資訊犯罪與資通安全管理

(資通安全認知(Awareness)與資通安全管理系統（ISMS))

林宜隆 博士
中央警察大學資訊管理學系、研究所教授
網路犯罪問題研究室召集人
TWNIC網路安全委員會委員
中華民國電腦稽核協會常務理事
中華民國資訊管理學會資通安全管理委員會主任委員
台灣電腦網路危機處理暨協調中心TWCERT/CC執行長

資訊犯罪與資通安全管理

- *台北市*「資訊倫理及法律責任」研習計畫:
- *加強台北市師生資訊倫理及法律責任之知識素養* 。 1.5小時
- *提昇師生*資通安全認知*與*資訊犯罪實例分析*瞭解*。 1.5小時
- *研習時間及對象：* 94年12月30日（星期五）3小時
- *對象：國小、國中、高中、高職及大專院校教師。*

資訊犯罪與資通安全管理
(資訊社會與安全管理)
報 告 大 綱

- 資通安全之迷思
- 資通安全與您何關？(安全VS犯罪?)
- 資通安全重要性與資訊犯罪
- 常見資通安全犯罪手法
- 資安法令宣導及案例分析
- 如何落實資通安全？

勾勒資訊化優質社會(e-Society)的藍圖

(資通安全與您何關？)

➢有關「NICI願景與推動策略」之提出，係基於資訊通信科技所帶動的技術變革，而作的國家資訊通信發展推動之規劃。

➢其內容，係以e-Taiwan爲願景，以基本建設、電子化政府(e-政府)、電子化產業(e-產業)及網路化社會(e-社會)爲推動架構，邁向高度資訊化優質的社會。(www.nici.nat.gov.tw),(www.gov.tw)

➢敵對國家可能發動資訊戰與網路戰

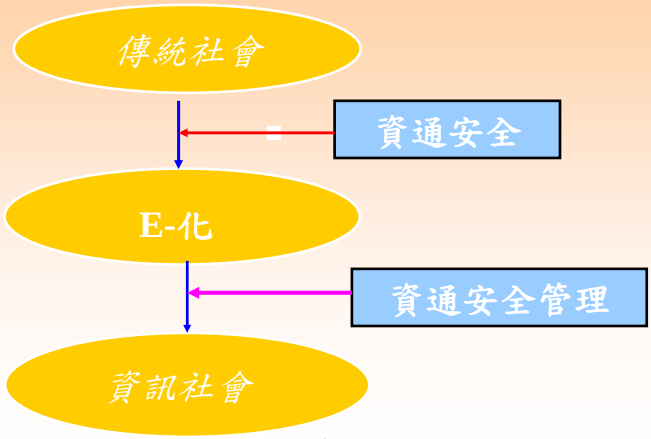
➢網路恐佈份子發動網路攻擊

➢犯毒、洗錢集團利用密碼技術造成執法機關在情報蒐集分析、防制及調查上的困難

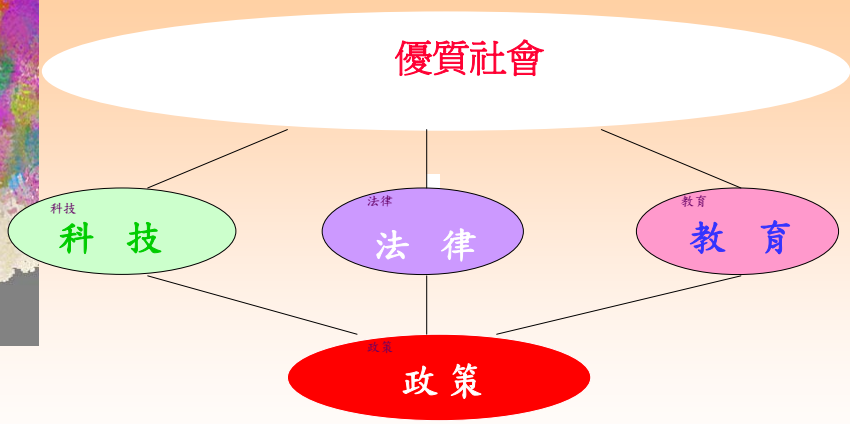
➢網路駭客破壞網路系統及重要資料

➢商業間諜竊取商業機密

建構優質資訊社會



建構優質資訊社會四大構面(PLSE)



重大駭客資安事件

- 2000年雙十節敏感時刻兩案駭客事件
- 2001年5月年美中駭客大戰我國亦遭波及
- 2002年7月大陸駭客入侵我國政府200餘台電腦主機
- 2002年9月大陸駭客法輪功爭議蓋台事件
- 2003年9月大陸駭客企圖大規模癱瘓我國電腦系統事件(國內共有88家廠商（單位）被駭客入侵植入木馬程式)。
- 2004年3月總統大選大陸駭客竄改網頁。
- (2004年7~9月?)（Phishing，高雄縣、台南市及基隆市政府網站)
- 2005年攻防演練、駭客入侵(大考中心) (5月) 、外交部網站(6月)、系統漏洞、電腦病毒、 網路詐騙、網路自殺等資安事件

公私機構可能面臨的資訊安全事件

- 內部人員不當存取網路97%
- 電腦病毒 90%
- 攜帶型電腦偷竊 69%
- 內部人員未經授權存取資訊 55%
- 被阻斷提供服務32%
- 入侵 31%
- 資訊竊取26%
- 破壞資料及網路 19%
- 通訊詐欺17%
- 財物詐欺 14%
- 無線竊聽13%
- 有線竊聽 2%

Sources: Issues and Trends:CSI/FBI Computer Crime and Security Survey, www.gocsi.com

資通安全管理(三部曲)

(資安文化)+(資安落差)

E(M)-Taiwan → (*資通安全管理*) → *E-Society*

(林宜隆,2001~2008)

資通安全認知、人人有責

資通安全管理、人人做到

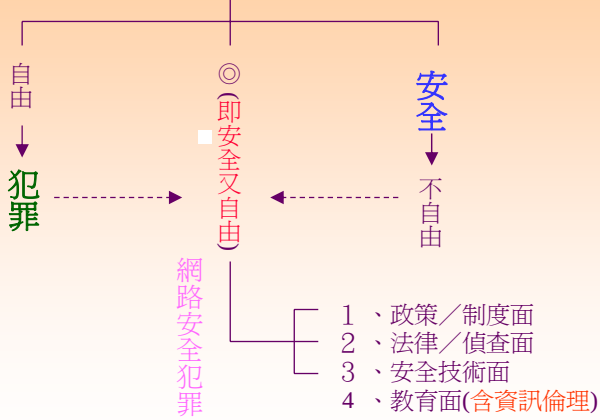
強化資通安全體系，打造資通安全環境

推動**M台灣**資安月，建構安全**S-Taiwan**

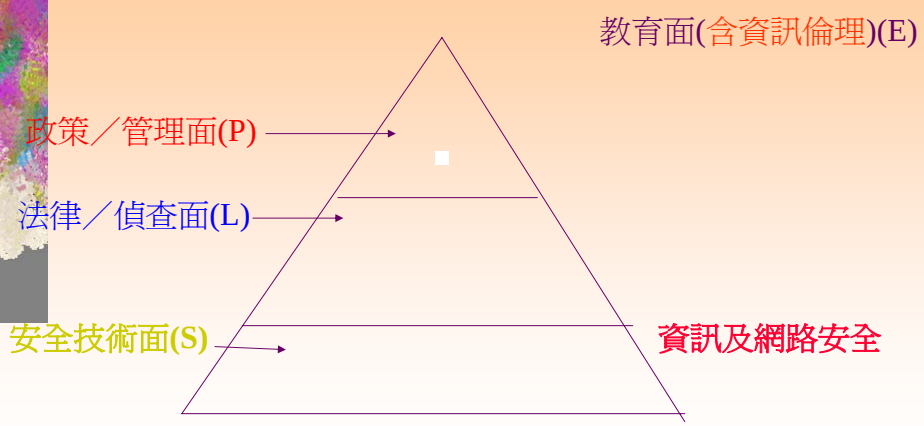
資通安全認知的意義

- NIST SP 800-16[Mark Wilson,1998]認爲認知是一個**改變人或組織態度和觀念的學習過程**，以了解安全的重要和當他失誤時的反面結果 。
- NIST SP 800-50[Mark Wilson and Joan Hash,2003]文件中，認知的目的很簡單，是要將注意力**著重在安全**，認知意指**給予個人識別資通訊科技安全考量並能相對的作出回應**。
- Chelsa Russell[Chelsa Russell,2002]認爲認知目的是**提昇安全與安全控管重要性的集體認知**，資通安全認知**訊息必須簡單清楚**並讓目標對象**很容易了解**。

資訊社會的犯罪概念
(資通安全之迷思)



網路安全與資訊犯罪(PLSE)



資訊社會與資通安全管理

(資通安全管理系統架構（ISMS))

- **PLSE**
- 網路政策與資通安全(政策面)-P
- 資訊犯罪與安全管理(法律面)-L
- 網路安全與危機管理(安全技術面)-S
- 資訊社會與數位內容(教育面)-E

資通安全威脅

OECD推動全球資安文化

什麼是資安文化，
誰是**participants?**
政府、企業、社會
及個人要各盡何種責任?

國家資通安全基礎建設

- 90年1月17日行政院第2781次院會通計畫並成立行政院國家資通安全會報
- 資通安全保護課題(PLSE)

1.安全管理政策　2.物體實體安全
3.人員安全管理　4.安全規章法律
5.硬體設備安全　6.軟體系統安全
7.網路通信安全

國家資通安全目標

- 積極防衛資通設施，維護國家運行體制
- 建立資通安全優勢，提升國家競爭力量
- 堅實資通安全建設，健全網路社群發展
- 主動偵測安全威脅，降低實質危害因素
- 建構安全通報體系，強化事前預警機制
- 保障民眾隱私權益，促進網路多元發展
- 增強執法專業能力，有效遏止網路犯罪

我國資安機制計畫全程計畫目標
(第一期:90~93年)

第一階段目標

(*90*年*1*月至*91*年*12*月)

建立國家資通安全基本防護能力

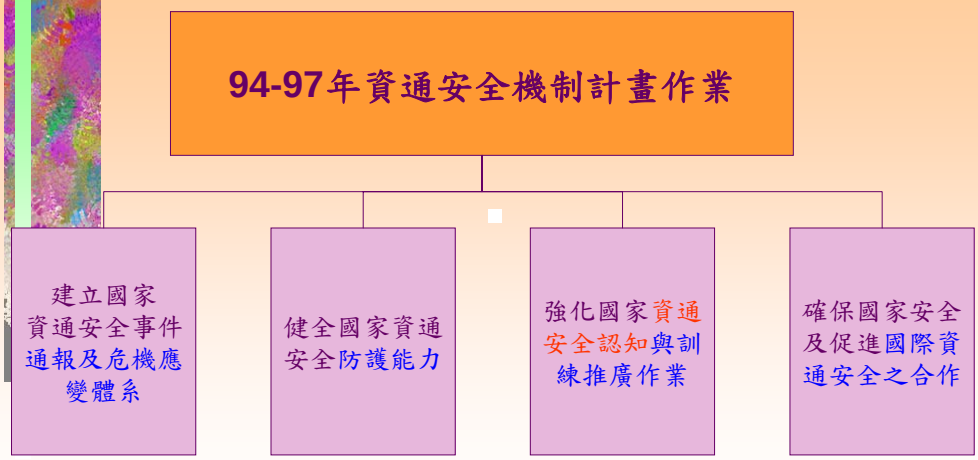
第二階段目標

(*92*年*1*月至*93*年*12*月)

建立國家資通安全整體防護能力

附件一

94-97年資通安全機制計畫作業架構



以上資料來源：國家資通安全會報，2004/12

美國911事件與英國77爆炸事件改變全球資通安全典範

◆世界突然變得不可預測、
毫無預警、時有危險
及威脅潛伏。

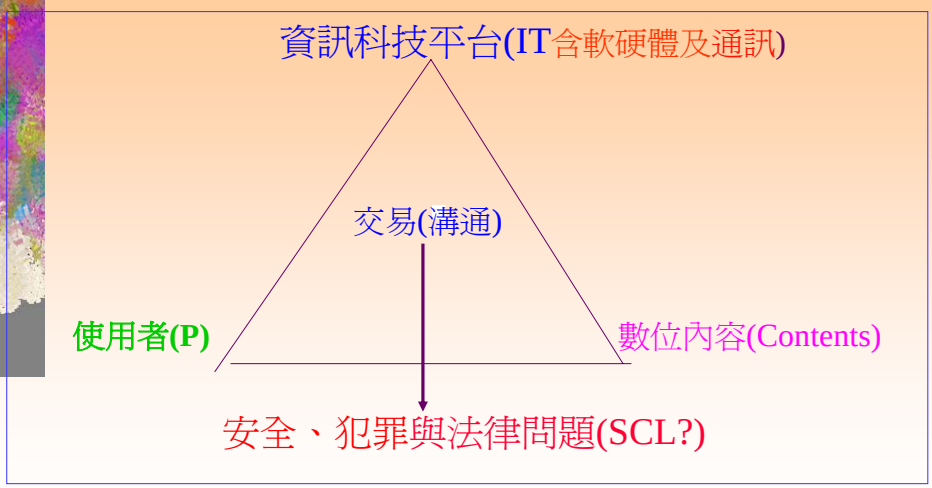
◆安全 .vs. 自由 (犯罪???)

加強推動資安認知(Awareness)

資通安全的最大威脅就是
:不知道威脅
或未能正確評估威脅；
推動Awareness
將是今後政府資通安全重點

資訊社會三個構面:(IT,C,P)

(資訊安全重要性) (林宜隆,2002~2008)



資通安全管理=CyberSecurity+CyberCrime+CyberLaw

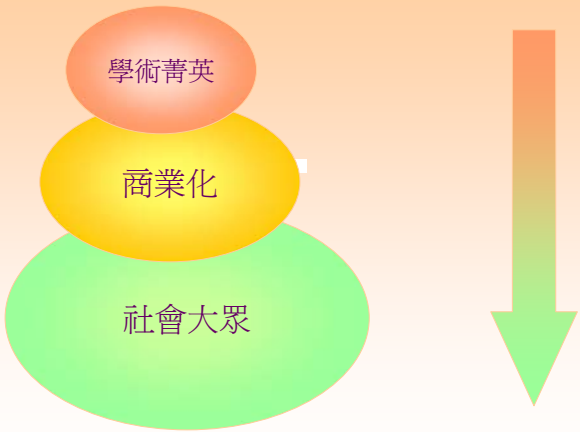
立法院92.06.03三讀通過刑法修正案，92.06.25總統公佈，新增妨害電腦使用罪專章(刑法第358~363條)-告訴乃論

- 第358條新增「無故入侵電腦罪」，凡無故輸入他人帳號密碼、破解使用電腦的保護措施或利用電腦系統的漏洞，而入侵他人的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。
- 第359條新增「保護電磁紀錄規定」則明訂，無故取得、刪除或變更他人電腦或其相關設備的電磁紀錄，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。
- 第360條「干擾電腦系統及相關設備罪」則規範駭客癱瘓網路的攻擊行為，凡無故以電腦程式或其它電磁方式干擾他人或其相關設備，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。

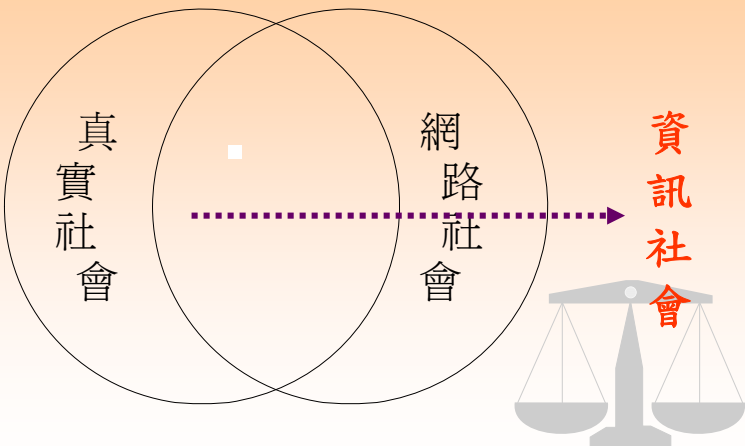
立法院92.06.03三讀通過刑法修正案，92.06.25總統公佈，新增妨害電腦使用罪專章(刑法第358~363條)-公訴罪

- 第361條由於公務機關的電腦系統若遭侵入，往往會造成國家機密外洩、有危及國家安全之虞，因此修正案規定，對於公務機關電腦或相關設備犯上述三條條文者，加重其刑至二分之一。
- 第362條「製作專供電腦犯罪之程式罪」則是針對電腦病毒程式的設計者，凡製作專供犯本章的罪的電腦程式，而供自己或他人犯罪，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。
- 第363條但上述三條(第358~360條)條文都是告訴乃論，必須由受害人提出告訴才受理偵辦。

知識經濟時代資訊社會的演進

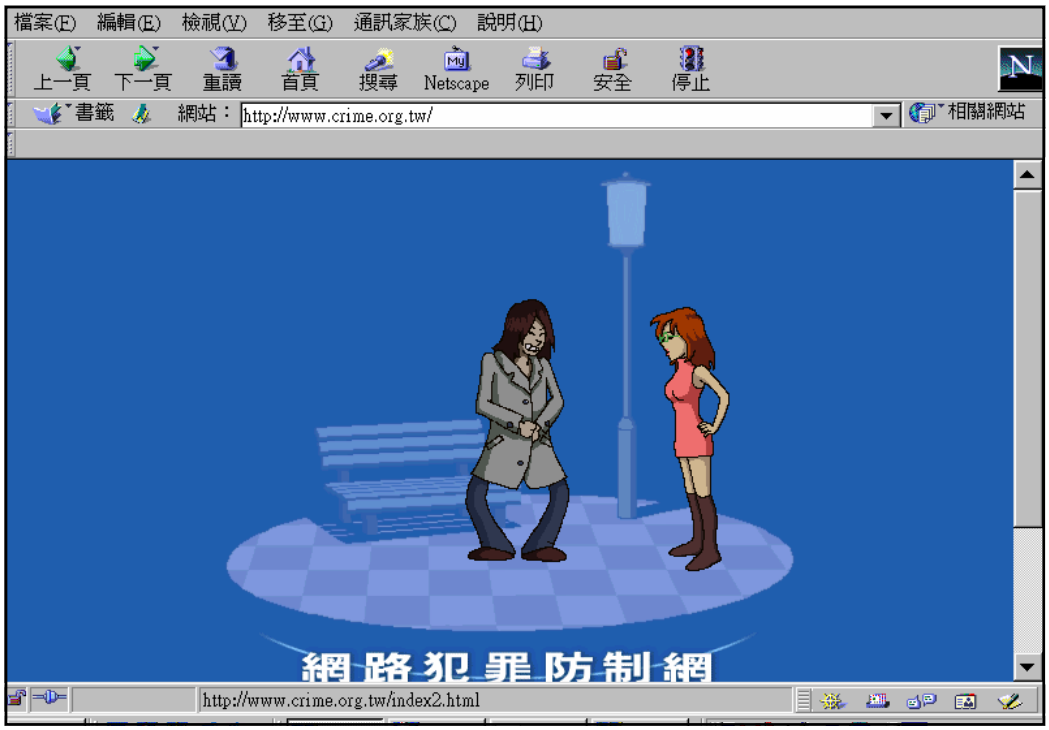


資訊社會與真實社會相互影響



📖E法律問題鳥瞰

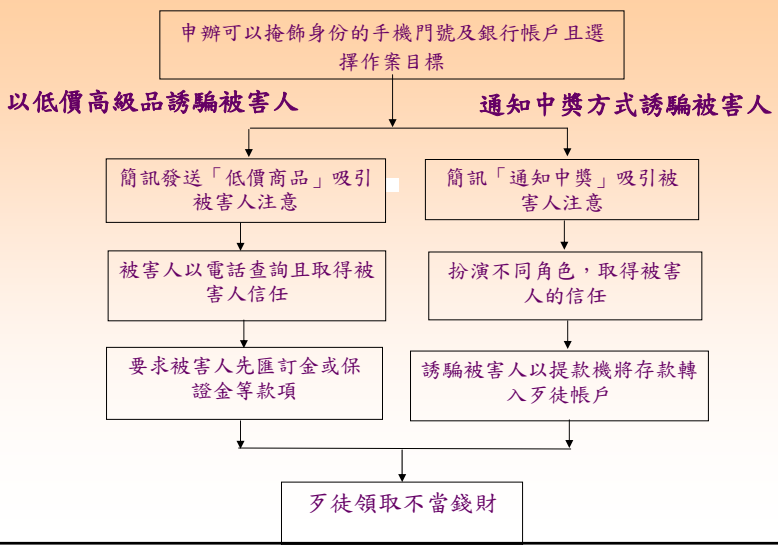
- 電腦犯罪(刑法修正案) 86年8月10日修正公布
- 妨害電腦使用罪專章(刑法修正案) 92年6月26日修正公布
- 個人資料保護(個資法修正案) 84年8月11日公布
- 智慧財產權(著作權修正案920605,商標法,專利法)
- 網路廣告規範,通訊保障及監察法 ,電信法
- 網路內容管理(網路色情,援助交際)(網路內容管理法?)
- 消費者購物保護
- 數位簽章(電子簽章法90.10.31三讀通過)
- 垃圾郵件(Spam Mail)(電子垃圾郵件管理辦法?)
- 北市版網咖管理條例 (90.11.14).
- **網路基本法、網路管理法和網路使用者管理辦法**等法律 ……etc. (資訊)網路犯罪



(資訊)網路犯罪案例分析

*案例一:*行動電話簡訊犯罪型態探討(常見資訊安全犯罪手法)

- 行動電話簡訊犯罪流程剖析



一、行動電話簡訊犯罪型態探討(續)

- 簡訊詐騙案例之犯罪分析(I)

三嫌偽造證件辦門號，傳簡訊詐財

犯罪時間：九十一年十月

犯罪地點：高雄

蒐集同學錄，剪下照片製作假身分證

↓

假身分證申辦手機門號，並以高價販售圖利且發送中獎簡訊進行詐財

↓

通信業者損失高額通信費

轉帳購手機錢被提光

犯罪時間：九十一年十月

犯罪地點：台中縣沙鹿鎮

以簡訊傳送兜售低價新型手機

↓

要求被害人先透過提款機匯款，進而騙取存摺中的大筆存款

↓

多位民眾同時收到此簡訊且受騙

二、網路拍賣詐欺案例之犯罪分析：

- 犯罪時間：民國九十年三月十日、十一日
- 犯罪地點：網路咖啡店
- 犯罪事實：曾姓嫌犯利用網路拍賣產品以假競標假交易的方式，通過評價制度的審核，讓網友失去戒心後，而網友們在參與競標電子產品，對方告訴網友只要先把前匯到指定的帳戶就會收到貨品，被害人左等右等還是等不到東西寄來才發現受騙上當。增姓嫌犯以同樣手法總共犯下一百多件詐欺案，所得金額高達好幾百萬 。
- 犯罪者剖析：曾姓少年、19歲。
- 犯罪造成損害：網友財務損失。
- 犯罪方式：以假競標的方式，通過評價制度審核結標後告知網友匯款至指定帳戶網友匯款後，從此音訊全無

以假競標的方式，通過評價制度審核

↓

結標後告知網友匯款至指定帳戶

↓

網友匯款後，從此音訊全無

三、線上遊戲寶物入侵詐騙案例之犯罪分析：

犯罪時間：民國九十二年十月起。

犯罪地點：網咖、家中。

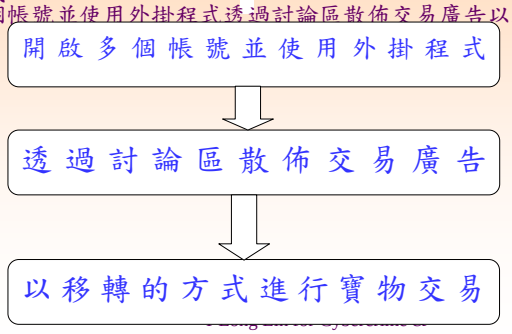
犯罪事實：嫌犯利用外掛程式，並搭配十多個帳號干擾遊戲程式進行，複製遊戲的錢幣、裝備等寶物。使線上遊戲的電腦主機當機，並到處張貼販售虛擬寶物的廣告。

犯罪者剖析：嫌犯張姓男子從事資訊工程工作，並與大陸駭客合作，利用外掛程式干擾線上遊戲程式。

犯罪損害：導致線上遊戲公司當機無法提供服務，並違反線上遊戲交易之平衡。

起訴罪名：以妨害電腦使用罪移送。

犯罪方式：
開啟多個帳號並使用外掛程式透過討論區散佈交易廣告以移轉的方式進行寶物交易



四、網路銀行虛擬鍵盤盜取帳號密碼案案例分析

犯罪時間: 民國94年4月間執行例行**網路巡邏**時發現。

犯罪地點: 臺中市。

犯罪事實: 陳嫌意欲突破「虛擬鍵盤」、「網路ＡＴＭ」及「晶片卡」等機制從中盜取存款，自行設計鍵盤側錄程式，成功破解四十餘家網路銀行的「虛擬鍵盤」，並成功蒐集被害人「電腦名稱」、「公司統一編號」、「銀行帳號」、「提款卡密碼」、「晶片卡密碼」、銀行網路之「使用者名稱」及「登入密碼」等近千筆資料。

犯罪者剖析: 陳ＯＯ，三十八歲，臺中人。陳嫌到案後坦承，因經商失敗而欠錢花用，才會想偏門賺錢。

犯罪損害: 此舉無疑是國內首件突破網路銀行的「虛擬鍵盤」安全機制案件，對網路金融交易秩序而言是一大資安警訊。案經刑事局前往陳嫌住處實施搜索，當場查獲犯案所使用之上網電腦、偽造金融卡、非法取得之他人金融卡磁條資料及卡片燒錄機、陳嫌所撰寫之木馬程式及解讀內容、側錄所得之他人相關資料等贓證物。

起訴移送: 陳嫌亦因此觸犯妨害電腦使用罪、妨害秘密、電腦處理個人資料保護法及偽造文書等罪嫌。

犯罪流程: 1.惡意撰寫鍵盤側錄程式。
2.以新版驅動程式名義，提供民眾下載使用。
3.暗中蒐集民眾的銀行機密資料。

偵查流程: 1.暗中蒐集民眾的銀行機密資料。(從網路上監看銀行機密資料的 流向，並追查流向之主機IP位置。)
2.以新版驅動程式名義，提供民眾下載使用。(追查提供驅動程式下載之電腦主機，並追查記錄檔查看何人提供原使檔案提供下載。)
3.惡意撰寫鍵盤側錄程式。(調查嫌疑人是否擁有電腦程式語言賺寫能力，追查嫌犯求學經歷以及相關背景。)

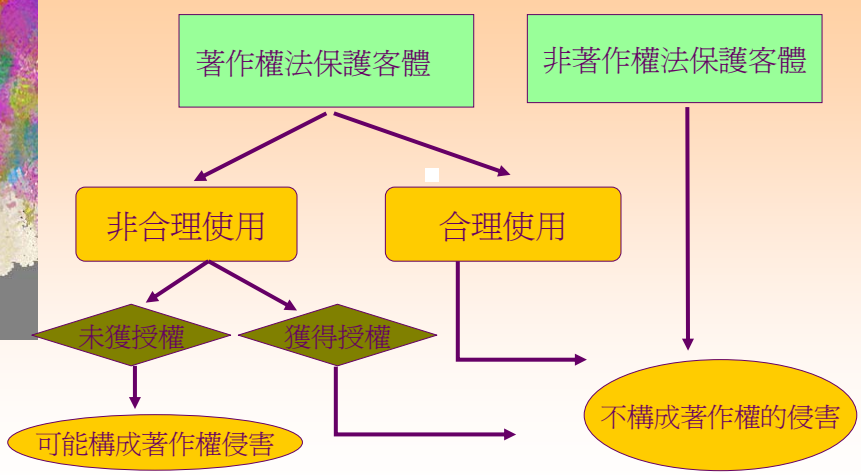
查獲贓證物: 犯罪用手機等數支。

偵辦單位: 刑事警察局偵九隊。

案例五:網路著作權問題之提出

- 我想要建立一個自己網站，從網路上抓取圖形與程式應用？
- 在網路上賣大補帖，貼補學費？
- 要交學校作業，從網路上找到幾篇不錯的文章
- 在個人網站上提供MP３音樂、共享軟體、註冊碼供人下載？
- 幫忙別人寫網頁打工賺錢，網頁的著作權是否歸自己所有？

面對著作權的思考模式



著作權法第九十一條

(立法院93.08.24三讀通過刑著作權法修正案)

重製盜版光碟之處罰(New）

- 第九十一條 擅自以重製之方法侵害他人之著作財產權者，處三年以下有期徒刑、拘役，或科或併科新臺幣七十五萬元以下罰金。
- 意圖銷售或出租而擅自以重製之方法侵害他人之著作財產權者，處六月以上五年以下有期徒刑，得併科新臺幣二十萬元以上二百萬元以下罰金。
- 以重製於光碟之方法犯前項之罪者，處六月以上五年以下有期徒刑，得併科新臺幣五十萬元以上五百萬元以下罰金。
- 著作僅供個人參考或合理使用者，不構成著作權侵害。

散布盜版光碟之處罰(New）

(立法院93.08.24三讀通過刑著作權法修正案)

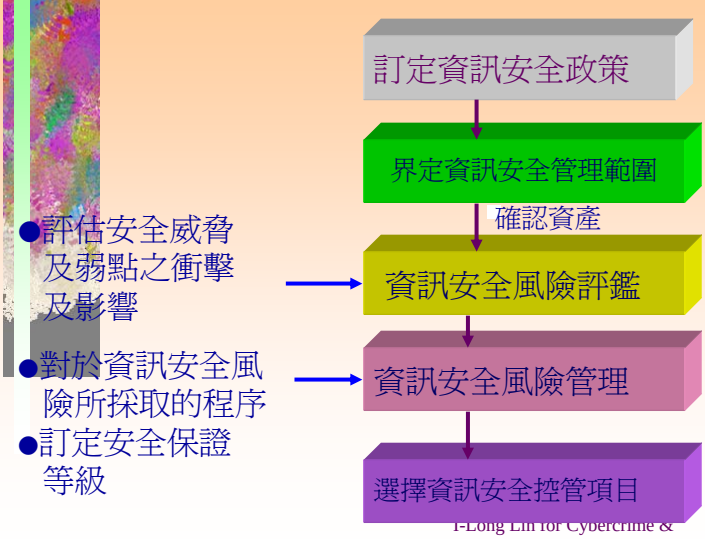
- 第九十一條之一 擅自以移轉所有權之方法散布著作原件或其重製物而侵害他人之著作財產權者，處三年以下有期徒刑、拘役，或科或併科新臺幣五十萬元以下罰金。
- 明知係侵害著作財產權之重製物而散布或意圖散布而公開陳列或持有者，處三年以下有期徒刑，得併科新臺幣七萬元以上七十五萬元以下罰金。
- 犯前項之罪，其重製物爲光碟者，處六月以上三年以下有期徒刑，得併科新臺幣二十萬元以上二百萬元以下罰金。犯前二項之罪，經供出其物品來源，因而破獲者，得減輕其刑。

📖(資訊)網路犯罪之防範對策 (如何落實資訊安全？)-PLSE

➓➔資訊安全管理推動工作必須以全方位觀念永續推動(3E策略)

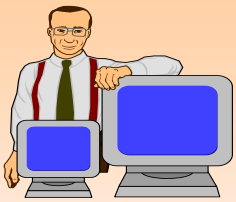
➓➔網路犯罪之防範對策可從政策面(P) 、法律面(L)、安全技術面(S)、甚至利用網路的普及性及方便性之教育面(E)上，透過道德倫理觀念（如**網路倫理**）的宣導，提昇網路使用者自我控制的能力（即**網路自律**）及避免犯罪，進而達到犯罪預防目標。

資訊安全管理制度(ISMS)規劃

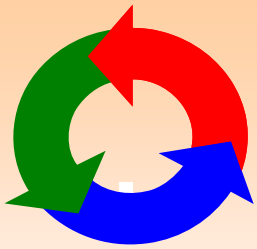


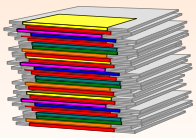
- 評估安全威脅及弱點之衝擊及影響
- 對於資訊安全風險所採取的程序
- 訂定安全保證等級

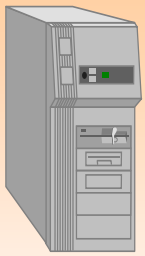
政府資訊安全管理規劃重點



人員安全(P)







實體安全(IT)

資訊、文件及軟體安全(C)

資訊安全風險評鑑 (RISK=A.V.T)

資產價值(A)

➔貨幣價值
➔隱藏價值
➔對手價值

安全弱點(V)

➔作業上的安全弱點
➔人員的安全弱點
➔有形的安全弱點
➔科技上的安全弱點

風險分析

安全威脅(T)

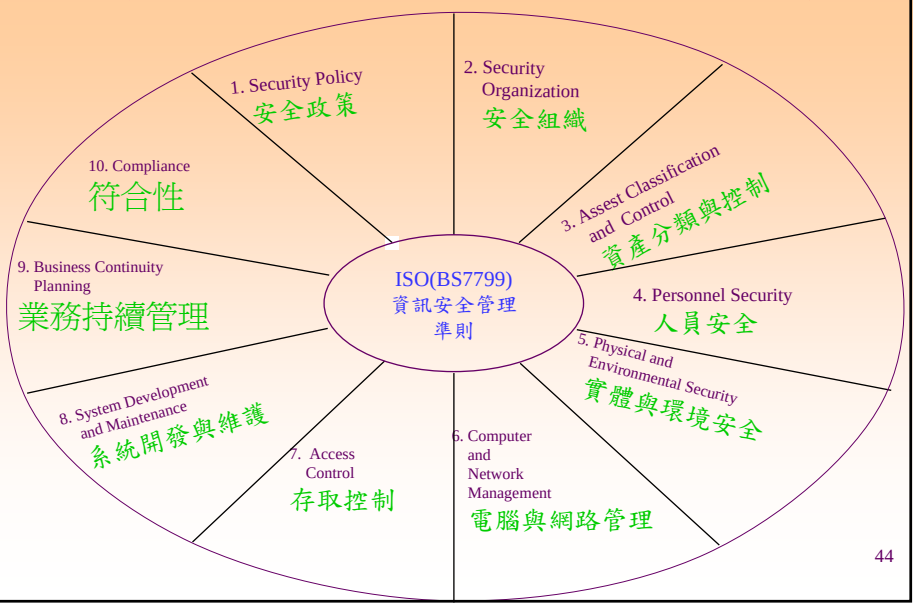
對策

➔政策規劃(P)
➔法規執行 (L)
➔技術工程(S)
➔教育訓練(E)

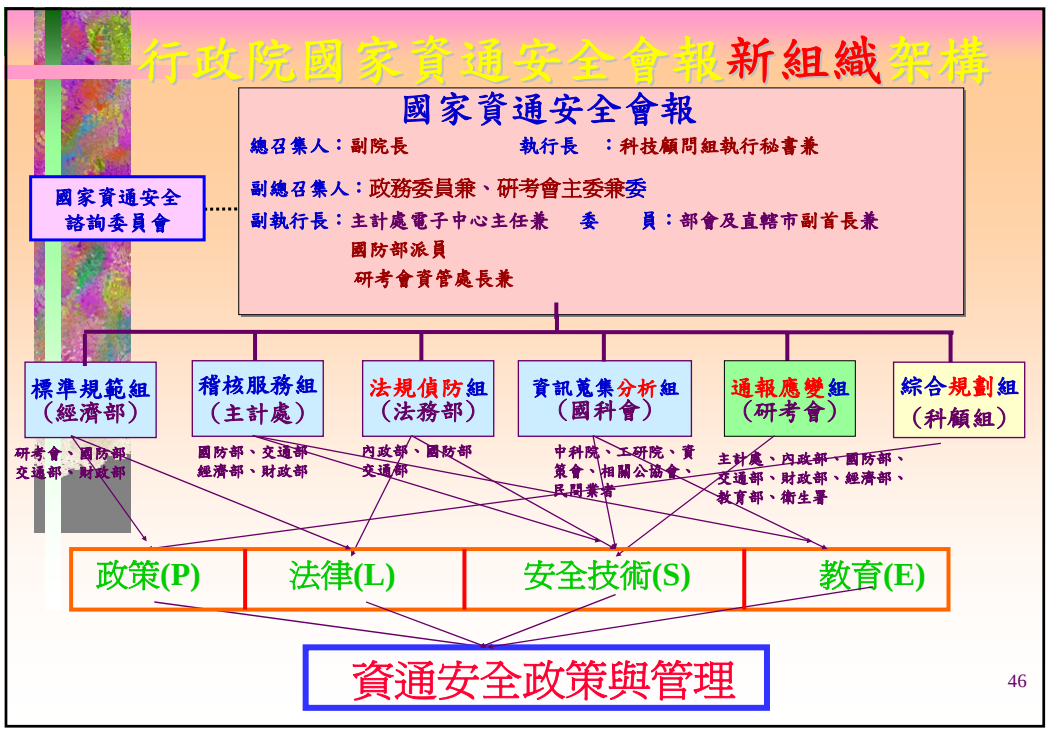
資訊犯罪之防範對策
一、政策面

- ➔法務部高檢署於86年9月成立「**電腦犯罪防治中心**」，其運作加快腳步，制訂出五大工作目標(86.09.26)，使其有效遏止電腦網路犯罪的蔓延及擴大。其五大工作目標如下：
  - 1.研擬防治電腦犯罪及網路犯罪的政策。
  - 2.溝通檢、警、調及各相關執行、研究機關的見解及作法。
  - 3.加強執法人員在職訓練。
  - 4.強化國內外電腦犯罪及網路犯罪的研究，建立網路犯罪研究資料庫。
  - 5.加強教育宣導，以建立適用電腦及網路社會的倫理及秩序，以減少網路犯罪的發生。
- ➔我國**通資訊基礎建設安全機制**(90年1月17日行政院院會通過)之犯罪偵防。
- ➔成立行政院國家資通安全會報((90年3月1日)之網路犯罪小組。
- ➔成立國家級「資通安全鑑識科技研究中心」

資訊安全管理安全模型(ISMS管理架構)
(ISMS-ISO17799:2000/BS7799-1/CNS17799)



標準	目的	內容
安全政策	爲資訊安全提供管理方向和支援。	建立安全政策文件
安全組織	建立組織內的管理體系以便安全管理。	組織內部資訊安全責任；資訊採集設施安全；可被第三方利用的資訊資產的安全；外部資訊安全評審；外包合約的安全。
資產分類與控制	維護組織資產的適當保護系統。	利用資產清單，分類處理，資訊標籤等對資訊資產進行保護。
人員安全	減少人爲造成的風險。	減少錯誤，偷竊，欺騙或資源誤用等人爲風險；保密協議；安全教育培訓；安全事故與教訓總結；懲罰措施。
實體與環境安全	防止對關於IT服務的未經許可的介入，損傷和干擾服務。	阻止對工作區與實體設備的非法進入；業務機密和資訊非法的存取、損壞、干擾；阻止資產的丟失，損壞或遭受危險；桌面與螢幕管理阻止資訊的洩漏。
電腦與網路管理	保證電腦與網路設備的正確和安全維護。	確保資訊處理設備的正確和安全的操作；降低系統失效的風險； 保護軟體和資訊的完整性；維護資訊處理和通訊的完整性和可用性；確保網路資訊的安全措施和支援基礎結構的保護； 防止資產被損壞和業務活動被干擾中斷；防止組織間的交易資訊遭受損壞，修改或誤用。
存取控制	控制對商業資訊的存取。	控制存取資訊；阻止非法存取資訊系統；確保網路服務得到保護；阻止非法存取電腦；檢測非法行爲； 保證在使用移動電腦和遠端網路設備時資訊的安全。
系統開發與維護	保證系統開發與維護的安全	確保資訊安全保護深入到作業系統中；阻止應用系統中的用戶資料的丟失，修改或誤用；確保資訊的機密性，可靠性和可用性；確保IT專案工程及其支援活動在安全的方式下進行；維護應用程式軟體和資料的安全。
業務持續管理	防止商業活動中斷和災難事故的影響。	防止商業活動的中斷；防止關鍵商業過程免受重大失誤或災難的影響。
符合性與稽核	避免任何違反法令、法規、合約約定及其他安全要求的行爲。	避免違背刑法、民法、條例，遵守契約責任以及各種安全要求；確保組織系統符合安全政策和標準；使系統審查過程的績效最大化，並將干擾因素降到最小。



資訊犯罪之防範對策
二、法律面：

- 因應日新月異的電腦及網路等新科技型態的犯罪型態，立法院院會通過「中華民國**刑法修正草案**」(86.10.08完成修正案三讀) (92.06.03完成修正案三讀通過第三十六章妨害電腦使用罪專章第358~363條)。
- ➔其次更應加速制訂**網路基本法**、**網路管理法和網路使用者管理辦法**等法律，並配合網際網路迅速發展及複雜網路犯罪問題，以利我國NII計畫推展及提昇國家競爭力。
- ➔英國通過電子郵件檢查管理法(2000/08)。
- ➔我國電子簽章法90.10.31三讀通過。
- ➔**教育部校園網路使用規範** (90年12月26日核定)
  - ➔成立「資通安全鑑識與犯罪研究中心」

(資訊)網路犯罪之防範對策
三、安全技術面

- ➔資訊安全技術所需探討的議題就不只是傳統的電腦安全而已，網路的安全技術反成爲最迫切需討論研究的重點。要使網際網路的發展能繼續維持榮景，並對人類生活有幫助，就必需研究網路安全技術(防火牆技術,密碼技術及PKI/CA認證制度)與資訊安全管理系統(如BS7799, ISO17799/CNS17799)， ，讓人類在使用網路時，除了方便外，還要有免於恐懼的自由。
- ➔藉由探討網路相關安全問題及其所可能遭遇的威脅，針對網際網路上之資料安全、軟體安全、操作安全、環境安全、管理安全及安全稽核等六大方面，研訂安全的預防策略或研發安全偵測及防範軟體，強化網路資訊系統的安全性，從而建立完整網路資訊安全系統，提供安全控管的能力。
- ➔如防禦機制最新發展、電子商務安全機制之建立、安全管理最新趨勢、備份備援最新發展 。

📖 (資訊)網路犯罪之防範對策
四、教育面

- ➔網路上的新新人類---駭客(Hacker)，往往只為了一時的好奇與試探，但卻不知自己的行為以為法所不容，在這種情形之下，政府機關必須負起全部的責任，及加強宣導網路之法律問題及電腦(網路)的安全問題，讓民眾有適法的空間及條件。透過家庭、學校教育，甚至設立加強社會控制的網站及遊戲，提昇自我控制的能力，以避免觸入法網。
- ➔ 另外法務部高檢署於86年9月成立「電腦犯罪防治中心」，其制訂出五大工作目標中，有關教育面工作者，即加強法制教育宣導，以建立適用電腦及網路社會的倫理及秩序，並有效遏止電腦網路犯罪的蔓延及擴大，以減少犯罪的發生。
- ➔教育部於90年11月成立「網路法律諮詢委員會」
  - (http://www.crime.org.tw),(www.edu.tw)(www.ec.org.tw)
- ➔教育部於92年03月成立「不當資訊防制小組」

資訊網路八大守則
(資安文化)

- 請勿使用網路傷人
- 經本人同意之後，才可以藉閱他人檔案
- 請勿使用網路製造假消息
- 請勿使用網路偷竊財務
- 自行拷貝或使用未付費的軟體是非法行為
- 獲得擁有者授權之後，我們才可以使用他人數位資料
- 在設計程式時，應先考慮其對社會影響力(安全性與穩定性)
- 使用網路時應表現對他人的尊重與體諒

『肯定自己上網的能力，
尊重他人上網的權利』

未來資通安全新知識與新科技 (Cyber security Manag.)

- Hacking and Attack/Defence Strategy
- Cybercrime and CyberForensics
- Digital Evidence and Cyberevidence
- Cybercriminology(如MOP理論)
- Cyberlaw
- ISMS(ISO17799:2000/BS7799/CNS17799/17800)
- Cyber Security Management and Governace

資通安全管理課程規劃 (ISMS三大方向) (林宜隆,1998~2005)

- 資訊科技(IT)與安全管理
  - IM(ITM+IRM),DC&N,IS,ISMS, OS&OSS,NS&NM,AI&ES,EIS,DSS, ,EC&KM,BISP,ASP,ICP,EIP,PIP,GIP,Wireless,Firewall,IDS, 駭客攻防技術與策略,密碼理論,IR事件通報與處理機制...
- 資訊犯罪理論與資訊(科技)法論
  - 網路犯罪學(Cybercriminology&cybersociety),資訊法論,資訊倫理,IP Law,IT Law,MP3,資訊社會學,數位證據(DESOP)...
- 犯罪偵查理論與資安鑑識
  - 偵查理論,電腦犯罪偵防,數位證據搜證與鑑識,資訊戰與電腦病毒,弱點評估技術與工具,Digital Evidence,Computer Audit, Anti-Virus, Anti-Spam, Cyber Forensic, PIS,...

資安專業人才

(林宜隆,2004~2005)

- 資安防護人才(Q/Y, UNIT,Contents)
- 資安攻擊人才
- 資安鑑識人才
- 資安偵查人才
- 資安教育人才
- 資安治理人才

、結論與建議

結論

- ➔任何一個網路安全系統中，最重要的還是「人」。無論花費多少百萬美元來配備電腦軟、硬體，要是沒有嚴格訓練工作人員，總能被突破防線進入系統。是以再精密的網路安全資訊系統與防護措施，最重要的還是**管理制度(ISMS,ISO17799/BS7799/CNS17799)的建立**加以緊密結合。
- ➔利用資訊及保護資訊同等重要；一分事前的預防重於十分的事後的補救；面對數位行政時代的來臨，各級人員對機關資訊機密維護負有重要責任
- ➔取得機關上下的支持，讓安全成爲行政文化的精髓之一；營造機關上下齊心維護安全的組織氣候是最好的安全對策
- ➔成立「國家資通安全鑑識與犯罪研究中心」
- ➔麻省理工學院教授Nicholas Negroponte，在所著「數位革命」中提出：吾人必須省思「原子世界」的法律，是否適合套用在「位元世界」。
- ➔ All law will be internet law(Cyberlaw) 。

、結論與建議

ISMS建議

@ 資訊安全認知人人有責、
資訊安全管理人人做到。

@不習慣 ⟶ 習慣 ⟶ 成自然

@防禦機制最新發展、建立電子商務安全機制、
安全管理最新趨勢、備份備援最新發展
((IT,C,P)—(FW,IDS,AV,AS,CF,VPN,PKI….)

@建立資通安全鑑識防護體系與機制(事前、事中、事後)

@建立資安防護體系、檢驗資安應變能力、健全資安發展環境

未來資通安全新知識與新科技
=cybersecurity+cybercrime+cyberlaw
(=資通安全+網路犯罪+資訊法律)

『肯定自己上網的能力，
尊重他人上網的權利』

謝謝指導

資通安全認知、人人有責
資通安全管理、人人做到

加強台北市師生資訊倫理及法律責任之知識素養，
以提高師生資通安全認知與實例分析瞭解。

paul@mail.cpu.edu.tw
http://www.crime.cpu.edu.tw