KPMG

INFORMATION TECHNOLOGY ADVISORY

澎湖縣教育網路中心
資訊安全教育訓練

ADVISORY

林茹玉 顧問師
安侯企業管理股份有限公司
中華民國99年01月

AUDIT ▪ TAX ▪ ADVISORY

講師介紹

林茹玉(Lucy Lin)

KPMG 資訊科技諮詢服務 顧問
lucylin@kpmg.com.tw
886-2-8101-6666 ext. 08985

專業證照

- ISO 27001 Lead Auditor認証合格
- ISO 20000 Lead Auditor認証合格
- ITIL Foundation認証合格
- Trend Micro Certified Security Expert

ISMS建置經驗

- 衛生署、台灣電力公司、司法院、國民健康局、北區醫療聯盟、中區國稅局、北區國稅局、職訓局、教育部八校聯合輔導等。

內控稽核

- 台灣郵政、富邦金控、亞太電信、長春石化、中菲航等

憑證中心與註冊窗口稽核

- GRCA、GCA、XCA、HCA、MOICA、臺灣網路認證中心

資安教育訓練前言-您的幾個疑問..

課程大綱

ISO 27001 簡介

教育體系資通安全管理規範

資訊資產管理

實體環境安全管理

個人電腦資安防護秘笈

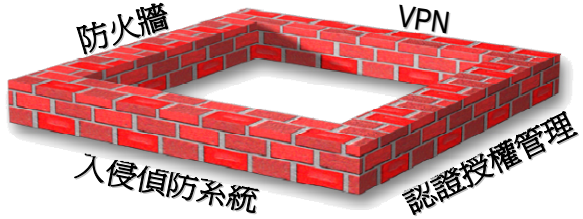
2010年校園資安管理的新挑戰

Q & A

一般都會注意...

- 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

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

何謂資訊安全管理系統(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

資訊安全之目的達成下列三大目的

- 機密性(Confidentiality)
  - 確保只有被授權的人可以存取
- 完整性(Integrity)
  - 確保資訊及處理方法的正確及完整
- 可用性(Availability)
  - 確保被授權的人有需要時可以存取

資安管理三要素

透過資訊安全管理三要素來確保資訊安全三要素

BS/ISO/CNS比較

英國標準	國際標準	台灣標準
BS7799-2:2005	ISO27001:2005 ISMS資安管理系統認證標準	CNS27001:2006
BS7799-1:2005	ISO27002:2007 ISO17799:2005 ISMS作業規範	CNS17799:2006
	ISO27003 ISMS導入指南(未定)	
	ISO27004 資安管理有效性量測標準(未定)	
BS7799-3	ISO27005 風險管理	
	ISO27006 驗證機構認證規範	
	ISO27007 ISMS稽核的參考指南(未定)	
	ISO 27799 醫療行業資安認證導入指南	

ISO 27001資訊安全管理制度簡介

ISO/IEC 27001:2005 - 資訊安全管理系統驗證規範

ISO/IEC 27002:2005 - 資訊安全管理系統實務準則(ISO 17799)

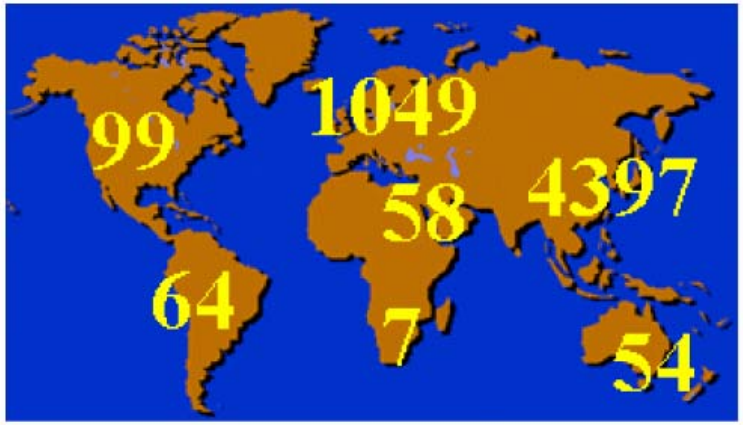
- 本文(0 ~ 8)
- 11 大管理要項(A.5~A.15)
- 39 個執行目標
- 133 個控制項目

ISO 27001 涵蓋範圍

ISO 27001是國際最廣泛接受的資安驗證標準

ISO 27001 adopted by many countries for domestic use and translated in different languages

ISO 27001認證全球推廣情況

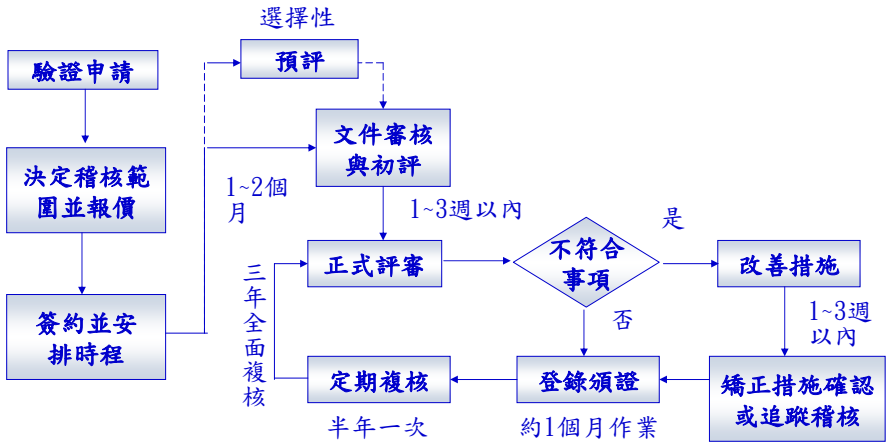


ISMS Registrations by Continent

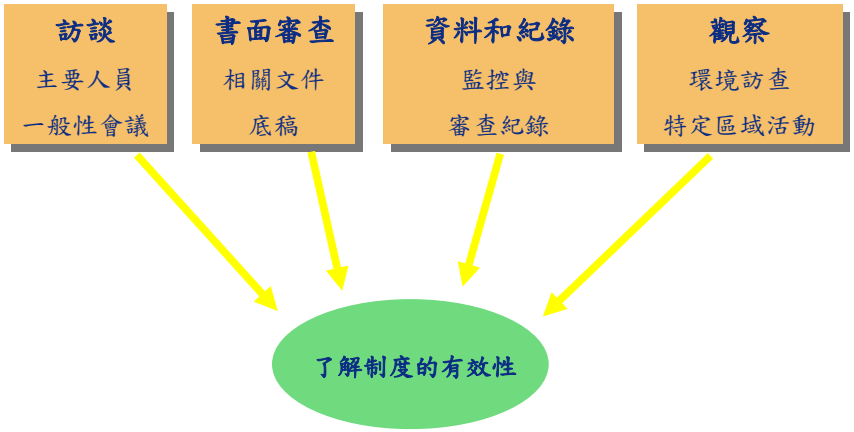
http://www.iso27001certificates.com/

對資訊服務績效的影響

ISO 27001驗證流程



稽核方式



稽核發現類別

- **Nonconformities：不符合事項**
  - Major主要
  - Minor次要
- **Observations：觀察事項**
  - Commendation 建議
  - Requires review as a future IN may be raised
    未來可能成為不符合事項而需要再覆核
- **Opportunities for Improvement：改善機會**

如何才能通過驗證?

- 要通過ISO27001認證，必須符合以下四個條件：
  - 必需要符合標準本文的規定
  - 政策與文件必須要符合所選用的ISO27001條文要求
  - 落實程度要符合政策與文件
  - 不能有過多的次要缺失集中在同一條文或是單位

ISO 27001 簡介

教育體系資通安全管理規範

資訊資產管理

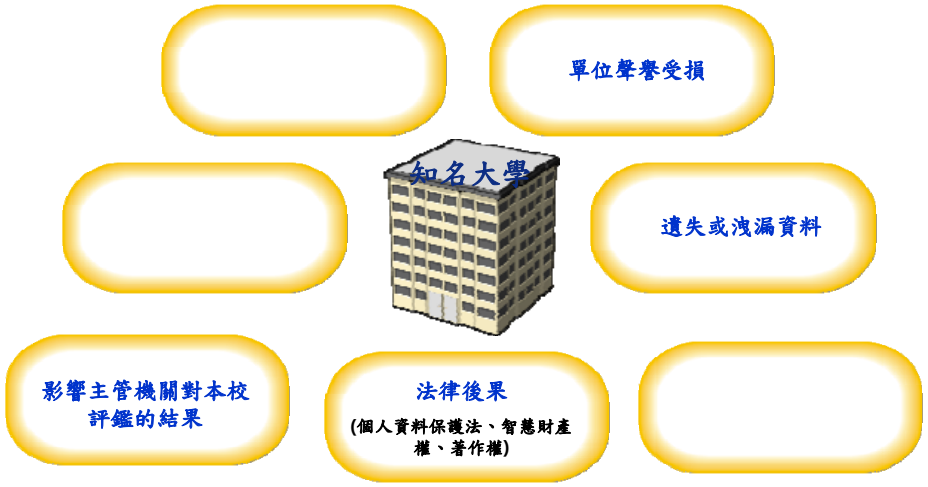
實體環境安全管理

個人電腦資安防護秘笈

2010年校園資安管理的新挑戰

Q & A

資訊安全問題對學校造成的影響



教育機構之資訊安全需求

為什麼教育機構需要資訊安全

- 學籍資料保護
- 成績資訊保護
- 強化資訊網路防護能力
- 建立資安管理相關機制、程序與PDCA流程管理

教育機構所擁有的資訊特色

- 機密等級雖不高但有一定敏感性
- 涉及個人隱私
- 適用電腦處理個人資料保護法之相關規定

教育機構常見資安問題

- 較容易被惡意人士入侵當作攻擊跳板，電腦病毒流竄也偶有所聞
- 網路資源易被誤用
- 資安防護意識不高
- 資安管理機制未完整建立

政府機關資訊安全責任等級分級作業

教育部所屬機關及各級公私立學校資訊安全責任分級

- A 級：教育部、台大醫院、成大醫院
- B 級：入學考試常設機構、大學、區域網路中心、縣(市)教育網路中心、陽明大學附設醫院
- C 級：技術學院、專科學校、部屬館所
- D 級：高中職、國中小學
- 承辦入學考試業務機關學校比照B級單位(包括四技二專、國中基測承辦學校)

作業 / 名稱 / 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
A級	NSOC直接防護/ SOC自建或委外、IDS、防火牆、防毒、郵件過濾裝置	通過第三者驗證	每年至少2次內稽	1.每年至少(3、6、18、3小時) 2.資訊人員、資安人員需通過資安職能鑑定	維持至少2張資安專業證照
B級	SOC(選項)、IDS、防火牆、防毒、郵件過濾裝置	通過第三者驗證	每年至少1次內稽	1.每年至少(3、6、16、3小時) 2.資訊人員、資安人員需通過資安職能鑑定	維持至少1張資安專業證照
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
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

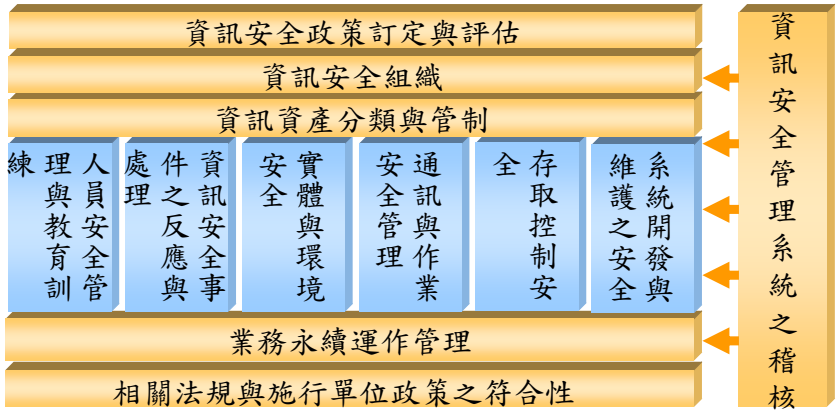
教育體系資通安全管理規範

- 參考 ISO 27001:2005、CNS 17800 以及我國政府規範等法令標準，訂定出適用於教育體系之資通安全管理規範
- 使各級學校與教育網路中心能以最低成本與時間，建構嚴謹且合適之資訊安全管理系統
- 配合教育部規劃之「**教育機構資安驗證機制**」，建構國內專屬之第三方驗證標準
- 教育部已於 96 年 6 月 11 日發函各機關學校公布推動「教育體系資通安全管理規範」及「國中小學資通安全管理系統實施原則」以做為教育體系各機關學校落實資安管理制度參考

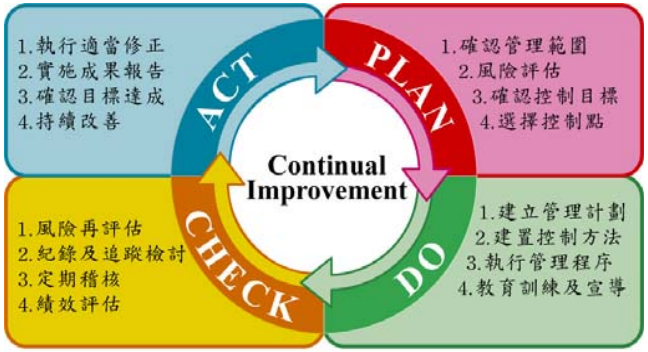
教育體系資通安全管理架構

11 個控制領域、 36 個控制目標、 100 個控制措施

（每個控制領域會包含多個控制目標；每個控制目標會對應一個以上的控制措施）



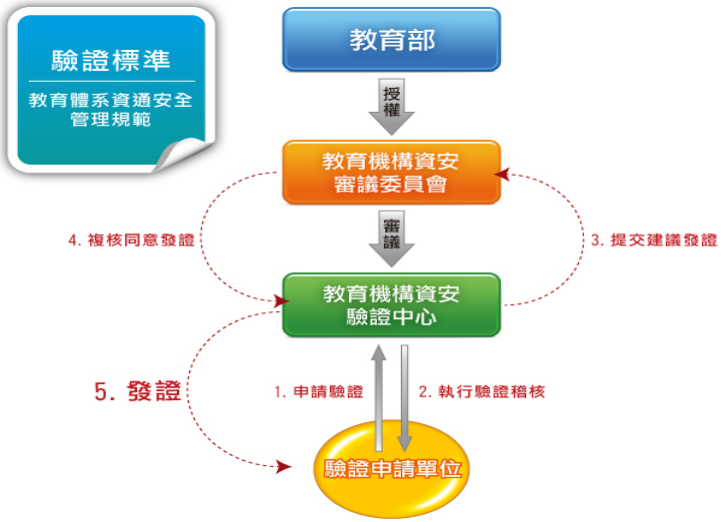
方法論



評比項目	教育體系資通安全管理規範:96年5月30日版	ISO27001
領域	11	11
控制目標	36	39
控制項	第一群：100項 / 第二群：69項	133項

資訊安全管理成功必要條件

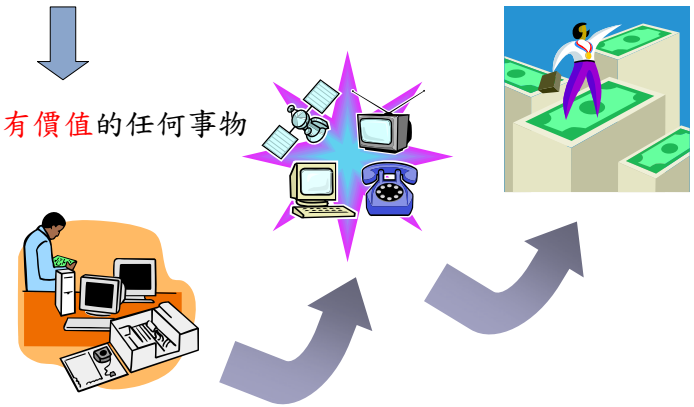
教育機構資安驗證機制



資訊資產特色

資訊資產 → 資訊 → 組織營運之命脈

即對組織有價值的任何事物



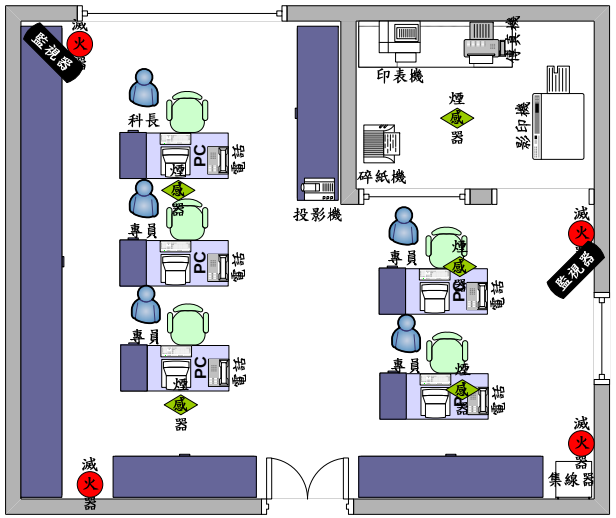
資訊資產管理目的

- 了解單位財產管理現況，確保資產帳物之一致性
- 有效管理資訊資產，提升利用率
- 協助各項管理制度有效運作
- 適切保護資訊資產→ 確保達成資訊安全之要求

ISO 27001 資訊資產管理

A.7.1 資產責任	
目標：達成及維持組織資產的適切保護。	
項目	**控制**
A.7.1.1 資產清冊	應明確識別所有資產，並製作與維持所有重要資產的清冊。
A.7.1.2 資產的擁有權	與資訊處理設施相關的所有資訊及資產應由組織指定的部門"擁有"。
A.7.1.3 資產之可被接受的使用	與資訊處理設施相關的資訊與資產，其可被接受的使用之規則應予以識別、文件化及實作。
A.7.2 資訊分類	
目標：確保資訊受到適切等級的保護。	
A.7.2.1 分類指導綱要	資訊應依其對組織的價值、法律要求、敏感性及重要性加以分類。
A.7.2.2 資訊標示與處置	應依照組織所採用的分類法，發展與實作一套適當的資訊標示與處置程序。

哪些是資訊資產?



電腦送修機密資料外洩

資料來源：蘋果日報 2008.02.02

資安觀點

- 電腦及儲存媒體送修前應確認是否含有機敏性檔案。
- 在網路上張貼猥褻照片或販賣淫照光碟，依妨害風化、違反著作權法移送法辦，最高可處2年以下徒刑。

檔案銷毀

資料來源：iThome 2008/01/31

檔案銷毀標準一覽		
名稱	**說明**	**複寫次數**
DOD 5220-22-M	美國國防部使用的檔案銷毀技術	3次
German VISITR Standard	德國政府使用的磁碟刪除技術	7次
Bruce Schneier's algorithm	由資訊安全專家Bruce Schneier提出的檔案銷毀標準	7次
Peter Gutmann's Algorithm	Peter Gutmann與Colin Plumb提出的檔案銷毀標準，覆寫等級最高。	35次
RCMP DSX Methode	加拿大皇家騎警隊（RCMP）公布的檔案銷毀標準，是加拿大官方所使用的檔案銷毀技術。	3次覆寫與3次驗證覆寫

ISO 27001 簡介

教育體系資通安全管理規範

資訊資產管理

實體環境安全管理

個人電腦資安防護秘笈

2010年校園資安管理的新挑戰

Q & A

天然災害


2000年911恐怖攻擊


2004年南亞海嘯


2009年 88水災


2010年 海地大地震

從101超高大樓實體環境風險管理談起

可能的營運風險來自....天災人禍

實體環境風險管理-從預防、偵測與矯正規劃做起

101大樓的風險管理作為

風險管理措施	措施分類	針對風險
堅固的地基與阻尼系統	預防性	地震、颱風等天災
安全可靠的垂直運輸服務	預防性	無法進行人員移動與貨物運輸
雙份備援配電機制與不斷電機制	矯正性	電力中斷
24小時無間斷空調供應	預防性	空調中斷
配備無電力自動灑水系統	矯正性	火災
配備雙路由光纖網路骨幹	矯正性	通訊中斷
配備420套監視設備、門禁與自動發卡系統	偵測性、預防性	人為破壞

ISO 27001實體環境安全管理(1/2)

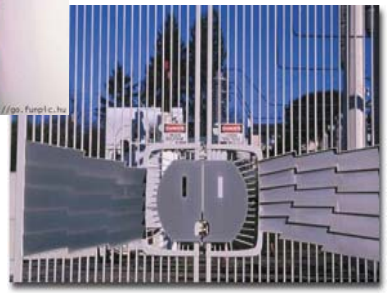
A.9.1 安全區域	
目標：防止組織場所與資訊遭未經授權的實體存取、損害及干擾。	
項目	**控制**
A.9.1.1 實體安全周界	應使用安全周界（諸如牆、卡控入口閘門或人員駐守的接待櫃檯等屏障），以保護含有資訊及資訊處理設施的區域。
A.9.1.2 實體進入控制措施	安全區域應藉由適當的入口控制措施加以保護，以確保只有經授權人員方可允許進出。
A.9.1.3 保全辦公室、房間及設施	應設計辦公室、房間及設施的實體安全並施行之。
A.9.1.4 對外部與環境威脅的保護	應設計並施行實體保護，以避免遭受火災、洪水、地震、爆炸、民眾暴動及其它天然或人為災難的損害。
A.9.1.5 在安全區域內工作	應設計在安全區域內工作的實體保護與指導綱要，並施行之。
A.9.1.6 公共進出、收發及裝卸區	諸如收發與裝卸區及其他未經授權人員可進入作業場所之進出點宜加以控制；若可能，並宜與資訊處理設施隔離，以避免未經授權的存取。

ISO 27001實體環境安全管理(2/2)

A.9.2 設備安全	
目標：防止資產的遺失、損害、竊盜或破解，並防止組織活動的中斷。	
項目	**控制**
A.9.2.1 設備安置與保護	應安置或保護設備，以降低來自環境之威脅與危害造成的風險，以及未經授權存取之機會。
A.9.2.2 支援的公用設施	應保護設備不受電源失效及其他支援的公用設施失效所導致的中斷。
A.9.2.3 佈纜的安全	應保護傳送資料或支援資訊服務之電源與電信佈纜，以防止竊聽或損害。
A.9.2.3 佈纜的安全	應正確地維護設備，以確保其持續的可用性與完整性。
A.9.2.5 場所外設備的安全	安全應適用於場外設備的，並考慮其在組織場所外工作的各種不同風險。
A.9.2.6 設備的安全汰除或再使用	含有儲存媒體的設備，其所有項目在汰除前應加以檢核，以確保任何敏感性的資料與有版權的軟體已被移除或安全地覆寫。
A.9.2.7 財產的攜出	未經事前授權，設備、資訊或軟體不應帶出場外。

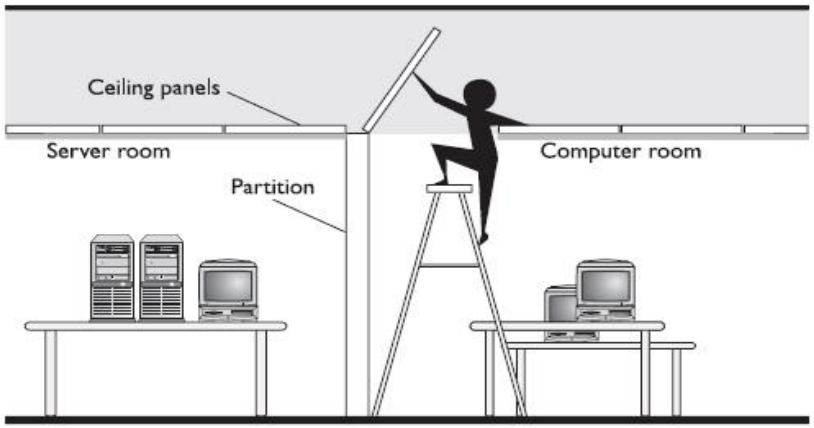
實體安全目標

- Deter威嚇
- Delay 延遲
- Detect 偵測
- Assess 評估
- Respond 回應



資訊安全實體防護

實體環境的弱點



辦公／異地備援場所需考慮的條件

- 地理條件
  - 災害發生時距離是否足夠
- 可存取的時間
- 安全性
- 環境
  - 溫濕度、防火、電力管理控制等
- 成本
  - 運送、運作費用、災害復原/反應服務

備援場所種類

- 組織自行擁有運作
- 與內部或外部單位相互協議
- 廠商提供設施

Site	Cost	Hardware Equipment	Telecom-munications	Setup Time	Location
Cold Site	Low	None	None	Long	Fixed
Warm Site	Medium	Partial	Partial/Full	Medium	Fixed
Hot Site	Medium/ High	Full	Full	Short	Fixed
Mobile Site	High	Dependent	Dependent	Dependent	Not Fixed
Mirrored Site	High	Full	Full	None	Fixed

資料來源:NIST 800-34 Contingency Planning Guide for Information Technology Systems

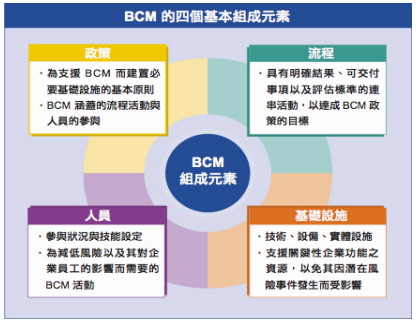
Mobile Site

看不見的風險...

他山之石- 2006新加坡金融局BCM演練:架構

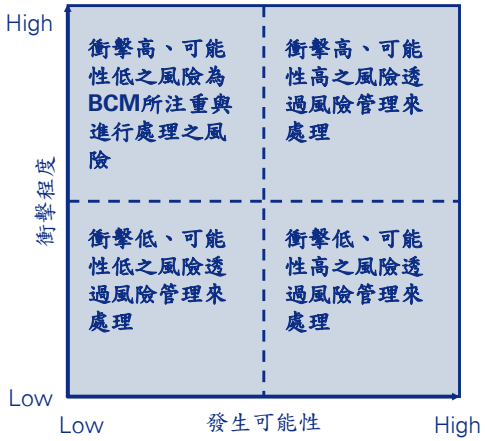
新加坡政府公開BCM標準與作業守則

新加坡政府技術參考文件 TR19：2005 將 BCM 描繪成涵蓋六大領域與四個基本元素：



2008年5月22日，新加坡政府宣布，所有向政府提供服務的服務供應商都必須擁有BCM計畫，否則，他們可能不能向政府提供服務。

營運持續管理與風險管理之關係

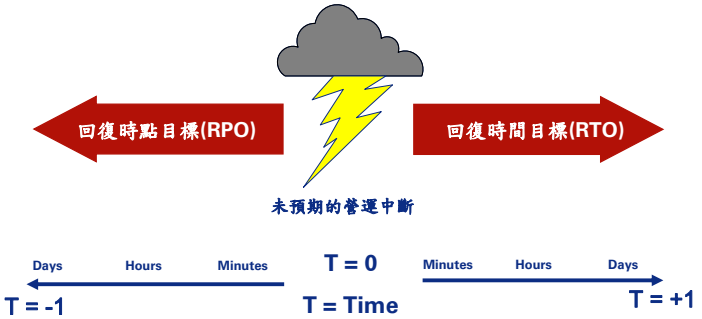


BCM的3個重要時間指標

MTPD (Maximum Tolerable Period of Disruption)最大可容忍中斷時間

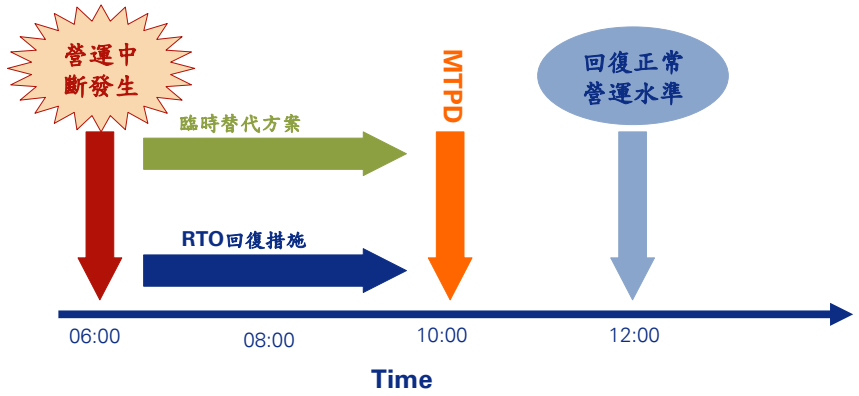
RTO (Recovery Time Objective)回復時間目標

RPO (Recovery Point Objective)回復時點目標



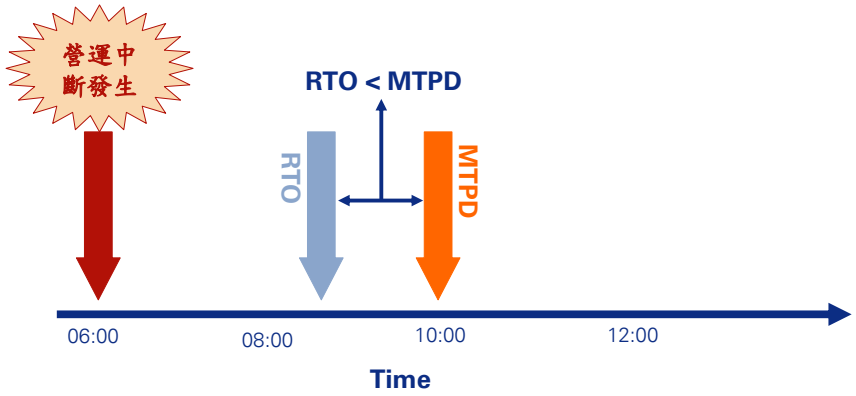
MTPD與RTO關聯示意圖(一)

思考營運持續管理措施要從"Worst Case"出發，如此才會充分考量到中斷事故所帶來之最大損害

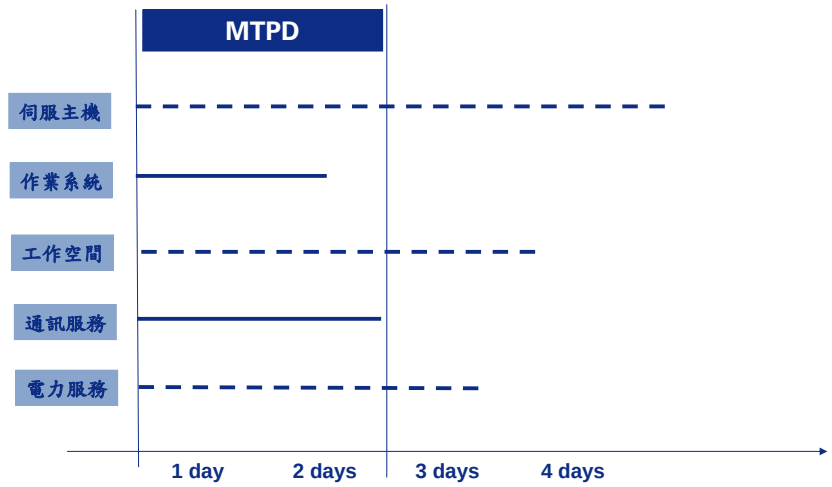


MTPD與RTO關聯示意圖(二)

回復時間目標(RTO)=執行營運持續計畫所需要的時間



回復資源重置時間與MTPD之關聯

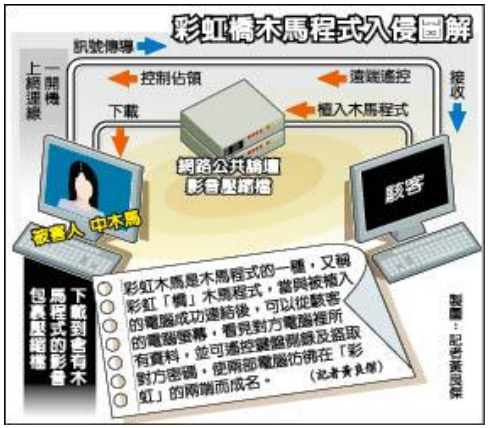


資安迷思篇

網路的新應用與威脅 – 致命的吸引力

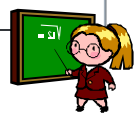
從網路狗仔隊來的威脅

新聞來源：資安人網站 2008/12/08



資安觀點

- 定期更新防毒軟體
- 拒絕下載不明軟體
- 視訊用畢後關閉或封貼鏡頭



從顧客來的威脅

從空氣來的威脅

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。

從對岸來的威脅

從內部不肖員工來的威脅

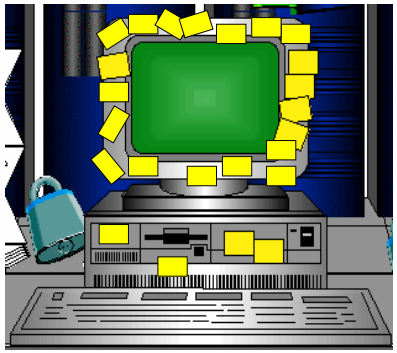
郵差偷標單21黃金地停標
旅店內拆封影印 檢調當場捕9人

國有財產局標售土地爆發重大弊端，不肖建商涉嫌和土地掮客江達德、張祥村連手，勾結郵局郵務士偷出標單，拆封、影印、封回後，以略高於對手的價格，企圖搶下包括前聯勤信義俱樂部等，預訂開標的二十一件土地標案。檢調昨天緊急展開搜查，國有財產局認為標單全部無效，在開標前宣布停標，引發建商譁然。

從內部粗心員工來的威脅

- 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
- …

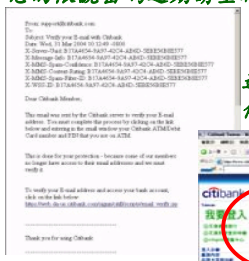
密碼輸入? 明碼張貼!!



網路騙術何其多?
網路釣魚與社交工程實況模擬

案例1：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

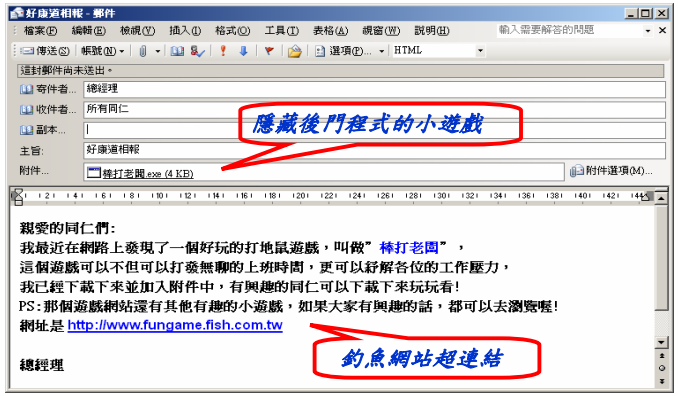
顯示網址-http://www.citibank.com.tw

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

網路騙術何其多?
網路釣魚與社交工程案例

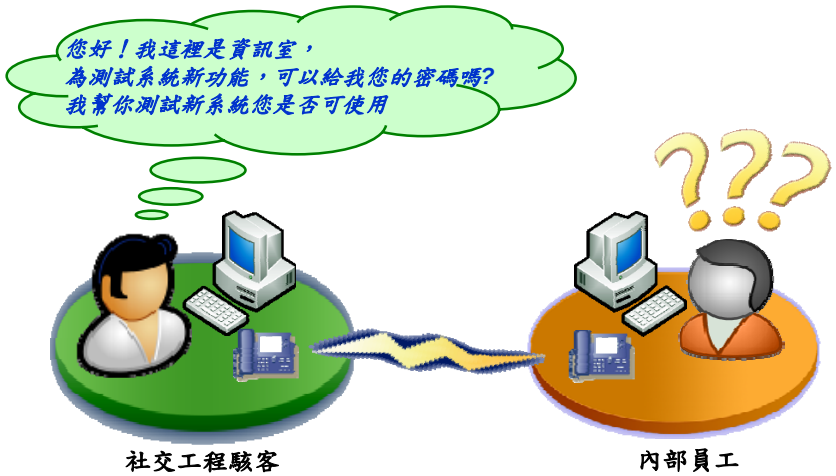
案例2：老闆的Email?

- 假藉主管之電子郵件，透過所夾帶之附加檔案與超連結，進行社交工程。



網路騙術何其多?
網路釣魚與社交工程案例

案例3：我是資訊單位的同仁?



何謂社交工程

社交工程(Social Engineering)為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。

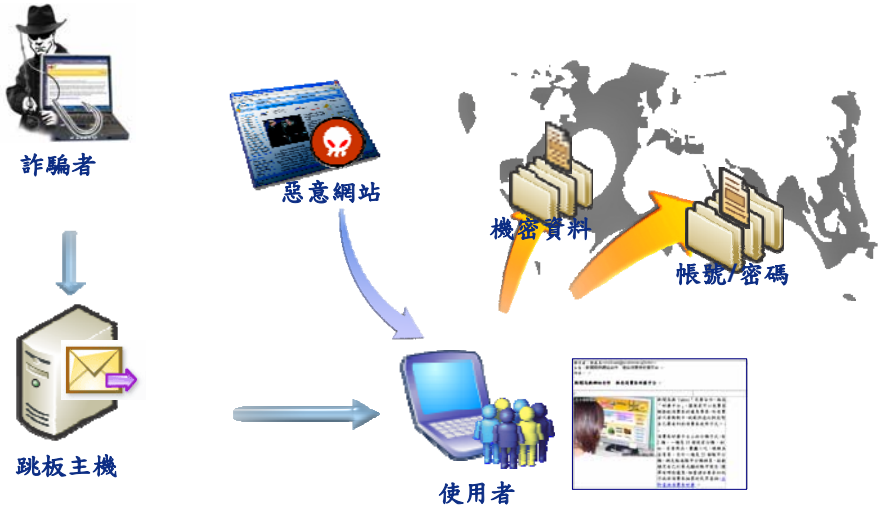
- 以人為本騙術為主
- 技術門檻較低
- 貪心：撿便宜的個性
- 好奇：探索感興趣的事務
- 缺乏警覺：有那麼嚴重嗎？

社交工程的攻擊手法

- 社交工程途徑
  - 電話
  - 電子郵件隱藏電腦病毒
  - 網路釣魚
  - 圖片中的惡意程式
  - 偽裝修補程式
  - 即時通
- 攻擊手法
  - 假冒為同事
  - 假冒新進員工
  - 假冒廠商、客戶或政府單位
  - 假冒具有權威的人
  - 假冒系統廠商，表示欲提供系統修補程式或更新程式
  - 假冒好心人士，告訴對方如果電腦發生問題可以找他，然後製造問題，讓受害人打電話來求援...等

社交工程幽默

電子郵件社交工程手法



引毒上身？五成網友主動下載有毒影音檔、電子郵件

- **資安案例**

總是抱怨網路毒駭事件層出不窮的使用者聽到以下消息，可能要先檢討自己為何如此「手癢」囉！入口網站最新調查顯示，網路中毒原因的前三名分別為「下載有毒的音樂或影音檔案」（27.6%）、「帳號被盜」（26.7%）及「收到夾帶有毒檔案和連結的電子郵件」（24.2%），除了帳號被盜，有五成 以上的網友都是「主動被駭」，主因來至網路安全知識的不足，而誤入「毒」徑。

網友最容易點選「跟搜尋結果相關的網站」（42.3%）及「好友寄的信件或訊息」（29%）而上了有毒程式的釣鉤，誤入電腦被 駭的危機。而另外依序還有「免費試玩或下載」（13.9%）、「火辣性感圖」（7.3%）及「折扣好康」（5.7%）等誘人資訊也會讓網友忍不住點選。
透過交叉分析也發現有趣的現象，會被「折扣好康」內容吸引的女性網友為男性的三倍，而「火辣性感圖」的內容吸引者則大多數為男性網友。

調查顯示，有五成網友是主動下載有毒影音檔，開啓電子郵件，讓自己曝露於網路毒駭的問題中。（圖／Yahoo！提供）

惡意郵件攻擊

資料來源：法務部全球資訊網

- 好康報、養生保健、休閒娛樂、公務相關、美食、八卦新聞…

同仁對於可疑電子郵件應有警覺性

為何我會收到這封郵件?

- 應確認寄件來源及寄件者

我是否應該收到這封郵件?

- 應確認郵件主旨及郵件內容

我是否應該開啟這封郵件?

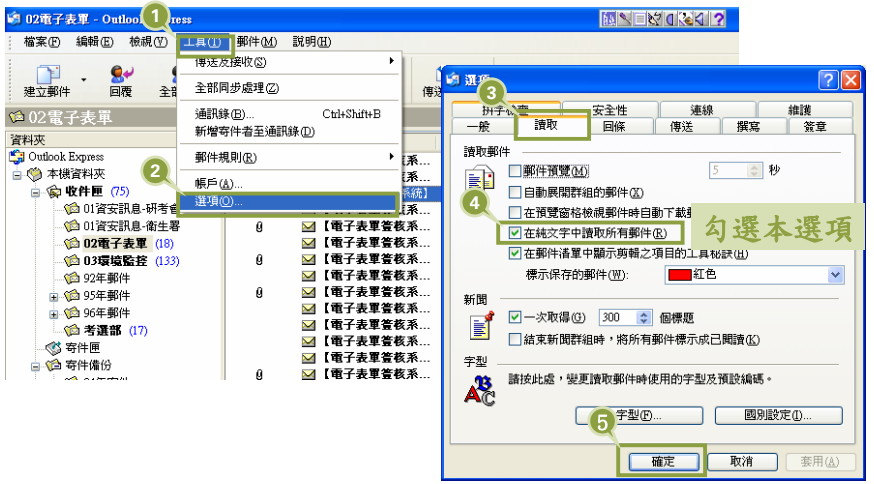
- 是否與業務工作相關
- 不開啟(點選)連結是否有影響
- 審慎查證(寄件者或資訊室)

電子郵件安全防制措施

- 電子郵件應「關閉預覽郵件」設定。
- 電子郵件應設定為「以純文字模式」開啟郵件。
- 不隨意開啟及轉寄與業務無關之電子郵件及網站。
- 如發現為不明來源或疑似網路釣魚之郵件應直接刪除。
- 不隨意點選或下載郵件內之連結與附件檔案。
- 如發現可疑信件應先通報資訊單位查證。
- 不隨意開啟郵件(確認寄件人)
- 善用密件收件人
- 不隨意留下郵件地址予他人
- 注意陌生之寄件者
- 了解組織傳送郵件規定

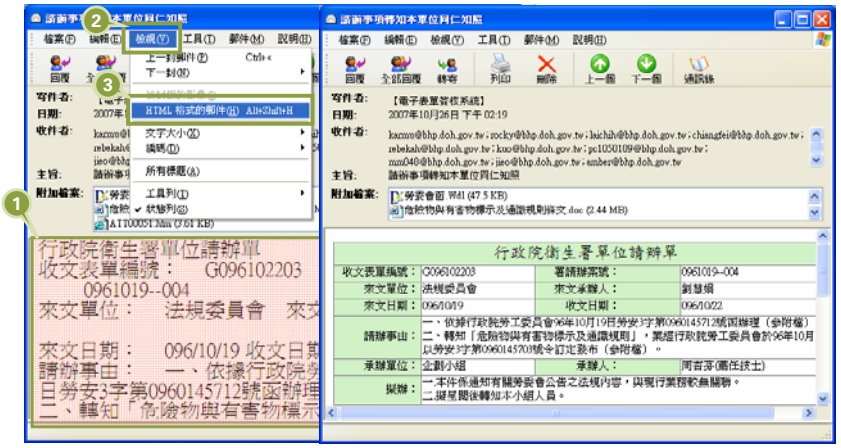
以純文字開啟郵件

- 預防郵件內藏自動執行程式



純文字郵件恢復正常檢視

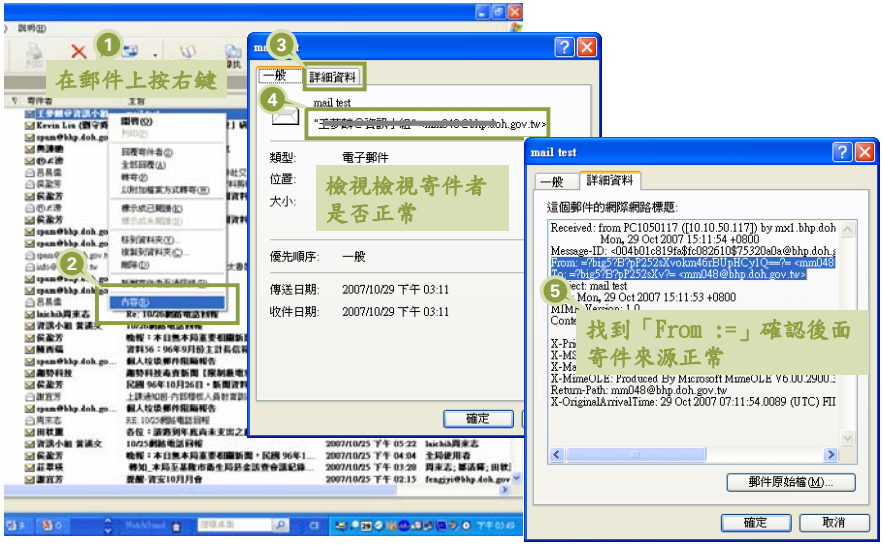
- 確認郵件為安全時



開啟郵件確認安全無誤

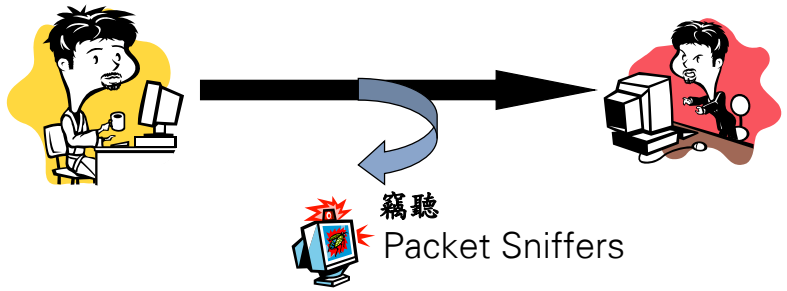
內容恢復正常

判斷郵件真偽



保衛傳送中的資訊

- 將資料加密使得任何未擁有解密金匙的人無法窺探其內容



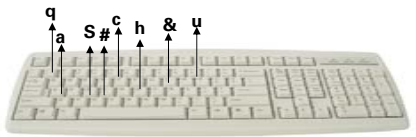
密碼設定小技巧

http://www.i-security.tw/class/B1/index.htm

1.以注音輸入法按鍵來當成密碼
你好嗎→Su#cla#8&

2.以英文字或數字穿插
good + 5829 → g5o8o2d9

3.將英文字母往前位移,如Birthday往前位移1個字母
Ahqsgczx



4.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

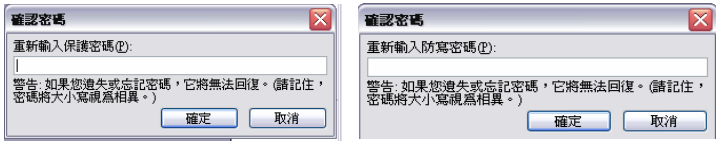
Best wishes for a happy New Year.
→BwfahNY

Word檔簡易加密法(1/2)

- Step1：開啟要加密的Word文件，依序點選功能表【工具】→【選項】。
- Step2：出現「選項」對話框後，點選＜安全性＞活頁標籤，接著在「保護密碼」旁的空白欄中輸入欲設定的密碼，如需增加文件防寫功能，可以在「防寫密碼」的空白欄中輸入欲設定的密碼，完成後按下【確定】。

Word檔簡易加密(2/2)

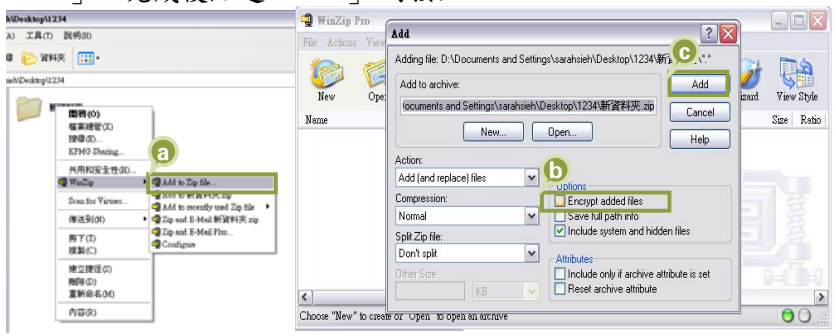
- Step3：接著會出現「確認密碼」對話框，於空白欄位中輸入上一步驟設定的密碼，然後按下【確定】。如有設防寫密碼，會多跳出「防寫密碼」的確認窗，步驟亦相同。



- Step4：設定完成後，務必記得點選【儲存檔案】，此份文件就受到所設定的密碼保護。
- Step5：下次當要開啟（編輯）這份文件時，Word都會要求再次輸入先前所設定的密碼，若是輸入錯誤，就無法進入編輯的視窗。

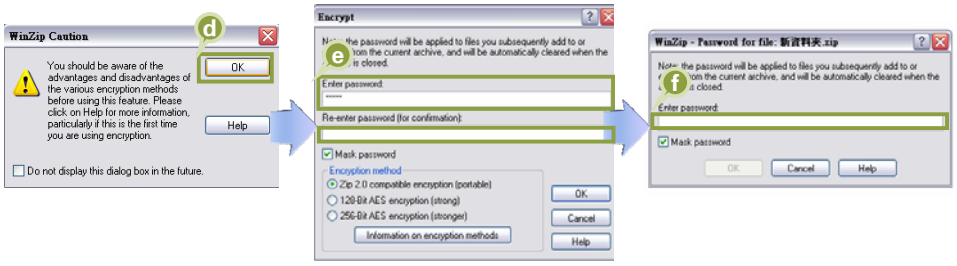
ZIP壓縮檔加密(1/2)

- Step1：開啟「Windows 檔案總管」。
- Step2：在要加密的檔案或資料夾上按一下右鍵，然後依序指向 [WinZip] → [Add to Zip file...]，並點選。
- Step3：出現「Add」對話框後，在[Options]區塊中，勾選「Encrypt added files」，完成後點選「Add」 的按鈕。



ZIP壓縮檔加密(2/2)

- Step4：出現「Caution」的對話框後，點選「OK」。
- Step5：接下來會出現「Encrypt」的對話框，在「Enter password」的的空白欄中輸入欲設定的密碼，並在底下的空白欄中再輸入相同的密碼一次，完成後點選「OK」，此即完成加密的動作。
- Step6：下次當要解壓縮這份文件時，會跳出「 Password」的對話框，必須輸入先前所設定的密碼，才能執行。



資料備份的重要性

資料備份的重要性(續)

不論是紙本或電子檔的重要資料，皆應：
1.定期備份
2.存放在不同地方(異地備份)

不同的儲存媒體，如：

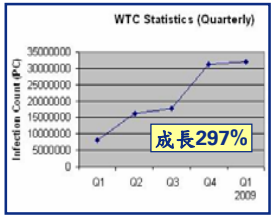
USB成病毒溫床

新聞來源：趨勢科技 2009 新聞稿

- 資安案例

根據趨勢科技全球防毒研究暨支援中心公布的第一季報告指出，2009年度台灣總共有 34,436,986次電腦遭受病毒感染案例，這個數量已將近2008年度全台灣總感染數量之47 %（2008年全台灣總感染數量為73,517,376 次）。與上一季（2008年Q4）相比，2009年第一季電腦感染總數增加9.79 %，與去年Q1同期比較，感染總數則成長高達297%。其中，USB病毒為主要感染媒介 關閉自動播放功能為自保之策

由於USB隨身碟及其它行動裝置的普遍使用，亞洲地區目前是自動執行式惡意軟體的熱門感染區。台灣第一季的前十大病毒中，感染前兩名的病毒即為USB病毒。經由USB 等可卸除式儲存裝置為感染途徑之一的Conficker/WORM_DOWNAD蠕蟲變種WORM_DOWNAD.AD，台灣在第一季也列入全球前十大感染國家的第四名。



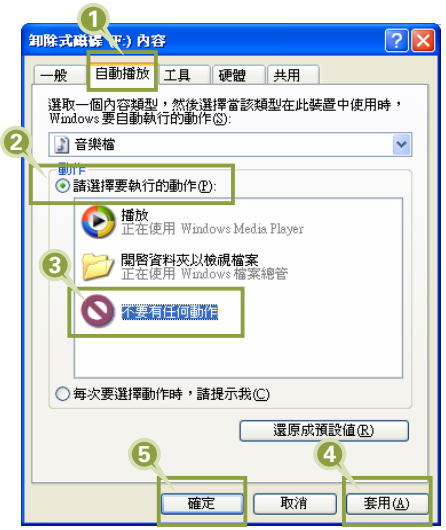
Taiwan Top 10 Malware	PC Count
MAL_OTORUN2	19533619
MAL_OTORUN1	5822990
TROJ_GENERIC.DIT	611638
VBS_LOVELETTER.A	482795
CRYP_NSANTI-3	481000
MAL_INFOSTL	413372
CRYP_NSANTI-4	237912
CRYP_NSANTI-5	234050
CRYP_OPET-3	227140
CRYP_OPET-2	198301

台灣2009第一季十大病毒統計

預防USB病毒的方法

關閉USB自動播放功能可以避免感染病毒的USB插入電腦時自動執行病毒檔案，以下提供兩種關閉USB自動播放的方式給網友參考：

- **Shift鍵：**
  插入USB裝置的同時按住Shift鍵不放，自動播放便不會啟用
- **磁碟機設定：**
  進入「我的電腦」，右鍵點選USB裝置後選「內容」，再點選自動播放標籤，針對四種不同的內容類型都選擇「不要有任何動作」，即可停用自動播放。



電腦幫忙記密碼 小心被駭偷光光

- **資安案例**

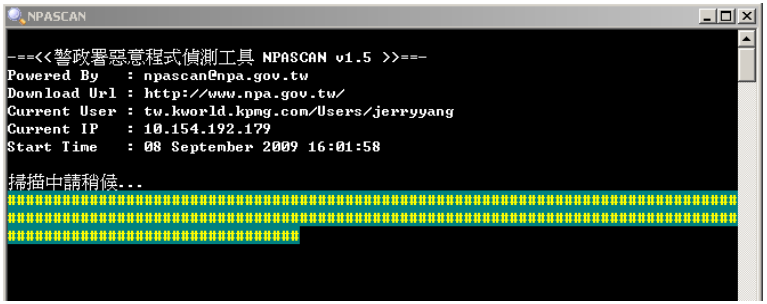
帳號密碼太多太難記，想靠電腦記憶省腦力，事實上電腦不一定比人腦可靠，專家指出，讓瀏覽器把密碼記下來，一旦電腦遭入侵，重要的帳號密碼就很容易被偷走，建議民眾除了時常更新密碼外，也不要把所有的帳號密碼存在同一個檔案裡。有沒有算過一整天使用電腦要輸入幾組帳號密碼？打開電腦，收發電子郵件、啟動即時通、進入部落格甚至是上網轉帳，一般人少說有四組以上的帳號密碼，更別談是電腦重度使用者，要靠腦袋瓜記住這麼多數字，光想就暈頭轉向，不少人為了方便使用，乾脆讓電腦幫忙記住密碼，不過專家提醒，電腦被入侵，最大的損失通常是帳號密碼被竊取，而讓伺服器記憶密碼，其實藏有潛在風險。

Cookies可以提供哪些資料?

如何刪除Cookie?

電腦健康檢查程式：NPASCAN

- 警政署資訊室特別研發迥異於市售防毒軟體掃毒模式之最新"健檢程式"，此「個人電腦健康檢查程式NPASCAN」可有效偵測目前市面上防毒軟體無法清除之病毒
- 採用行為分析模式進行偵測與防毒軟體之特徵碼比對模式不盡相同，因此沒有更新病毒碼之困擾，亦不需常駐於系統中。
- 下載資訊：http://rogerspeaking.com/index.php?dl_id=5



網頁威脅防禦工具：趨勢科技 Web Threat Protection (WTP)

- 有效在連線上網時抵擋惡意連結及背景下載，避開與病毒接觸的機會
- 下載資訊： http://www.trendmicro.com.tw/wtp/micro/index.asp

檢查個人電腦密碼設定原則

- 點選[開始]→[設定]→[控制台]→[系統管理工具]→[本機安全性設定值]→[帳戶原則]→ [密碼原則]/[帳戶鎖定原則]

關閉郵件預覽

- 點選[檢視]→[讀取窗格]→[關]

設定螢幕密碼保護程式

- 於桌面點選滑鼠右鍵，選則「內容」

檢查系統漏洞修補情形

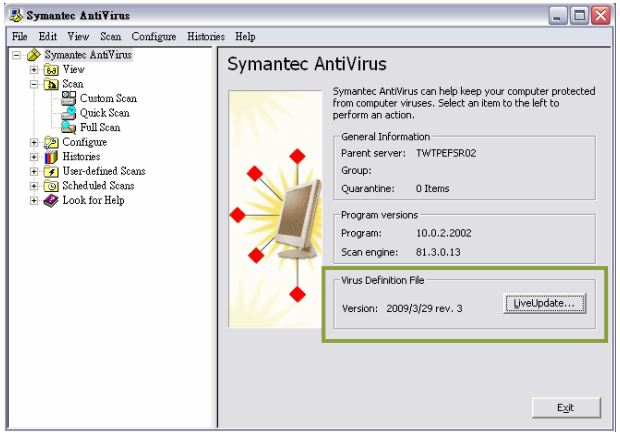
- [開啟IE]→[工具]→[Window Update]

如有下列情形，請洽電腦維修人員：

- 更新失敗
- 與其他同仁更新狀態不同
- 長期未有更新紀錄

檢查病毒碼更新狀態

- 點選右下角Symantec的盾牌查看到更新日期



確認軟體合法性

- 點選【開始】→【設定】→【控制台】→【新增或移除程式】→【變更或移除程式】→點選【移除】將非法軟體移除。

養成資安好習慣

- 不明人士要盤查(不明電腦連線也要禁止)
- 社交工程要小心(包括電話、電子郵件等途徑)
- 電腦不用要登出(下班要關機)
- 機密資料要保護(善用加密功能及軟體)
- 密碼設定要穩固(善用密碼設定小技巧)
- 重要資料要備份
- 應用系統要更新(杜絕已知的系統漏洞)
- 電腦防毒要更新
- 瀏覽網路要提防(提防網路釣魚、惡意程式碼)
- 電子郵件要過濾(垃圾郵件為電腦病毒及木馬感染途徑)

ISO 27001 簡介

教育體系資通安全管理規範

資訊資產管理

實體環境安全管理

個人電腦資安防護秘笈

2010年校園資安管理的新挑戰

Q & A

個資法篇

評比面向	現況	未來重要修法方向
名稱	電腦處理個人資料保護法	個人資料保護法
個人資料規範範圍	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、社會活動及其他足資識別該個人之資料	外加護照號碼、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式，其他得以直接或間接方式識別該個人之資料
法規適用行業	公務機關、徵信業、醫院、學校、電信、金融、證券、保險及大眾傳播業	所有行業均適用
個資法舉證責任	由民眾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
資料外洩通報責任	無規範	資料管理機關對資料盜失事件需主動告知

個人隱私外洩

新聞來源：聯合報 05/30/2009

- 數百教師個資 百度看光光
- 案例說明：

台中縣教育處日前彙整各國中、小學的認輔教師名冊，公告上網後兩、三天，即發現數百名國中、小教師的個人資料，被大陸最大入口網站「百度」蒐羅，包括服務學校、住址、電話、生日、身分證號碼及電子郵件信箱等個人資訊，皆可供公眾查詢。教育處經不斷連繫百度撤除，連發十幾封電郵給百度，該網站才將這些個資全撤除，但教師資料已於搜尋網站上公開約十天。

資安事故原因分析

資料管理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。

矯正及預防措施

1.必要公布之敏感資料應加密保護，利用電子憑證、簽章等限制存取權限。
2.審視機關個人資料保護之規範，制訂控制措施。

系統開發疏失

新聞來源: 蘋果日報 06/27/2009

- 國科會網站洩1.8萬個資 身分證字號學號全都露
- 案例說明：

國科會於2008年建置之「大專學生參與專題研究計畫通過案件綜合查詢資料庫」，收錄1997至2009年獲國科會專案補助的研究計劃。民眾發現只要把滑鼠游標移到學生姓名的連結上，瀏覽器左下方就會出現該生的身分證字號和學號，總計有一萬八千名學生的個資可供查詢。經媒體投訴，國科會查證後才發現程式有漏洞，已緊急修補。

資安事故原因分析

資訊系統於開發過程中，未考量及確認相關的安全要求及測試，導致開發上程式的疏失洩漏個人資料。

矯正及預防措施

制訂資訊系統變更或上線之安全要求，並落實程式及資料之安全控制程序、測試與稽核。

委外系統遭入侵

新聞來源：中央社 06/25/2008

- 遭駭客入侵 高市教育局加強網路機密維護
- 案例說明：

高雄市國中校務行政系統委由廠商開發維護，日前遭駭客入侵，國中學生資料被竊取，供補習班招生宣傳、寄送資料之用，目前調查尚無其他用途。高雄市政府教育局已與負責廠商聯繫，將入侵程式移除，並修補程式漏洞。

資安事故原因分析

未對委外廠商之服務提供進行必要的監視與稽核，以致於廠商開發之程式漏洞洩漏學生之個人資料。

矯正及預防措施

1. 應確保與委外廠商之合約中列入資訊安全責任及維護之協議。
2. 建立系統委外的安全控制機制，定期監視及稽核合約廠商。

個資外洩對教育機構可能造成之衝擊

- 造成機關學校形象受損
- 失去師生與家長之信任
- 相關人員面臨個資法等法律制裁
- 可能必須負擔鉅額賠償

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

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