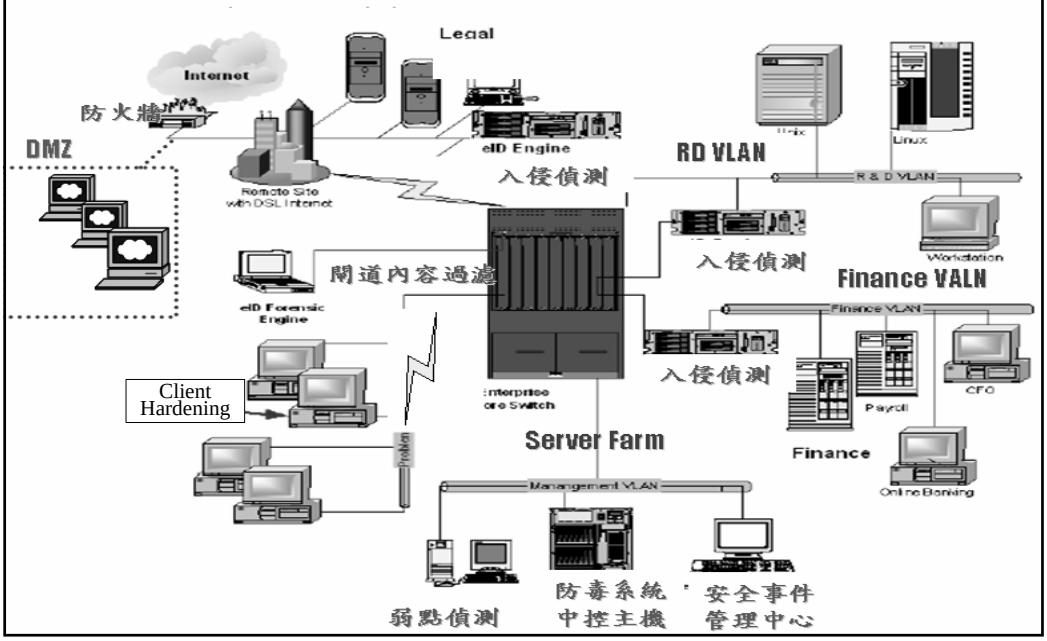
3. 因業務需要考慮e化系統時，應同時考慮相對帶來的資訊使用風險，並預先規劃控制措施
   - -什麼的業務，需要提供公眾網路上的「公開服務」?
   - -基本的查詢限制與存取控制，建立了嗎?
   - -定期的弱點檢測與追蹤，做了嗎?
   - -管理者與系統使用者教育，做了嗎?
   - -機敏資料的網路傳輸保護，做了嗎?
   - -資料庫的管理與定期備份，做了嗎?

4. 平日即熟悉並規劃應變組織.

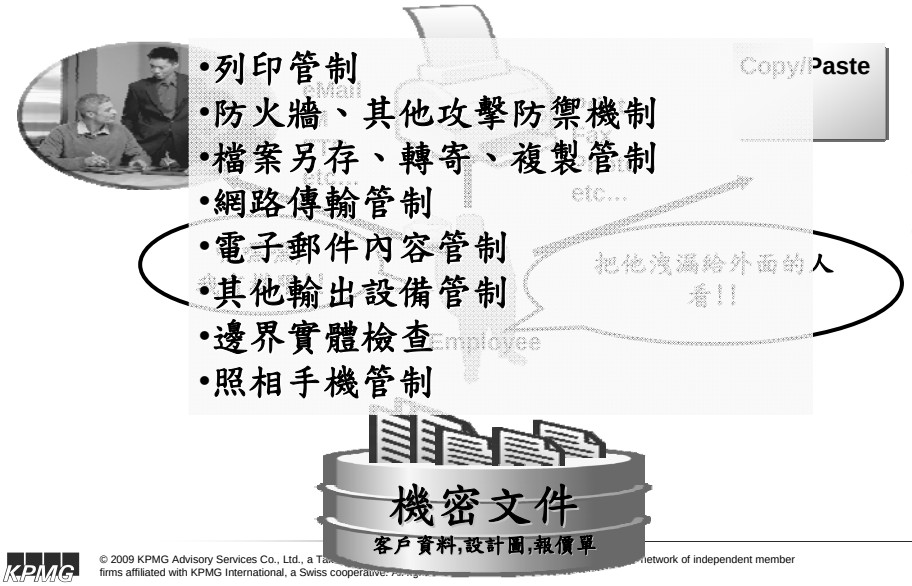
5. 預防勝於治療!

看新聞學資安(3)-
2008年的一級科技大廠洩密事件

網路環境示意圖



風險分析與管理作為



- 列印管制
- 防火牆、其他攻擊防禦機制
- 檔案另存、轉寄、複製管制
- 網路傳輸管制
- 電子郵件內容管制
- 其他輸出設備管制
- 邊界實體檢查
- 照相手機管制

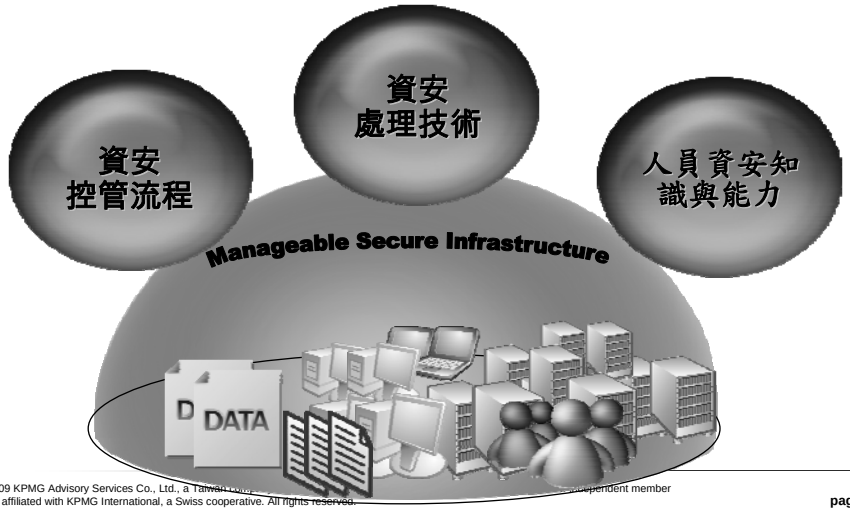
HD
USB
CD
NB
etc..

意料之外...

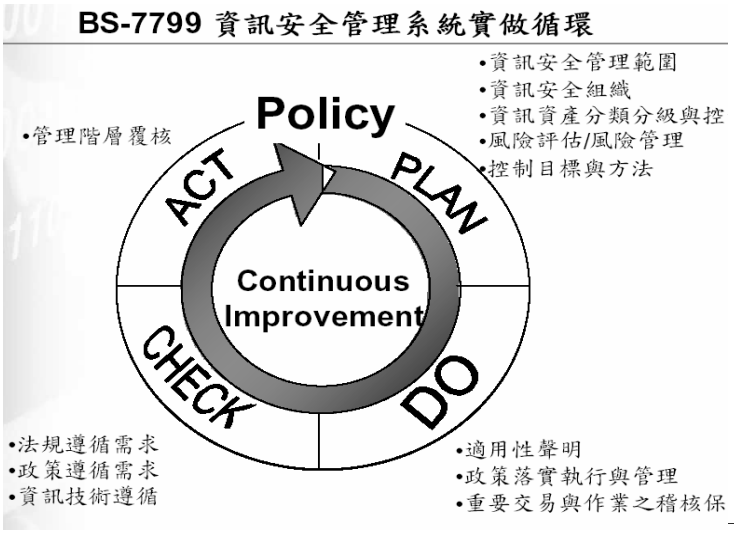
還有您想不到的方法.....??

何謂良善的資安內部管理責任?

資訊安全管理三要素



ISMS實作循環



應執行的資安管理範圍- 依據國際資安標準

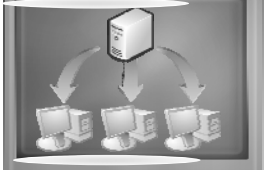
- 資訊安全政策
- 組織資訊安全
- 資產管理
- 人力資源管理
- 實體與環境安全
- 通訊與作業管理
- 存取控制
- 資訊系統取得/開發與維護
- 資訊安全事件管理
- 營運持續管理
- 符合性

ISO27001是國際資訊安全標準，用以規範並驗證ISMS之建置成果。

包含11項安全控制章節，共39項主要安全種類、135項控制，與一項介紹風險評鑑與處理的章節。

組織資安目標

強化基礎架構與管理策略



- 加強資安防禦機制
- 活化系統整體架構
- 改善資訊系統效能
- 建立標準作業程序
- 提升人員反應能力
- 降低資安事件損害

提升使用者資訊服務滿意度

- 明確資安組織權責
- 降低資訊使用風險
- 增加主管機關信賴
- 提高民眾使用信心
- 增強組織資安意識
- 提升危機處理能力

建立資訊安全管理制度與流程

- 建立資訊安全制度
- 進行資訊資產管理
- 完成資訊風險評鑑
- 執行資安事故通報
- 確保業務持續營運
- 制定資安稽核制度
- 奠定良好驗證基礎

教育機構保護個資之應有作為

- 僅收集業務所需之資料，不要過度收集
- 個資的獲取與傳遞，需取得學生家長或當事人同意
- 檢視現有校務資訊作業流程是否存在安全之漏洞
- 檢視現有校務公開資訊是否做到最小揭露原則
- 導入適當資安技術控管機制以防止資訊外洩
- 加強作業人員之資安訓練與政策宣導
- 依據資安分級，積極參考教育體系資安管理規範執行各項管理與技術之資安防護制度，以作為事前良善資料管理責任的積極證據
  - 校園通用之資安管理原則請參考: http://cissnet.edu.tw/manage.aspx
  - 教育體系資安管理規範請參考: http://cissnet.edu.tw/rule_edu.aspx

何謂良善的資安委外管理責任?

常見的資訊作業委外種類

由委外內容區分

- 資料處理作業委外(資料整理、登打、掃描、印刷等)
- 應用程式開發委外(網站維運、程式設計、程式撰寫等)
- 系統維運委外(於委外廠商機房等場所，進行主機代管、網路代管、電郵代管等)
- 資訊服務委外(於機關內部進行重要網路服務協助、資料庫管理協助、網站開發協助、主機管理協助、資安工作協助等)
- …其他

由委外方式區分

- 由業務單位獨立進行發包與委外管理
- 由資訊單位獨立進行發包與委外管理
- 由業務單位進行發包，並由資訊單位參與委外管理
- 由資訊單位進行發包，並由業務單位參與委外管理

常見委外安全管理風險疏失

政府委外資訊作業常見之資安風險事件

- **委外網站遭入侵或攻擊而導致營運中斷**
- **委外網站資料遭不當揭露(MOE, CCD)**
- **委外資訊作業營運中斷**
- **….Others**

政府委外資訊作業常見之管理疏失

- **未於合約明列完整資安要求**
- **系統開發完成未進行安全測試即驗收**
- **廠商系統維運環境與網路安全措施未盡完善**
- **廠商使用正式資料進行測試**
- **廠商於驗收完成後，仍持有系統最高權限帳號**
- **廠商進行程式更新時，未有完整之上線測試程序**
- **廠商進行程式更新後，未有定期之安全測試程序**
- **廠商直接以非組織移動式設備，連接組織內網路**
- **維護合約未及時銜接**

完整之資訊委外安全檢核建議

擬案與規劃(可明列於RFP或合約條款中，要求廠商遵守)

- 資安原則
- 保密條款
- 稽核權力
- 維護與保固
- 惡意損害賠償
- 合理成本分析
- 服務水準協議(SLA)

安全技術規格設計(可提示於RFP中，由廠商自行規劃)

- 系統開發委外-應用程式安全/後門
- 系統維運委外-機房安全設計/網路安全設計/存取控制方法)

系統測試 (可提示於RFP中，由廠商自行規劃)

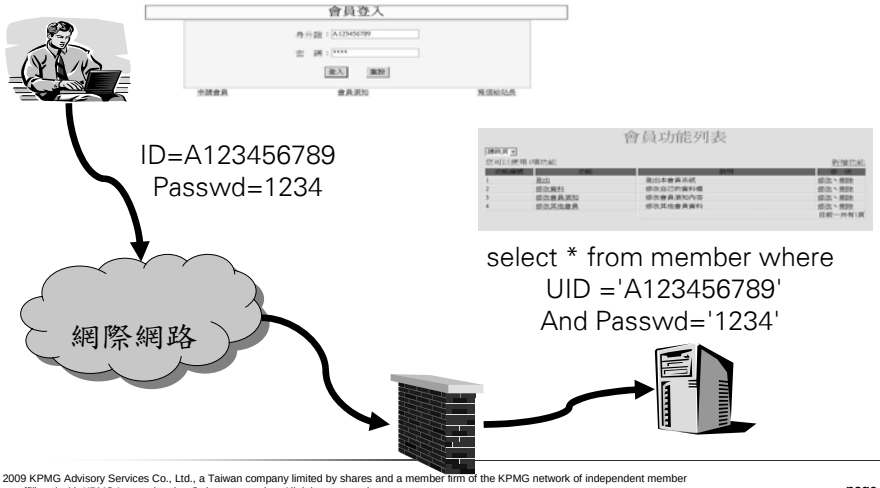
- 使用者測試方法
- 系統安全測試方法

系統上線與維運 (可提示於RFP中，由廠商自行規劃)

- 程式變更管理
- 弱點管理
- 備援備份設計
- 資安事件通報與處理

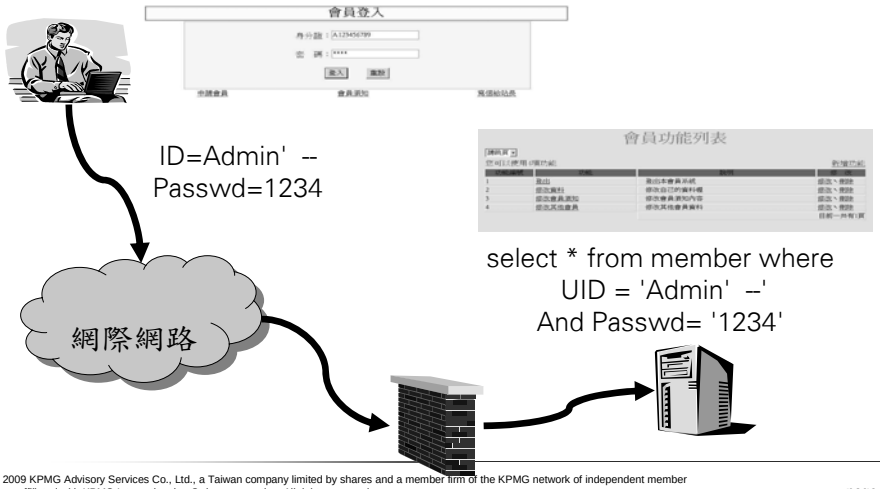
常見應用程式弱點- SQL Injection

- 正常連線狀態

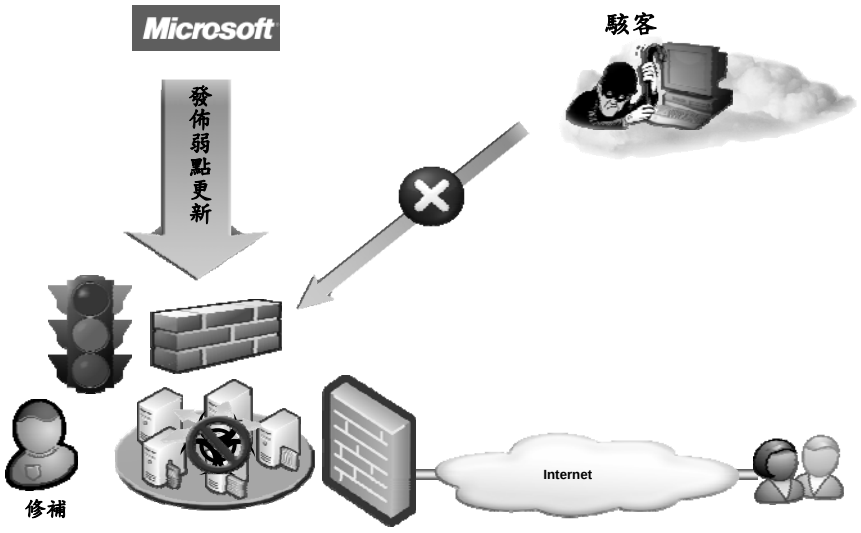


常見應用程式弱點- SQL Injection (續)

- **SQL Injection 攻擊**



系統漏洞



安全的Web應用程式委外開發原則

- 系統設計，請考量互動型態的必要性(查詢、論壇BBS、線上表單、留言版、上傳資料、噗浪等)。一般而言，靜態與單向網頁，安全性高於多媒體互動式網頁。
- 系統與設備置於組織內，在組織內資源可行之情況下，安全性高於系統維運委外。
- 定期的應用程式安全檢測是例行的必要工作
- 後台管理系統的安全性，應高於前台系統

Web程式登入之安全機制設計

網頁程式自我揭露-暴露!

http://hotel.ezfly.com/hotel/quickers/roomlist.asp?1=1&eventcd=dhh&website=ezhome--go02&RTDetailName=&sacode=&newsection1=109&DH_IMG.x=16&newhotelid1=213&DHindate=2009/6/23&DHCitySelect=台南&DHIDSelect=213&rdDHDay=on&newh_area1=台南&indate=2009/6/23&Price=0&DH_IMG.y=10&PlaceNo=109&place=台南&DHAreaSelect=109&outdate=2009/6/24&RoomCount=1&StayN=1

網頁程式自我揭露-安全!

個人資安小秘方-如何安全的使用個人電腦

個人電腦(含NB)使用安全秘笈- 基本型

- 系統密碼需設定
- 防毒軟體常更新
- 重要資料勤備份
- 釣魚網站有警覺
- 官方網站較可靠
- 不明郵件勿開啟

- 系統漏洞需補強
- 螢幕保護要啟動
- 機敏檔案得加密
- 公務電腦不共用
- 無線網路有風險
- 安裝軟體停看聽

個人電腦(含NB)使用安全秘笈- 進階型

- 考慮安裝個人防火牆
- 注意USB使用技巧(勿執行自動啟動)
- 最好採用浮動IP(家用電腦)
- 考慮針對機密檔案採用DLP資料防護工具
- 考慮使用硬碟加密系統
- …

電腦密碼設定原則- 應避免

絕對避免的密碼：

- 嚴禁不設密碼
- 與帳號相同
- 與主機相同
- 生日、身分證字號、英文姓名等個人資料，以及公司、部門等公司資訊
- 使用1111、1234、123456、2000、aaaa、abcdef此類簡單的組合
- 密碼別留在紙上或是文字檔中

應該避免的密碼：

- 避免使用英文單字或詞語，如iloveyou、superman
- 避免全部使用數字
- 避免連號或順序，如nopqrs、987654…

電腦密碼設定原則- 應做到

較佳的密碼原則：

- 通行密碼應至少每三個月更換一次，通行密碼組成為八位英數字（英文字母區分大小寫），且嚴禁轉知他人。
- 如於密碼使用期間，有被他人窺知之情形者，應即更換新碼；如因故被冒用致造成不良後果者，應負洩密之責。
- 密碼沒有明顯含義。
- 密碼要能記得住，一個連使用者都無法記住的密碼是無意義的。

一些密碼設定小技巧：

- 可以讓l == 1 or ! or |, O == 0, S == 5, A == 4, q == 9
- 以中文輸入法按鍵來當成密碼, 例如\"密碼\"的注音輸入為5j4up
- 以英文的一句諺語或一段歌詞， 取每個英文字字首當成密碼
- 以兩個英文字或數字穿插：例如: abcd + 1234 = a1b2c3d4，不過兩段數字的穿插是沒有意義
- 將英文字母位移數個字：例如: with往前位移三個字母 -> tfqe
- 自行變化原則，可以把上面的綜合起來使用，也可以自訂原則如鏡印、藏頭去尾。

個人資安小秘方-如何安全的使用電子郵件

網路騙術何其多？

網路釣魚與社交工程實況模擬

案例：花旗銀行的通知函?

花旗銀行通知函:
您的帳號密碼過期請重新確認

同時駭客取得
客戶帳號密碼

連入幾可亂真的花旗網銀
依指示重新確認帳號密碼

開始進行
網路轉帳

登入成功
連線至真正花旗網銀

顯示網址-http://www.citibank.com.tw

實際網址-http://www.citibank.com.tw hacker@cn

社交工程演練 – 概述

•社交工程（Social Engineering）：

- 利用人性的弱點進行詐騙，是一種非"全面"技術性的資訊安全攻擊方式，藉由人際關係的互動進行犯罪行為。
- 駭客通常由電話、Email 或是假扮身份，問些看似無關緊要的問題等各種方法來進行社交工程。

•社交工程攻擊目的

- 竊取帳號、密碼、身分證號碼或其他機敏資料，進而造成企業或個人極大威脅和損失的駭客攻擊手法。

•社交工程常見手法

- 偽造信件主題與內容
- 偽造寄信來源
- 假造的URL位址列
- 網頁中夾帶木馬與間諜軟體

電子郵件管理困境

困境

- 電腦病毒感染
- 垃圾郵件
- 機密 / 敏感資料外洩
- 員工工作效率

電子郵件的使用管理應注意下列事項

- 禁止冒用他人的帳號。
- 直接刪除來路不明或可疑郵件。
- 不理會任何廣告信。
- 不隨意洩露個人之Email資料。
- 轉寄郵件時，刪除他人的轉寄記錄。

社交工程自我保護

電子郵件防禦社交工程的方式

- 不隨意開啟郵件（注意陌生之寄件者）
- 取消郵件預覽
- 不隨意下載附件
- 確認寄件人與主旨的關係
- 非經查證，禁止直接點選郵件中的超連結
- 善用密件收件人
- 不隨意留下郵件地址予他人
- 了解組織傳送郵件規定

Q&A

kpmg.com.tw

68F, Taipei 101 Tower, No. 7, Sec. 5
Xinyi Road
Taipei 11049
Taiwan
Tel: +886 2 8101 6666
Fax: +886 2 8101 6667

安侯企業管理股份有限公司

台北市11049
信義路五段7號68樓（台北101金融大樓）
電話： +886 2 8101 6666
傳真： +886 2 8101 6667