107年國立東華大學圖書資訊中心（花蓮區域網路中心）教育訓練 -

資訊安全的基礎認知

國立東華大學整理

107年 08月01日(三)

大綱

前言

- 課程說明

一、資安概要

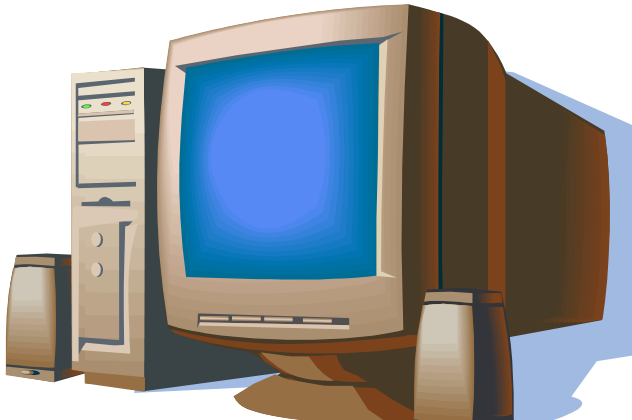
- 資訊安全與風險
- 資訊安全範圍
- 資訊安全管理制度組成

二、資安管理的挑戰

- 資安的威脅
- 社交工程
- 勒索軟體
- 如何防範

三、補充資料

- 未來攻擊趨勢 - 漏洞攻擊
- 未來攻擊趨勢 - 挖礦程式



一、資安概要

- 資訊安全與風險
- 資訊安全範圍
- 資訊安全管理制度組成

司法院及所屬網路遭駭

司法最新動態

公告日：	107.03.17
發布單位：	資訊處
標　　題：	有關司法院及所屬網路遭網軍攻擊事宜新聞稿
檔案下載：	1070317新聞稿.doc

有關司法院及所屬網路遭網軍攻擊事宜新聞稿

有關司法院及所屬網路遭網軍攻擊事宜，本院說明如下：

一、事實經過：107年3月7日20時30分許，司法院發現院內內網傳閱主機遭駭客入侵並下載駭客工具攻擊台北地院公文主機。該傳閱主機於當晚隨即關機，使用防火牆等資安設備阻斷連線。本院依法通報行政院國家資通安全會報技術服務中心通報本事件。於3月8日上午，經資安顧問協助鑑識，發現台南地院電腦教室之XP型電腦，前曾於107年1月11日攻擊本院傳閱主機並安裝惡意程式，而上開台南地院電腦前已於106年12月27日遭駭客從國外IP（目前僅知係來自巴基斯坦的帳戶）入侵成功，植入零時差電腦病毒（該病毒為新型病毒，嗣於107年3月9日始經趨勢科技公司確認為新品種病毒）。事後分析查證結果，提供本院及所屬各機關同仁之單一登入系統之帳號密碼，疑似已遭駭客以該電腦病毒入侵竊取。

二、司法院資訊處於3月8日已經採取的措施：(1)協同APT防衛系統廠商，立即檢測本院所屬各機關電腦遭入侵的情形，儘速將病毒清除阻絕。(2)全面清查全國法院還有多少台XP型電腦（台南地院電腦教室的電腦，就是XP型電腦而遭入侵），將儘速檢討該型電腦在網路系統中所扮演之角色。(3)全面在本院主機上佈建APT防衛系統，以期儘早偵測發覺電腦有遭入侵之情形。

三、經為時一週之清查後，本院目前已將受病毒感染之情況確認並控制住，目前已掌握之情況如下：

(一)遭植入之病毒有兩組，15支程式（詳細內容、名稱暫時保密）。

(二)受感染的電腦數目為243台（約百分之九十為XP型電腦、其餘百分之十是windows2003型電腦）。

(三)受入侵的法院總數是29個法院。

(四)尚未查出有入侵裁判書系統竄改裁判書之情形。

四、司法院將於再次確認受感染範圍後，封鎖殺除已經發現的病毒，並且全面更新帳號密碼，俾使駭客不能再入侵電腦系統。

一連串的流程

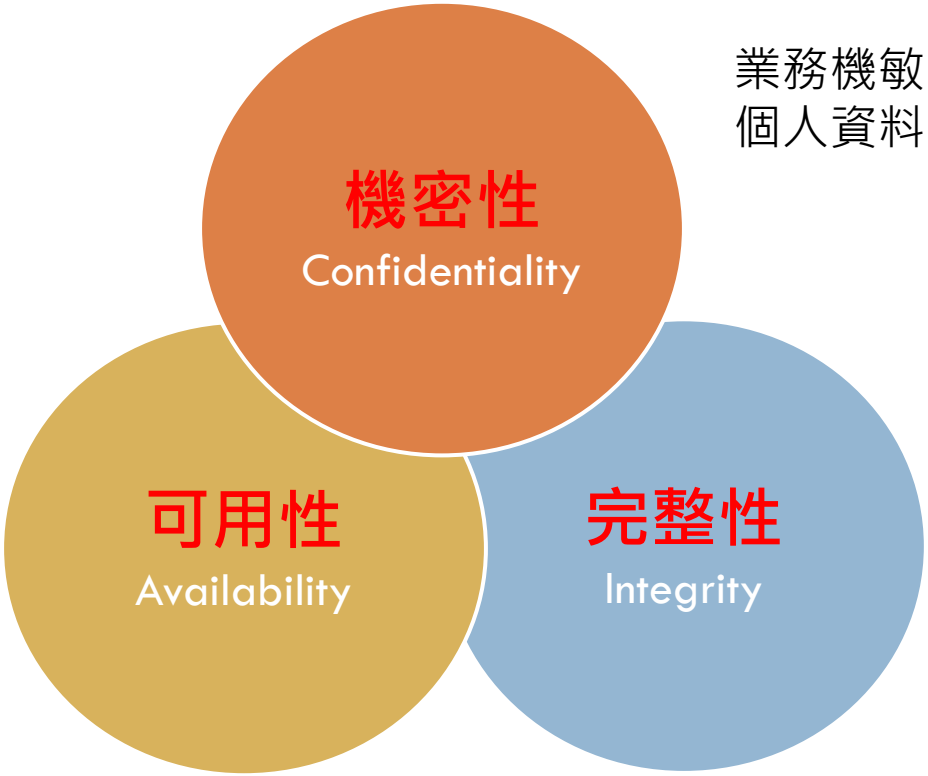
第一銀行盜領案

1. 從分行入侵內網
2. 建立內網潛伏基地
3. 暗中蒐集入侵情報
4. ATM入侵
5. 開啟ATM遠端控制
6. 植入ATM控制木馬，發動盜領

資料來源：iThome 2016-07-25 https://www.ithome.com.tw/news/107294

資訊安全與風險

- 資訊安全的概念在保護單位的資訊資產，避免資訊資產遭受各種威脅及降低可能的危害。



業務機敏資料、
個人資料外洩

服務中斷、
資料無法存取

資料遭到竄改

資訊安全與風險

- **機密性：**

  確保只有**經授權**的人才可以取得資訊，避免資訊洩漏。

- **完整性：**

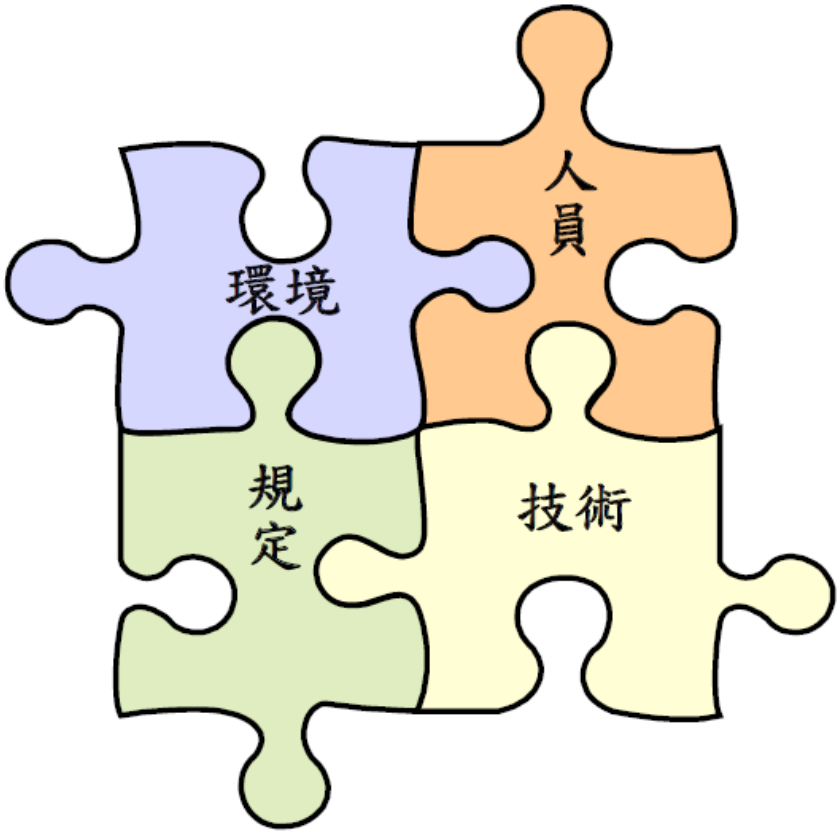
  確保資訊不受**未經授權**的竄改與資訊處理方法的正確性。

- **可用性：**

  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。

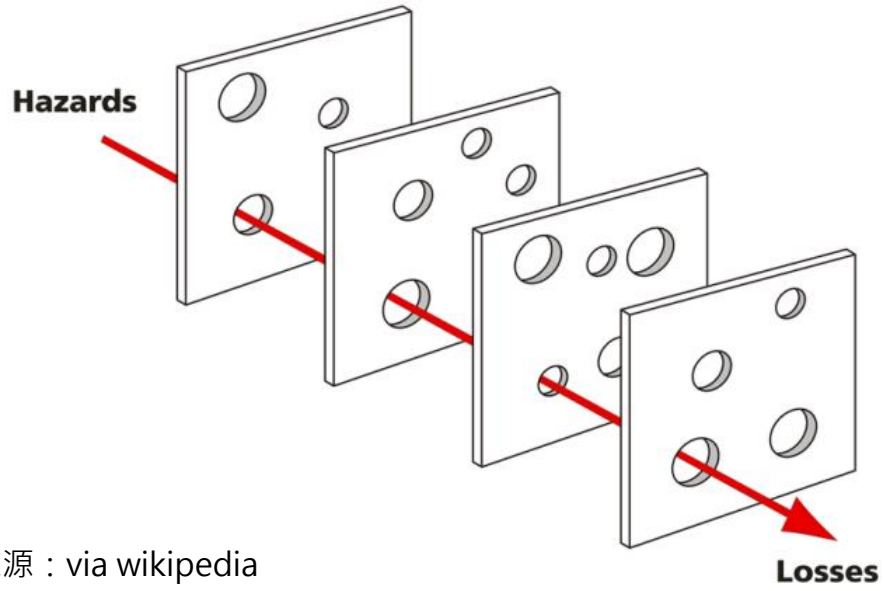
資訊安全範圍

- 資訊使用之「環境」
- 資訊使用之「技術」
- 資訊使用之「規定」
- 資訊使用之「人員」



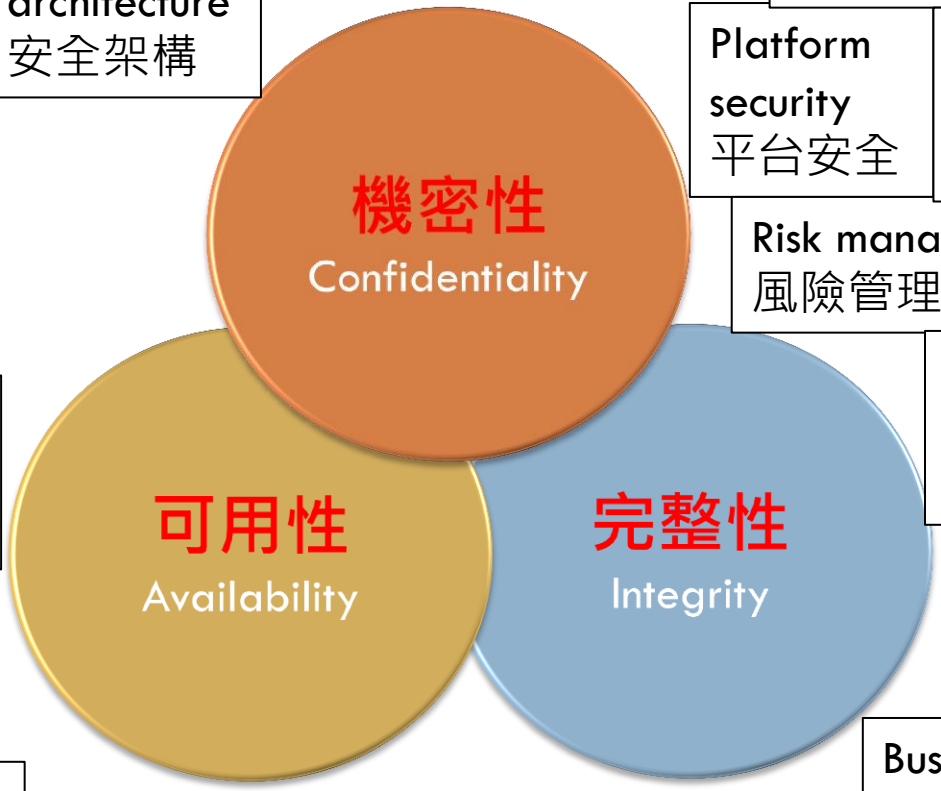
瑞士乳酪理論

- **瑞士乳酪理論**(Swiss Cheese Model) 形容意外事件發生，只是湊巧同時穿過每一道防護措施的漏洞，有如層層乳酪中湊巧有一組孔洞的集合，能讓一直線穿過。只要當時任何一個環節有做到保護，錯誤事件就不會發生。



圖片來源：via wikipedia

資訊安全管理制度組成



Incident response & crisis management
意外事件回應與犯罪管理

Security architecture
安全架構

Firewall & connectivity management
防火牆與連線安全

Platform security
平台安全

Monitoring & intrusion detection
監督與入侵偵測

Password management
密碼管理

Risk management
風險管理

Physical Security
實體安全

Penetration testing
滲透測試

Authentication & access control
身份驗證與存取控制

Fallback Planning
還原計畫

Certificate registration & management
認證註冊與管理

Business continuity Management
企業永續運作管理

Personnel security
人員安全

Virus prevention & detection
病毒防治與偵測

Infrastructure security management
基礎建設安全管理

Encryption加密

資訊安全弱點與威脅

- **弱點：**

是導致威脅發生的原因，不會直接導致資訊資產的損害。

- **常見的弱點：**

- 未受訓練或具備安全認知的人員。
- 錯誤的選擇及使用密碼。
- 缺乏存取控制、資料未備份...

資訊安全弱點與威脅

- **威脅：**

任何會直接導致資訊資產受到損害的人事物。

- **常見的威脅：**

- 人員操作錯誤、惡意破壞資訊及設備。
- 病毒感染、系統被入侵。
- 社交工程...等等事件。

公部門被駭　民眾個資洩漏

http://news.ltn.com.tw/news/life/paper/1091662

公部門防駭 今起資安演練到年底

2017-04-05

〔記者李欣芳／台北報導〕近一年來中央與地方政府各公務機關不斷發生遭駭客攻擊的重要資安事件，甚至導致涉及洩漏民眾個資高達十三萬筆，引發各界的重視，行政院將從今天清明節連假後的第一天上班日起，展開全國各公務機關的資安演練，這項演練行動將持續到今年底。

近期政府機關發生重大資安事件，行政院啟動個別專案資安查核進行檢討，並補強資安防護。（情境照）

行政院相關官員表示，演練包括中央與地方政府的公部門，將由負責這次演練的官員擔任攻擊手，測試資安應變能力，因此不便透露由哪個部門開始進行演練。

由於民眾向公務機關申請相關業務時，依法必須提供個人資料才能申辦業務，不過，中華郵政去年五月發生個資遭竊，造成消費者個資外洩一萬七千多筆，勞動部去年十月被駭外洩三萬四千筆個資、台北市資訊局今年一月也外洩七萬筆個資，外交部今年二月更發生不明來源ＩＰ成功駭入我數十個外館領務信箱，導致國人登錄出國資料的一萬五千多筆個資外洩，外交部領務局更因此召開記者會致歉。

行政院官員表示，近期政府機關發生重大資安事件，行政院立即啟動個別專案資安查核進行檢討，並補強資安防護，這次資安演練也盼提升公部門的資安防護能量。

資料來源：自由時報

二、資安管理的挑戰

- 資安的威脅
- 社交工程
- 勒索軟體
- 如何防範

駭客攻擊模式

- **過去**

  資訊系統侵入、破壞的知識僅由少數駭客掌握，學習相關技術有較高的門檻。

- **現在**

  駭客工具、病毒碼隨手可得，直接使用、快速學習人人都可以成為駭客，24小時進行漏洞攻擊。

資安的威脅

- **社交工程(Social Engineering)**

  利用人性弱點，應用簡單的溝通和欺騙技倆，以突破安全防護，遂行其非法的存取、破壞行為。

- **阻斷存取式攻擊（Denial of Access Attack）**

  勒索軟體被人歸類於此。

詐騙集團

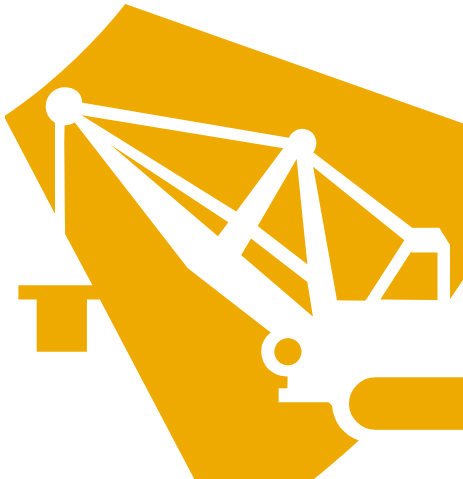
老婦收假檢警傳票 還騙警匯錢是「給孫子買房」

- 上月28日近中午時刻，陳婦前往銀行要提領90萬元，行員通知警方後，老婦態度變得很緊張，警方到場時，詢問老婦是否有手機，想要察看手機內是否有詐騙訊息，老婦則表示「我沒有電話」，並表示自己要領錢給孫子買房。
- 老婦的口袋內有一張「密件」，疑似為假檢警的通知書，要老婦將錢領出代為保管，老婦起初還否認有收到地檢署的通知書，直到警方循循善誘，老婦才將該張「手寫的通知書」拿出。

資料來源：自由時報 2018-07-21 http://news.ltn.com.tw/news/society/breakingnews/2495240

網路釣魚

- 網路釣魚（Phishing)是網路上常見到的社交工程，特別是利用E-mail來欺騙。
- 只要使用者警覺性不足，點選網頁連結或是開啟來路不明郵件附件檔案都可能被植入惡意程式。
- 當收到不尋常或是太好康的訊息，應思考訊息內容的可行性。



願者上鉤

引毒上身？五成網友主動下載有毒影音檔、電子郵件

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。

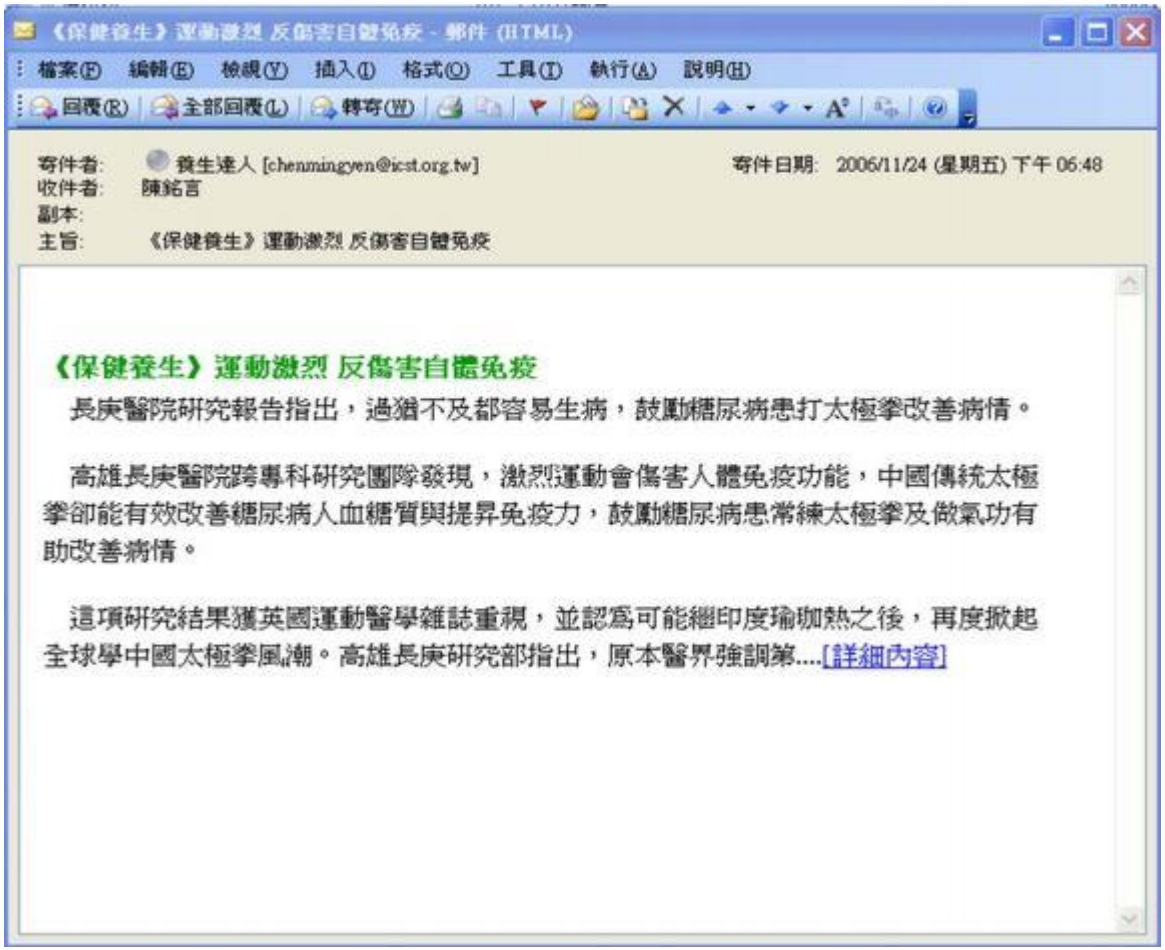
調查還顯示，網友最容易點選「跟搜尋結果相關的網站」（42.3%）及「好友寄的信件或訊息」（29%）而上了有毒程式的釣鉤，誤入電腦被駭的危機。而另外依序還有「免費試玩或下載」（13.9%）、「火辣性感圖」（7.3%）及「折扣好康」（5.7%）等誘人資訊也會讓網友忍不住點選。
透過交叉分析也發現有趣的現象，會被「折扣好康」內容吸引的女性網友為男性的三倍，而「火辣性感圖」的內容吸引者則大多數為男性網友。

資料來源：今日新聞 2009-04-01 https://www.nownews.com/news/20090401/914705

常見的釣魚方式有哪些?

- 利用電話佯裝資訊人員，騙取帳號及通行碼。
- 偽裝委外廠商之維護人員或上級單位人員，乘機騙取帳號及通行碼。
- 利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及通行碼，如網路釣魚。
- 利用電子郵件誘騙使用者開啟檔案、圖片，以植入惡意程式、暗中收集機敏性資料。
- 利用提供工具、檔案、圖片為幌子，誘騙使用者下載，如偽裝的修補程式 、p2p 下載軟體、工具軟體等，乘機植入惡意程式、暗中收集機敏性資料。
- 利用即時通訊軟體，偽裝親友來訊，誘騙點選來訊中之連結後中毒。

社交工程信件


《保健養生》運動激烈 反傷害自體免疫 - 郵件 (HTML)
檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)
回覆(R) 全部回覆(L) 轉寄(W)
寄件者: 養生達人 [chenmingyen@icst.org.tw]
寄件日期: 2006/11/24 (星期五) 下午 06:48
收件者: 陳銘言
副本:
主旨: 《保健養生》運動激烈 反傷害自體免疫
《保健養生》運動激烈 反傷害自體免疫
長庚醫院研究報告指出，過猶不及都容易生病，鼓勵糖尿病患打太極拳改善病情。
高雄長庚醫院跨專科研究團隊發現，激烈運動會傷害人體免疫功能，中國傳統太極拳卻能有效改善糖尿病人血糖質與提昇免疫力，鼓勵糖尿病患常練太極拳及做氣功有助改善病情。
這項研究結果獲英國運動醫學雜誌重視，並認爲可能繼印度瑜珈熱之後，再度掀起全球學中國太極拳風潮。高雄長庚研究部指出，原本醫界強調第....[詳細內容]

社交工程信件


深坑老街「大團圓」，週休二日好去處 - 郵件 (HTML)
檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)
回覆(R) 全部回覆(L) 轉寄(W)
寄件者: 老饕 [chenmingyen@icst.org.tw]
寄件日期: 2006/11/24 (星期五) 下午 07:02
收件者: 陳銘言
副本:
主旨: 深坑老街「大團圓」，週休二日好去處
附件: 深坑老街「大團圓」，週休二日好去處.doc (20 KB)
大團圓鄰近深坑老街，佔地面積大，環境舒服，吃飽飯可在院子裡散散步。(圖／王以瑾攝影)
到深坑一定吃豆腐嗎？「大團圓」鄰近老街，營業面積相當廣，算是這一帶的地標，這裡也賣好吃的豆腐餐，還有紅糟豆腐、泡菜臭豆腐都很經典；大團圓鄰近深坑老街，但不在老街上，廣大的佔地讓客人有更大的使用空間，吃完飯可以在花園裡散散步，很適合帶小朋友的家庭...[詳見附檔]

常見的社交工程信件標題

信件類別	寄件者/信件標題
時事類	1Thome<1theme@yahoo.com.tw> 駭客攻擊 8 家券商 金管會：恐還有下波
知識類	黃泰豐<larry1217@gmail.com> 「食色性也」不是孔子說的
健康類	綠色地球<xm4nk499@yahoo.com> 別再用寶特瓶裝水了！各項研究告訴你它可怕的真相！
美容類	Hellen<hellen520@gmail.com> 染唇妝過時啦！2017跟著李聖經擦上微醺MLBB唇才最潮
生活類	韓流最前線<girlpretty@hotmail.com> 變更嬌小，惹人疼！「胖胖單品」逆轉勝
新奇類	李蓉芬<melody8056@msa.hinet.net> 小二生超狂造句 讓網友驚呼：他超懂人性
美女類	杜肯<kentdo5717@outlook.com> 正妹車服員神到了 曾是黑澀會美眉

勒索軟體

WannaCry

勒索軟體

- **兩種類型**
  1. 鎖住被害者的電腦，要求被害者必須繳納贖金，才能拿回電腦的控制權。
  2. 加密被害者電腦上的檔案，亦是要求被害者繳納贖金，才能拿到解密金鑰。

- **軟體舉例**
  1. WannaCry
  2. Petya

- **受害平台**

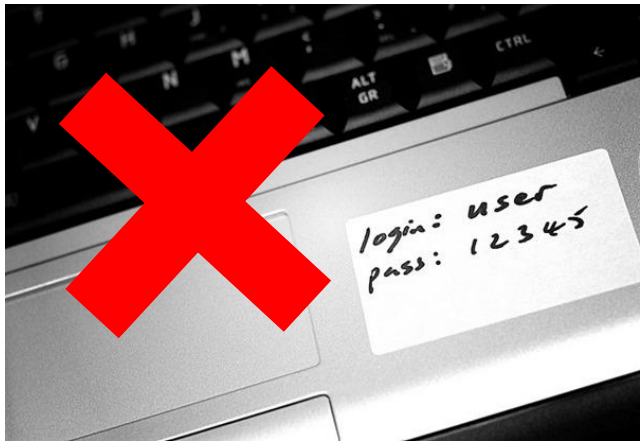
  大多都是以使用Windows作業系統為主的電腦設備，行動裝置暫無重大災情傳出。

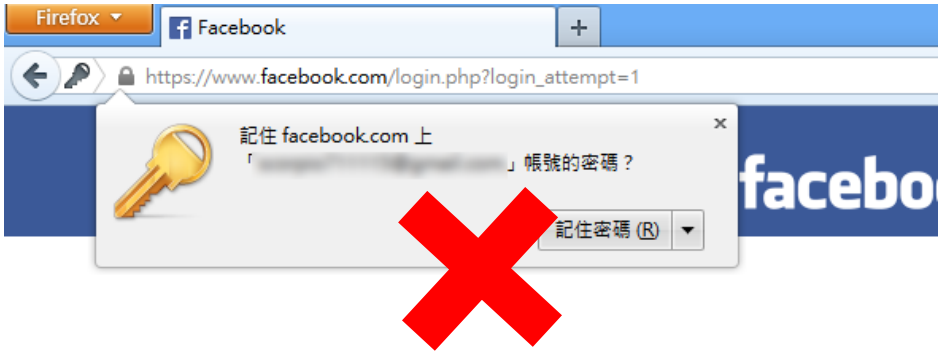
如何防範

1. 不要開啟未經確認的郵件與附件並關閉郵件預覽功能。
2. 不要點選可疑的網頁連結並關閉瀏覽器上的Flash、Active等元件。
3. 不要輕相信中獎、優惠、折扣、贈送、免費等不實訊息。
4. 要再三確認給予資訊者的身分，例如：電子郵件的寄件者身分、檔案提供者。
5. 確實安裝防毒軟體並定期更新、開啟防火牆。
6. 開啟作業軟體的自動更新。
7. 養成良好的備份習慣，例如：定期備份、多重備份、異機備份、異地備份。
8. 機敏資料應異地存取。

如何防範

- 帳密保管方式


login: user
pass: 12345


Firefox
Facebook
https://www.facebook.com/login.php?login_attempt=1
記住 facebook.com 上
」帳號的密碼？
記住密碼 (R)

ISO27000系列標準

- ISO/IEC 27000：資訊安全管理系統 - 綜述及詞彙
- ISO/IEC 27001：資訊安全管理系統 - 要求
- ISO/IEC 27002：資訊安全管理作業典集
- ISO/IEC 27003：資訊安全管理系統實施指導
- ISO/IEC 27004：資訊安全管理系統 - 測評
- ISO/IEC 27005：資訊安全風險管理
- ISO/IEC 27006：針對審查及認證資訊安全管理系統的實體之要求
- ISO/IEC 27007：資訊安全管理系統審查指導
- ISO/IEC TR 27008：資訊安全管理系統審查者指導
- ISO/IEC 27010：對於跨領域，跨組織間通訊的資訊科技，安全技巧及資訊安全管理
- ISO/IEC 27011：對於電信組織根據ISO/IEC 27002標準的資訊安全管理指導
- ISO/IEC 27013 ：ISO/IEC 20000-1 和 ISO/IEC 27001 整合實施的指導

ISO 27001:2013標準條文

0.簡介

1.適用範圍

2.引用標準

3.用語及定義

4.組織全景

5.領導作為

6.規劃

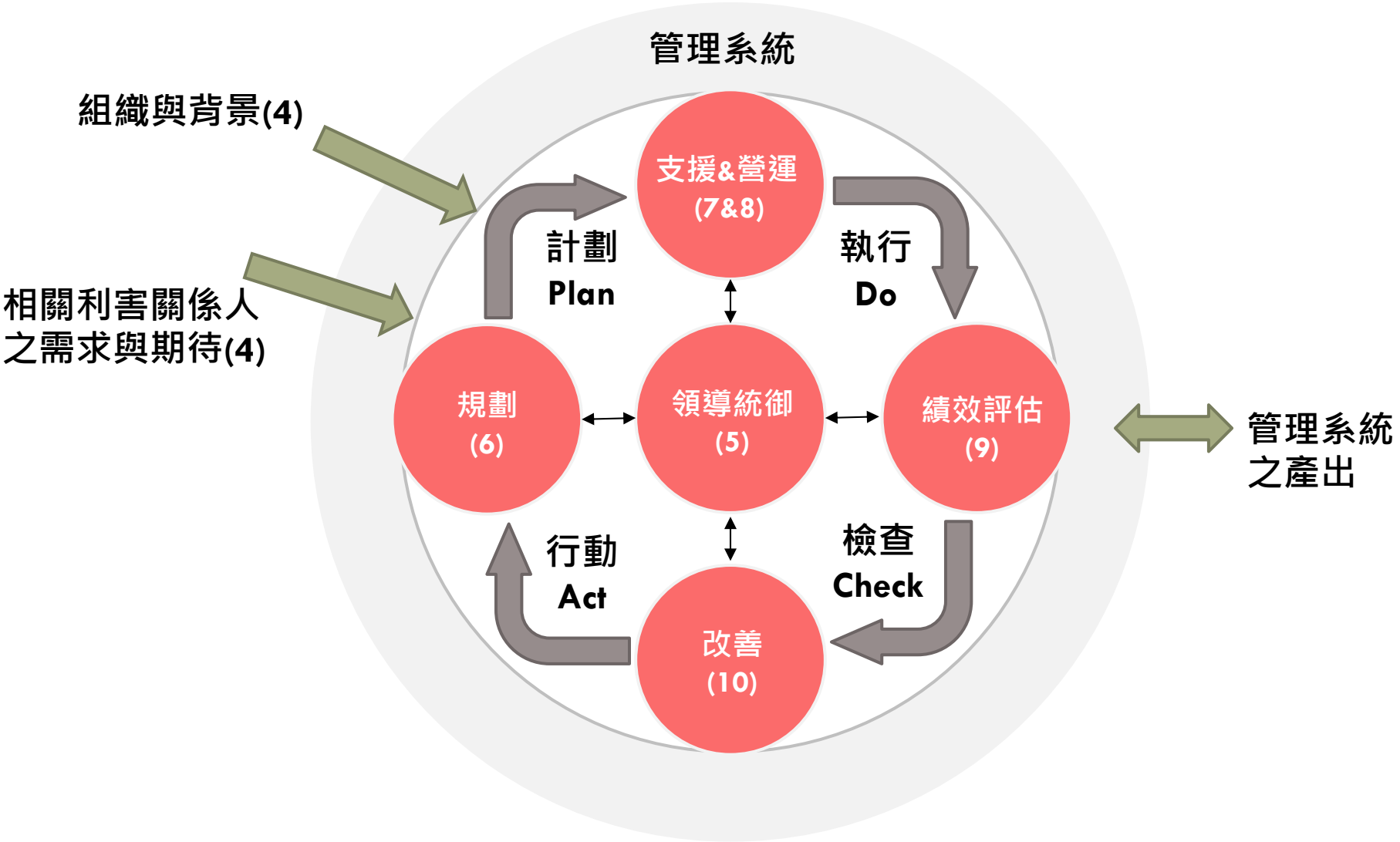
7.支援

8.運作

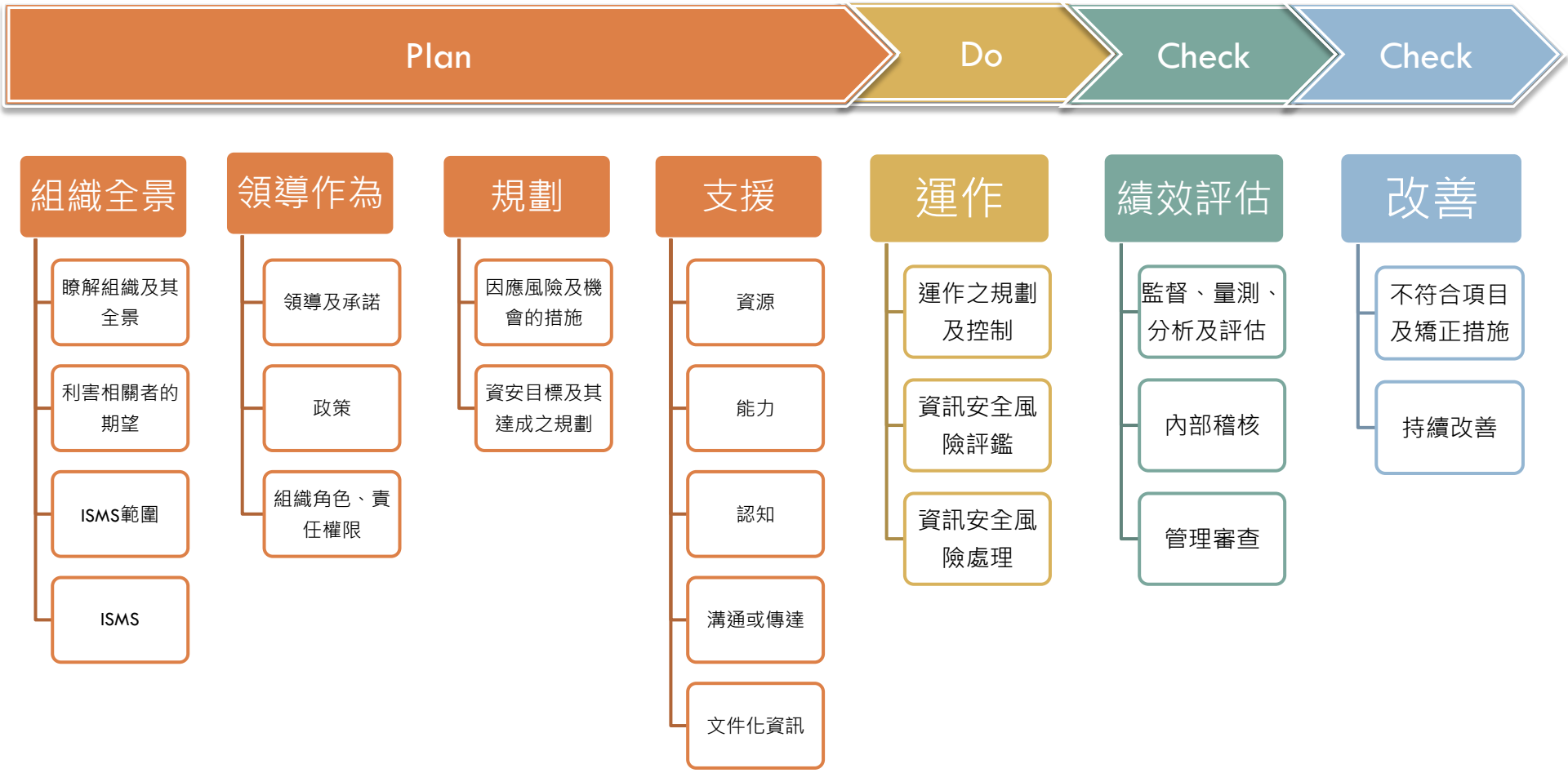
9.績效評估

10.改善

ISO 管理系統標準的高階結構（HLS）

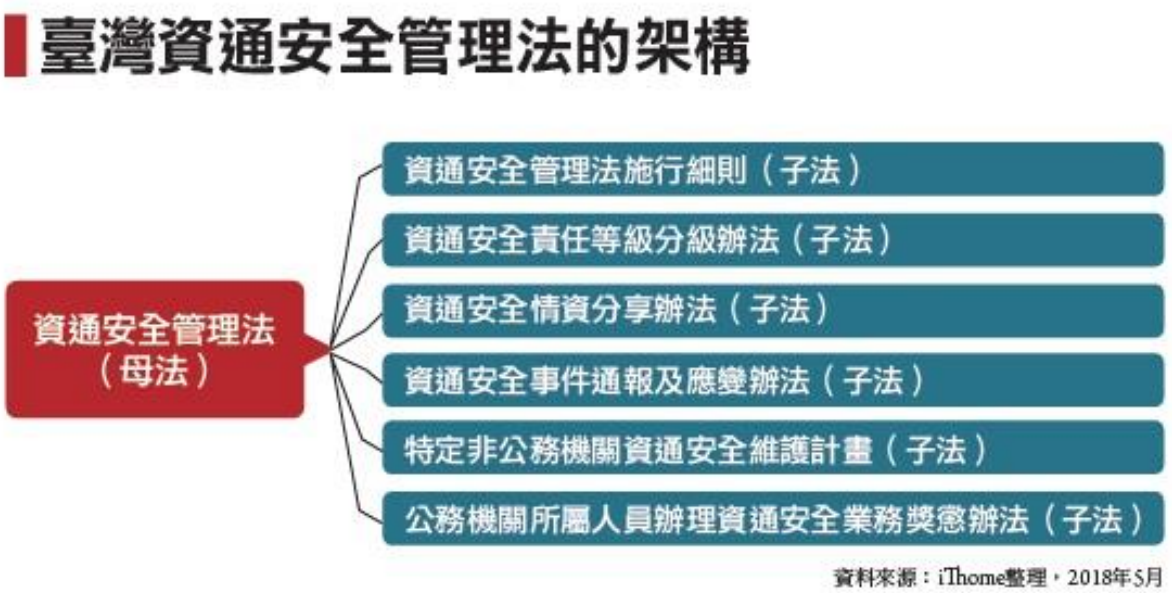


ISO 27001:2013 框架



資安管理法

- 今年5月11日立法院三讀通過《資通安全管理法》
- 公務機關最先適用資安管理法的規範
- 適用日期將訂在該法通過後的6個月生效



https://www.ithome.com.tw/news/123243

補充一

未來攻擊趨勢 - 漏洞攻擊

漏洞可能存在的地方

作業系統

- Windows、Linux、Android、MacOS．．等

服務套件

- OpenSSH、Apache、Adodb Flash．．等

通訊協定

- WEP、WPA2．．等

設備韌體

- 路由器、無線基地台、物聯網裝置．．等

零時差攻擊週期

定義：透過還沒有修補程式的安全漏洞進行攻擊之行為

漏洞攻擊防護建議

- 排定定期更新時程
- 嚴謹設備服務管理
- 良好的使用者操作習慣
- 多樣化資訊防禦系統

補充二

未來攻擊趨勢 - 挖礦程式

常見的虛擬貨幣

門羅幣
(Monero)

以太幣
(ether)

比特幣
(bitcon)

其他

挖礦程式感染方式

網頁掛碼

- 將挖礦程式掛碼於網頁中，讀取該網頁即開始挖礦

主機入侵

- 透過入侵主機後執行挖礦程式進行挖礦

程式內嵌

- 偽造或修改有名軟體(APP)讓使用者執行後挖礦

感染挖礦程式後的症狀

- CPU使用率上升
- 記憶體使用率上升
- 網路使用率上升
- 其他攻擊行為

挖礦程式的預防方式

避免連線可疑網站

定期修補系統

定期更新軟體

安裝防毒軟體

安裝外掛擴充套件

結束，感謝各位！

參考資料來源

一. 東華大學資安顧問

二. 教育體系資通安全暨個人資料管理規範

三. 恆逸教育訓練中心

四. 資安人

五. 台灣學術網路危機處理中心(TACERT)