校園資安防護認知及法令宣導

報告人：陳維民 資深顧問

NII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
- 行政院推動資訊安全現況
- 教育體系資通安全管理要求
- 使用者作業安全管理
- 資訊安全法令宣導
- 結語

課程大綱

- 資訊安全之概念說明

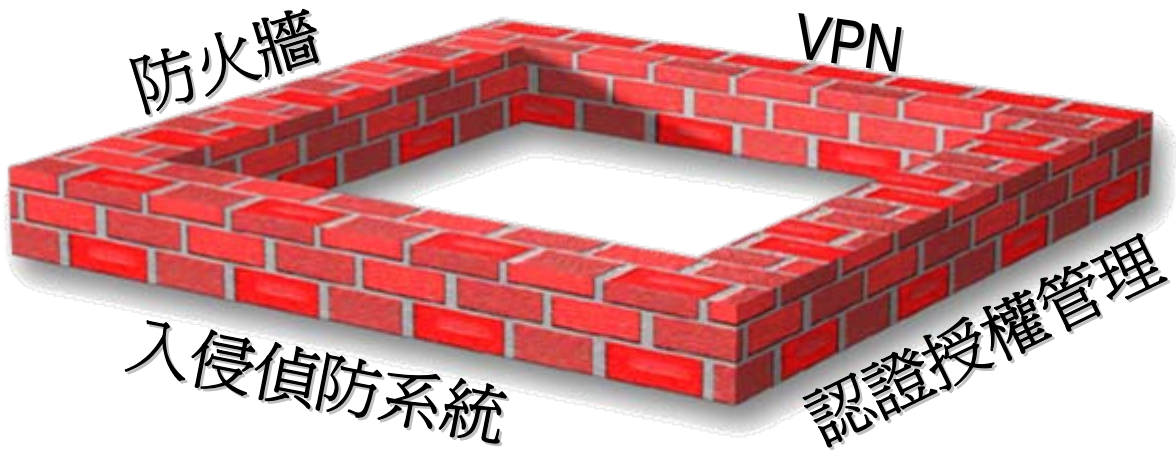
資訊安控的問題點

- 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

No Management, No Security

一般都會注意…

- 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

重要詞彙說明

- 何謂資產？
  - 對組織有價值的任何事物。
- 何謂資訊？
  - 資訊是一種資產，對於組織營運不可或缺。
  - 資訊存在形式有許多種，可以列印或書寫於紙本，可以電子形式儲存，或交談口述等，無論資訊形式為何，以何種方式分享或儲存，均應加以適當保護。

資產特色

- 不只侷限於電腦科技的產物
- 對組織有用的資訊都屬於資訊資產
- 無所不在

資料庫

資訊安全管理制度

- 資訊安全管理制度
  (Information Security Management System,ISMS)
  - 整體管理系統的一部份，以營運風險方案為基礎，用以建立、實施、操作、監督、審查、維持及改進資訊安全。

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

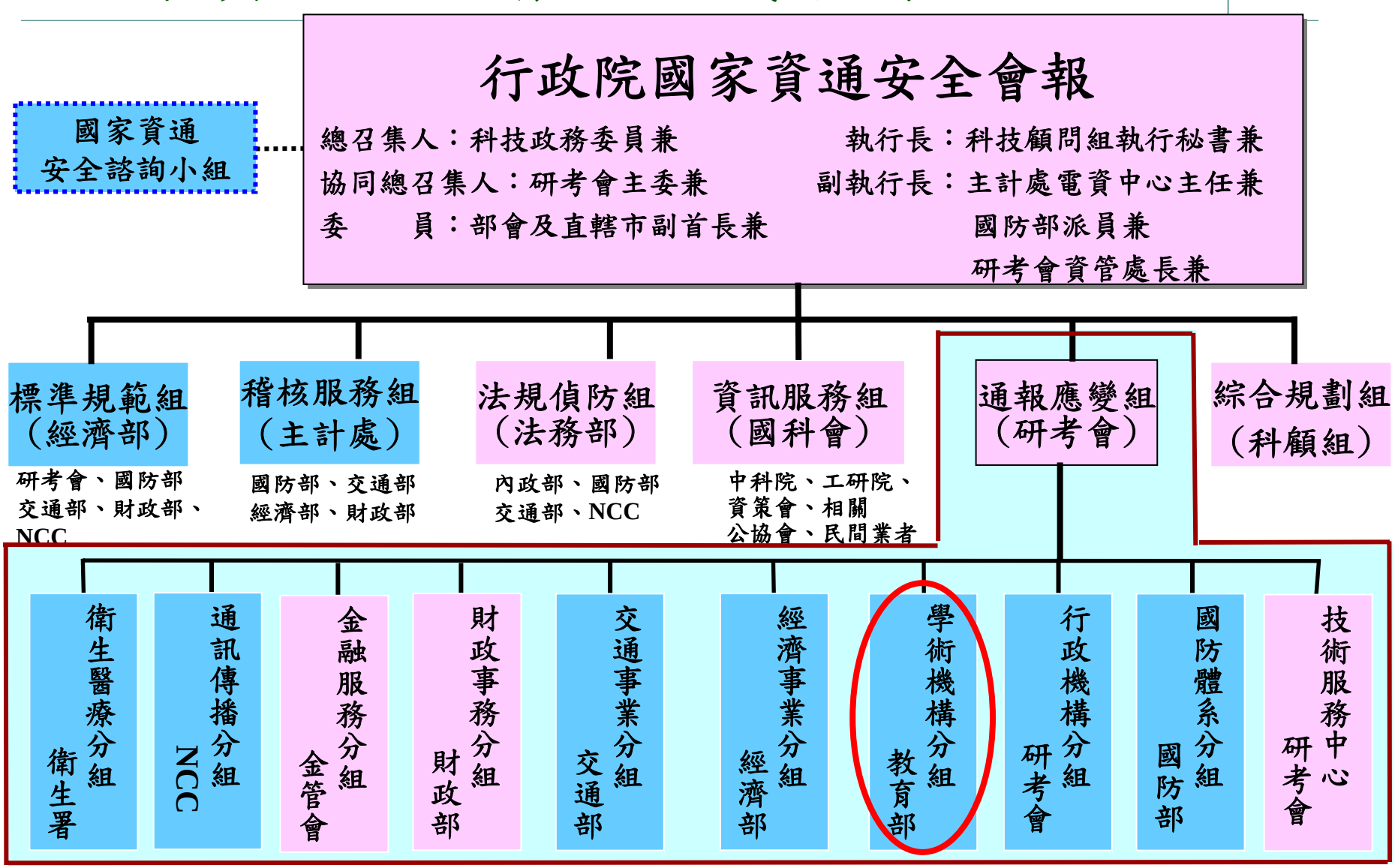
- 可用性(Availability)：
  確保經授權的使用者，在需要時可以取得資訊，並使用相關資產

ISMS目的在於保護資訊資產的機密性、可用性與完整性。

課程大綱

- 行政院推動資訊安全現況

國家資通安全會報組織架構



資通安全推動計劃

94年~97年
「建立我國通資訊基礎建設安全機制計畫」

NICST
國家資通安全會報

願　　景

確保我國擁有安全、可信賴的資訊通訊環境

94~97資通安全推動計劃 — 政策

1. 健全通報機制，加強應變能力
2. 強化資訊分享，建立互通管道
3. 提昇技術研發，增強防護能量
4. 確保資通安全，提升e化能量
5. 研訂資安法令，查緝網路犯罪
6. 保障人民隱私，加強宣導活動
7. 普及資安教育，加強人才培育
8. 加強區域聯防，建立國際合作

94~97資通安全推動計劃 — 目標

1.健全資通安全應變機制，以服務代替管制，達成二十四小時內通報機制效能

2.建置政府及重要基礎建設之資訊分享及分析中心，提升國家競爭力

3.建立二十四小時監控國家重要基礎建設資安系統，以降低資安威脅及減少被攻擊

4.建置安全無虞資通環境，確保民眾隱私權益，促進政府e化效能

5.推動資訊安全管理制度之認證達一百家以上，提升資安防護能量

6.配合國際資安法令及標準之發展趨勢，訂定我國資安相關法令及標準之制定率達70%以上

7.增強網路犯罪查緝能力，建立國家級資安鑑識實驗室

8.增強全民資安認知能力，培育專業資安人才，每年培育資安專業人才達400人以上

9.健全資通安全防護體系，有效遏止駭客入侵

10.積極參與全球資安活動，建立國際資安聯防機制

94~97資通安全推動計劃 — 範圍及策略

NICST 行政院國家資通安全會報
National Information & Communication Security Taskforce

策　略

1. 由政府機關落實，逐年向民間產業及企業推動
2. 由重點機關（構）推動，逐年全面性、全民性推動擴展
3. 政府機關及民間機構的密切合作，建立完備的資安整體防護體系

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	防禦機制強度	防護縱深	ISMS 推動作業	稽核方式	資安教育訓練(主官、主管、技術、一般)	專業證照
A 級(重要核心單位)	強度等級 4(註一)	NSOC 直接防護/自建 SOC、IDS、防火牆、防毒	96 年通過第三者認証(註二)	每年至少執行二次內稽	每年至少（4,6,18,4 小時）	96 年資安專業鑑定二張(註三)
B 級(核心單位)	強度等級 3	SOC(Optional)、IDS、防火牆防毒	97 年通過第三者認証	每年至少執行一次內稽	每年至少(4,6,16,4 小時)	96 年資安專業鑑定一張
C 級(重要單位)	強度等級 2	IDS,防火牆防　毒	各單位自行成立推動小組規劃作業	自我檢視	每年至少(2,6,12,4 小時)	資安專業訓練
D 級(一般單位)	強度等級 1	防火牆防　毒	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：大學、區域網路中心、縣(市)教育網路中心
- C 級：學院、專科學校・部屬館所
- D 級：高中職、國中小學

作業名稱 / 內容 / 等級	防禦機制強度	防護縱深	ISMS 推動作業	稽核方式	資安教育訓練(主官、主管、技術、一般)	專業證照
A 級(重要核心單位)	強度等級 4(註一)	NSOC 直接防護/自建 SOC、IDS、防火牆、防毒	96 年通過第三者認証(註二)	每年至少執行二次內稽	每年至少（4,6,18,4 小時）	96 年資安專業鑑定二張(註三)
B 級(核心單位)	強度等級 3	SOC (Optional)、IDS、防火牆防毒	97 年通過第三者認証	每年至少執行一次內稽	每年至少(4,6,16,4 小時)	96 年資安專業鑑定一張
C 級(重要單位)	強度等級 2	IDS,防火牆 防　毒	各單位自行成立推動小組規劃作業	自我檢視	每年至少(2,6,12,4 小時)	資安專業訓練
D 級(一般單位)	強度等級 1	防火牆 防　毒	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

資訊安全事件等級

- 依據91年06月06日行政院資通安全會報，第二次修訂之「建立我國通資訊基礎建設安全機制計畫」，資通安全事件等級概分為四級

  - **A 級**：影響公共安全、社會秩序、人民生命財產
  - **B 級**：系統停頓，業務無法運作
  - **C 級**：業務中斷，影響系統效率
  - **D 級**：業務短暫停頓，可立即修復

資安事件的類型

- 內部事件
  - 遭人為惡意破壞毀損、作業不慎等危安事件。
  - 設備故障
    - 能直接或間接影響機房安全資訊系統的各個設備的故障可視爲資通事件。
  - 人員差錯
    - 錯誤或不良的維護、錯誤設定和操作員的其他錯誤行為等。
  - 其他內部事件
    - 內部原因所引起的火災、爆炸等對機房安全可能產生重要之影響 。

資安事件的類型

- 外部事件
  - 因外部事件或自然事件所引起某一安全重要系統、元件或建築物故障的可能性，可經由設計和建造中所採取的因應措施，將其風險降低至可接受的程度
    - 病毒感染事件
    - 駭客攻擊（或非法入侵）事件
- 自然事件
  - 天然災害：颱風、水災、地震
  - 重大突發事件：火災、爆炸、核子事故

學術單位的資訊安全需求

- 為什麼學校單位需要資訊安全
  - 學籍資料遭竊
  - 考試成績遭竄改
  - 資料錯誤產生爭議（如選課系統發生錯誤）
  - 違反資料保護、智慧財產權等法規
  - 資訊服務中斷
  - 未授權之外部人員使用資源

- 學校單位所擁有的資訊特色
  - 以資訊之可用性為最優先考量
  - 具敏感性且涉及隱私與個人資料保護法相關規定

個案分享(一)

飆樂網 入侵百餘學校借殼

僅有小學學歷的黃○○，扮演「網路無殼蝸牛族」的駭客角色，涉嫌**侵入一百六十多所國中小及台中市教育局等部分機關的網站伺服器**，強佔空間供自己所架設的「飆樂網」等網站使用，昨天被調查局台南市調查站查獲，依刑法妨害電腦使用罪、違反著作權法等罪嫌移送法辦。

台南市調查站表示，經測試，黃俊明侵入這些學校的網站伺服器後，**可任意竊取學校的資料**，是否有資料被竊，因尚未接獲學校報案，還待調查。黃俊明坦承侵入學校網站，強佔校園網站的空間，但否認竊取學校的資料。他供稱，因對電腦網路有興趣，才入侵校園網站利用空間提供網友免費下載的服務。

個案分享(二)

學生個人資料 Google一覽無疑

學校網路外洩個人資料！日前國立大學學生使用Google搜尋自己姓名，竟查到來自學校網頁的個人資料。學生認為，校方若缺乏資料保護觀念，恐淪為詐騙集團幫兇。

某國立大學工業教育系畢業的鄭姓學生，一年來透過網路設定，讓搜尋引擎主動搜尋自己的名字的相關資料，發現自己的手機、住家地址等資料，竟可在網路上一覽無遺。

鄭姓學生表示，若詐騙集團利用學生資料犯罪，學校豈不成為幫兇？一、二年前他也曾在網路查到自己成績、繳納學費金額等資料。「這已經侵害個人隱私！」鄭姓學生認為，學費金額會曝露家庭背景，希望學校能儘速追查，並加強操作人員的教育。

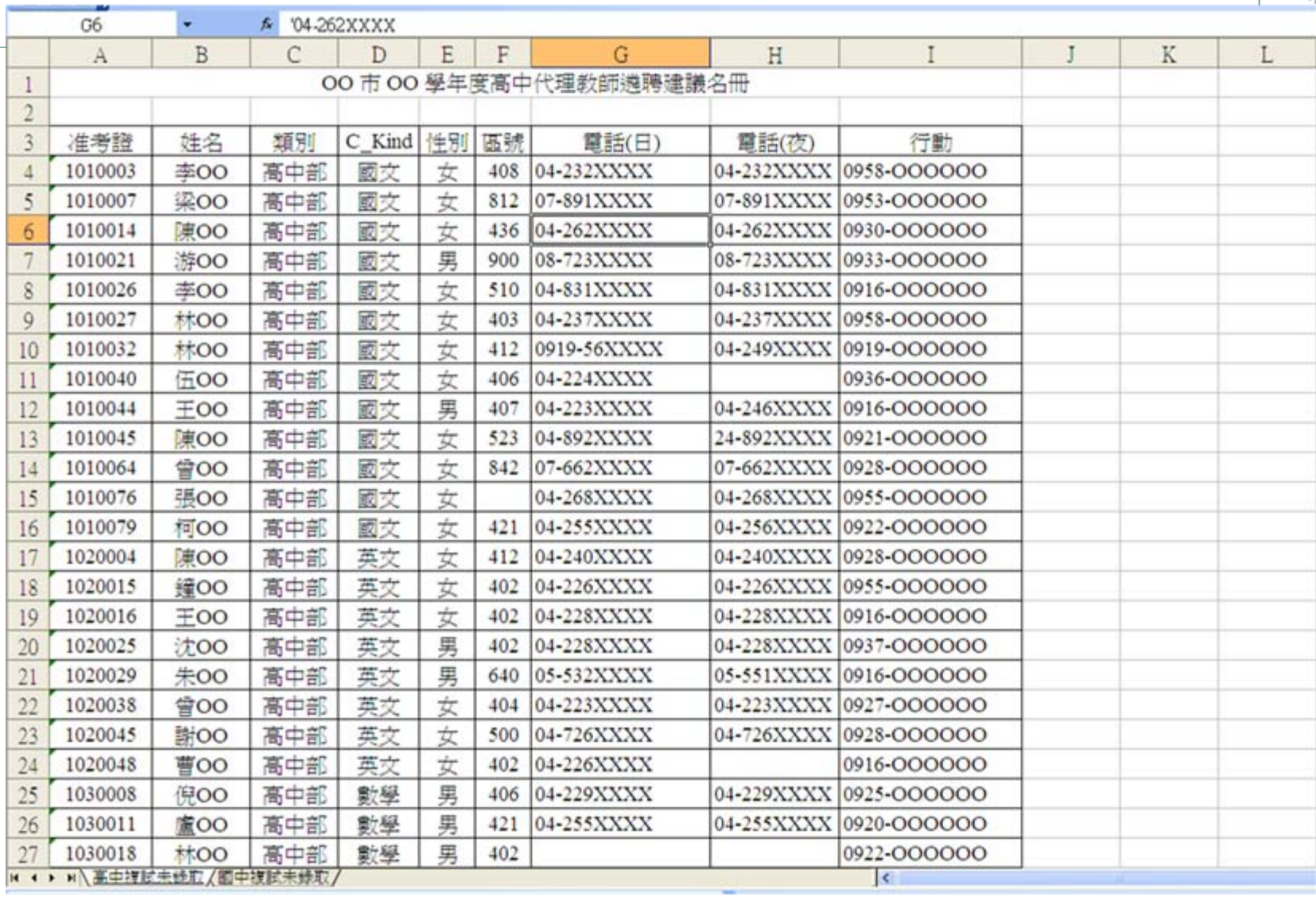
…

政治大學法律系教授馮震宇表示，網路外洩個人資料問題，主因為相關機構沒有採取安全措施。他表示，若學校因此造成學生權益受損，學生可依民法「人格權」的相關規定，向學校請求賠償。

人員疏失造成資安案例

在入口網站上使用某些關鍵字搜尋…

詳細個人資料網路公開



G6 '04-262XXXX

	A	B	C	D	E	F	G	H	I	J	K	L
1	OO市OO學年度高中代理教師遴聘建議名冊											
2												
3	准考證	姓名	類別	C_Kind	性別	區號	電話(日)	電話(夜)	行動			
4	1010003	李OO	高中部	國文	女	408	04-232XXXX	04-232XXXX	0958-OOOOOO			
5	1010007	梁OO	高中部	國文	女	812	07-891XXXX	07-891XXXX	0953-OOOOOO			
6	1010014	陳OO	高中部	國文	女	436	04-262XXXX	04-262XXXX	0930-OOOOOO			
7	1010021	游OO	高中部	國文	男	900	08-723XXXX	08-723XXXX	0933-OOOOOO			
8	1010026	李OO	高中部	國文	女	510	04-831XXXX	04-831XXXX	0916-OOOOOO			
9	1010027	林OO	高中部	國文	女	403	04-237XXXX	04-237XXXX	0958-OOOOOO			
10	1010032	林OO	高中部	國文	女	412	0919-56XXXX	04-249XXXX	0919-OOOOOO			
11	1010040	伍OO	高中部	國文	女	406	04-224XXXX		0936-OOOOOO			
12	1010044	王OO	高中部	國文	男	407	04-223XXXX	04-246XXXX	0916-OOOOOO			
13	1010045	陳OO	高中部	國文	女	523	04-892XXXX	24-892XXXX	0921-OOOOOO			
14	1010064	曾OO	高中部	國文	女	842	07-662XXXX	07-662XXXX	0928-OOOOOO			
15	1010076	張OO	高中部	國文	女		04-268XXXX	04-268XXXX	0955-OOOOOO			
16	1010079	柯OO	高中部	國文	女	421	04-255XXXX	04-256XXXX	0922-OOOOOO			
17	1020004	陳OO	高中部	英文	女	412	04-240XXXX	04-240XXXX	0928-OOOOOO			
18	1020015	鍾OO	高中部	英文	女	402	04-226XXXX	04-226XXXX	0955-OOOOOO			
19	1020016	王OO	高中部	英文	女	402	04-228XXXX	04-228XXXX	0916-OOOOOO			
20	1020025	沈OO	高中部	英文	男	402	04-228XXXX	04-228XXXX	0937-OOOOOO			
21	1020029	朱OO	高中部	英文	男	640	05-532XXXX	05-551XXXX	0916-OOOOOO			
22	1020038	曾OO	高中部	英文	女	404	04-223XXXX	04-223XXXX	0927-OOOOOO			
23	1020045	謝OO	高中部	英文	女	500	04-726XXXX	04-726XXXX	0928-OOOOOO			
24	1020048	曹OO	高中部	英文	女	402	04-226XXXX		0916-OOOOOO			
25	1030008	倪OO	高中部	數學	男	406	04-229XXXX	04-229XXXX	0925-OOOOOO			
26	1030011	盧OO	高中部	數學	男	421	04-255XXXX	04-255XXXX	0920-OOOOOO			
27	1030018	林OO	高中部	數學	男	402			0922-OOOOOO			

高中複試未錄取 / 國中複試未錄取 /

個案分享(三)

刪選課紀錄「駭」同學差點畢不了業

高雄1所科技大學電子工程系鄭姓學生，涉嫌在陳姓同學的個人電腦裡植入木馬程式，取得帳號及密碼後，進入學校網站刪除被害人的「電腦選課紀錄」，害同學差點畢不了業，他落網後供稱「只是單純惡作劇」，沒有其他不法意圖。

這所科技大學的電算中心人員指出，學校網站「沒有被駭」，被害人先前曾把自己的帳號及密碼告訴其他同學，鄭姓學生輾轉得知帳號、密碼後，以被害人的帳號、密碼登入學校網站刪除電腦選課紀綠，所以沒有其他人被害，至於被害人部分，學校也已及時補救。

警方將鄭姓學生依**妨害電腦使用罪及妨害秘密罪**嫌函送辦。

個案分享(四)

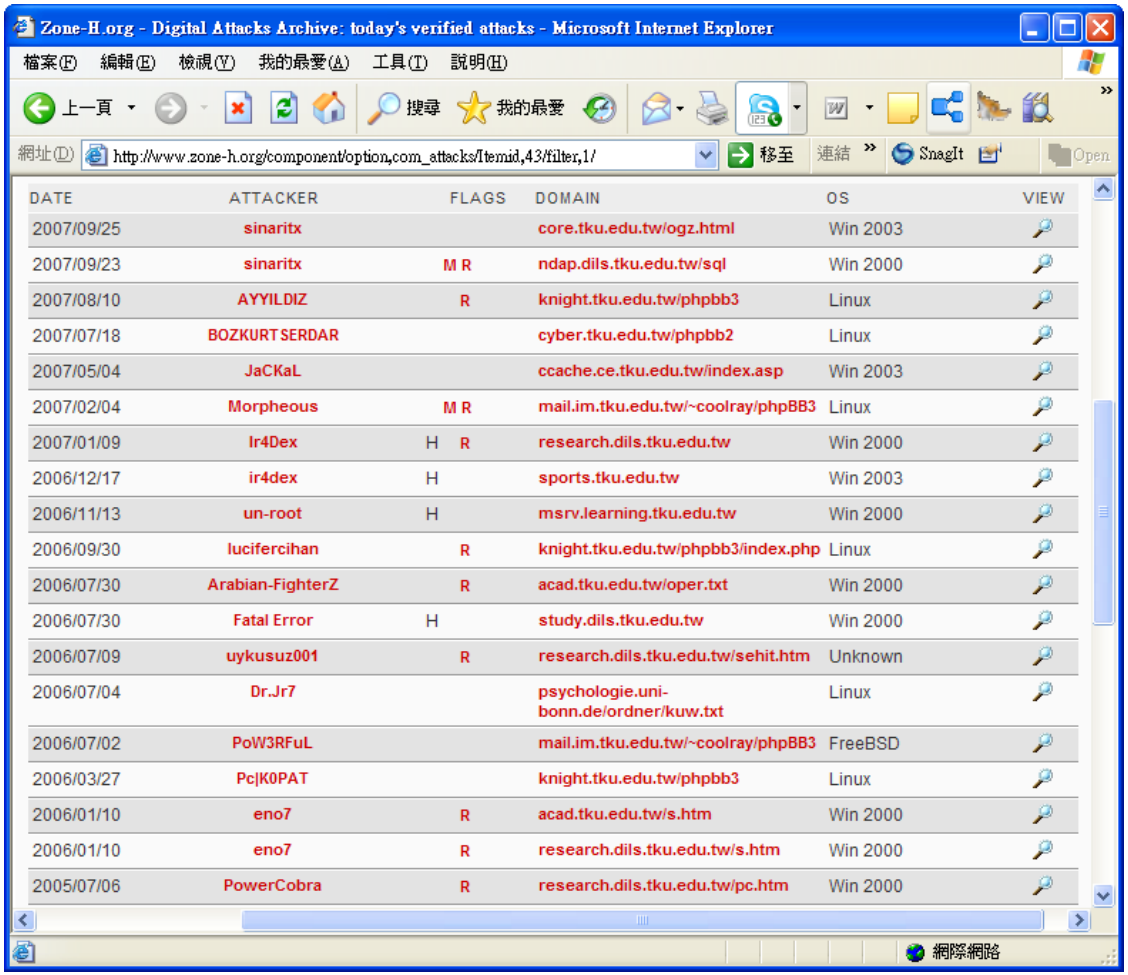
基測個資外洩案 逮19歲駭客

高雄檢方偵辦國中基測個資外洩案，意外發現剛高中畢業的楊姓學生，竟受雇扮「駭客高手」，用自學「駭功」，侵入至少八十所國中小學網站，竊取十多萬筆學生資料。目前他已申請上某大學資訊工程系。

楊姓學生供稱，靠自學「駭功」上國中小網站搜尋弱點，找出漏洞後，利用ASP（動態伺服器網頁）弱點測試取得權限密碼，再上傳木馬程式，伺機下載學生資料。因侵入的學校太多，他記不清，至少八十所。他侵入的學校，有些網站連防火牆都沒有，有的只要改變侵入路徑，就可進入拿資料。

警方將他依違反**電腦處理個人資料保護法**移送，檢察官以十萬元交保。

校園資安分析



DATE	ATTACKER	FLAGS	DOMAIN	OS	VIEW
2007/09/25	sinaritx		core.tku.edu.tw/ogz.html	Win 2003	
2007/09/23	sinaritx	M R	ndap.dils.tku.edu.tw/sql	Win 2000	
2007/08/10	AYYILDIZ	R	knight.tku.edu.tw/phpbb3	Linux	
2007/07/18	BOZKURTSERDAR		cyber.tku.edu.tw/phpbb2	Linux	
2007/05/04	JaCKaL		ccache.ce.tku.edu.tw/index.asp	Win 2003	
2007/02/04	Morpheous	M R	mail.im.tku.edu.tw/~coolray/phpBB3	Linux	
2007/01/09	Ir4Dex	H R	research.dils.tku.edu.tw	Win 2000	
2006/12/17	ir4dex	H	sports.tku.edu.tw	Win 2003	
2006/11/13	un-root	H	msrv.learning.tku.edu.tw	Win 2000	
2006/09/30	lucifercihan	R	knight.tku.edu.tw/phpbb3/index.php	Linux	
2006/07/30	Arabian-FighterZ	R	acad.tku.edu.tw/oper.txt	Win 2000	
2006/07/30	Fatal Error	H	study.dils.tku.edu.tw	Win 2000	
2006/07/09	uykusuz001	R	research.dils.tku.edu.tw/sehit.htm	Unknown	
2006/07/04	Dr.Jr7		psychologie.uni-bonn.de/ordner/kuw.txt	Linux	
2006/07/02	PoW3RFuL		mail.im.tku.edu.tw/~coolray/phpBB3	FreeBSD	
2006/03/27	Pc|K0PAT		knight.tku.edu.tw/phpbb3	Linux	
2006/01/10	eno7	R	acad.tku.edu.tw/s.htm	Win 2000	
2006/01/10	eno7	R	research.dils.tku.edu.tw/s.htm	Win 2000	
2005/07/06	PowerCobra	R	research.dils.tku.edu.tw/pc.htm	Win 2000	

- 2007年 *.tw 網站被『變臉』的案件數達1828件
  - .gov.tw佔了142件
  - .com.tw佔了846件
  - .edu.tw佔了420件
  - .org.tw佔了130件
  - .net.tw佔了19件

課程大綱

- 教育體系資通安全管理要求

教育體系資通安全管理要求

- 教育部於 96 年 6 月 11 日發函各機關學校公布以下兩份規範文件，作為教育機構資訊安全管理制度建置之參考
  - 「教育體系資通安全管理規範」
  - 「國中小學資通安全管理系統實施原則」

教育體系資通安全管理規範發展背景

- 為協助教育體系各級單位，以有限的成本與時間，達到資訊安全之目標，95年度由成功大學賴溪松教授、NII 團隊共同草擬，並邀請產官學研界專家共同檢視與修正。
  - 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訊安全管理規範。
  - 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。
  - 未來配合教育部規劃之「**教育體系資訊安全管理驗證機制**」，建構國內專屬之第三方驗證標準。

教育體系資通安全管理規範設計原則

- 施行單位規模
- 施行單位之業務內容
- 施行單位可運用之資源
- 施行單位之執行能力
- 施行單位於資訊安全控管上的需求
- 最低的成本達最高之安全控管效益
- 新增控制目標說明與控制項對應表以利了解

規範設計之準則

- 將ISO 27001:2005(E)中不適用各連線單位之項目與以刪除或合併(刪除項目請參閱刪除之規範與控制項)；並將語義不清或不適用之文字進行修改。

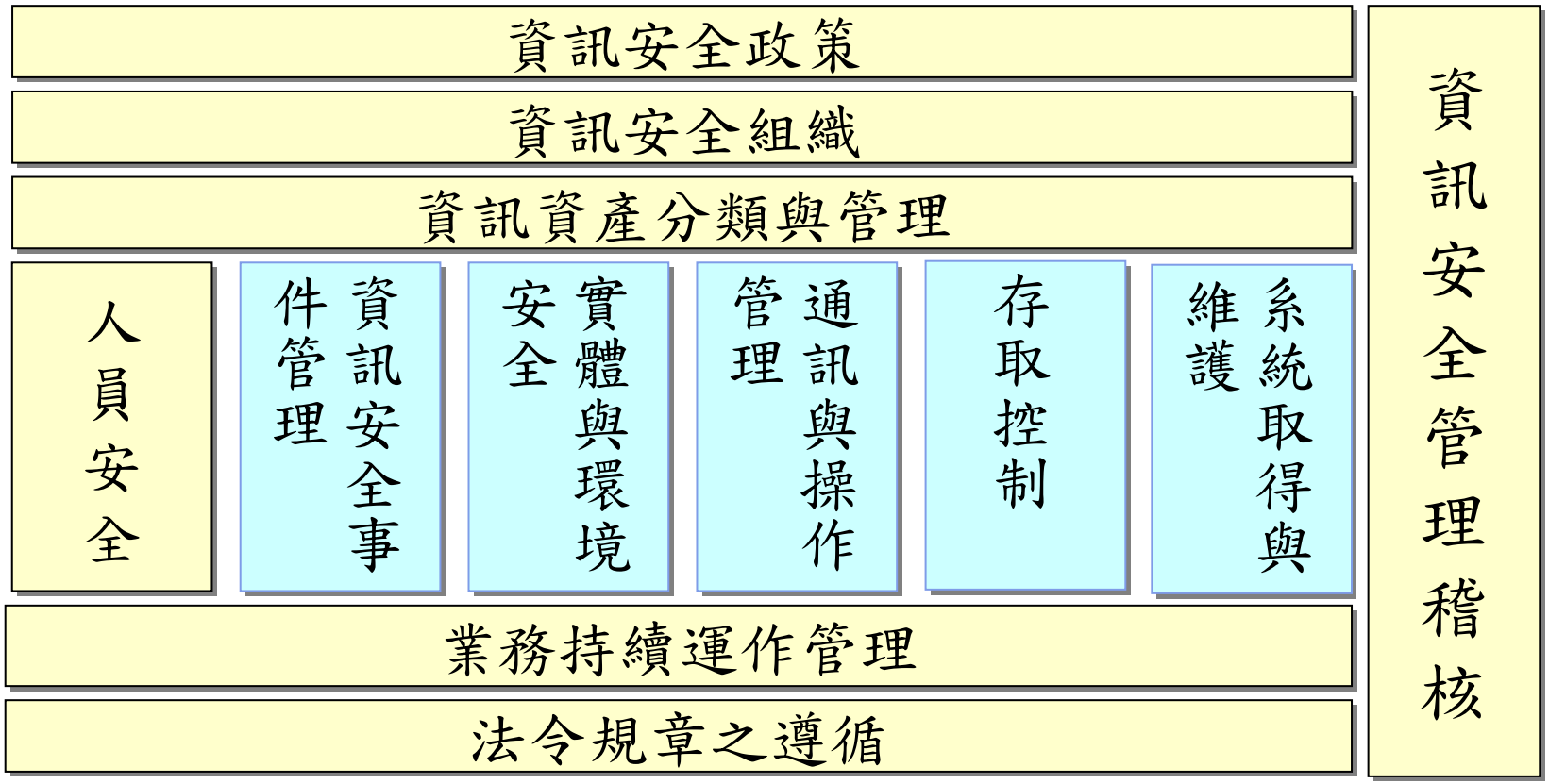
- 將行政院及所屬各機關資訊安全管理規範為稽核項目之範本，並刪除其中不適用之項目，並調整其中的內容。

適用範圍

- 本標準適用於教育部電算中心、部屬館所、縣市網中心、大專院校以及高中職資訊管理單位等資訊業務相關單位(或其他管理單位認為應加入ISMS規範範圍之部門)。
- 依單位層級區分二群
  - 第一群：教育部電算中心、部屬館所、縣市網中心、公私立大專院校(計網中心及校務行政)等。
  - 第二群：公私立高中職學校為主要。
- 依業務分為「學術網路系統」與「行政資訊系統」。

ISO27001涵蓋之內容

11 個領域、 39 個控制目標、 133 個控制要點



與 ISO 27001 標準的比較

規範名稱	章節數	控制目標	較適用於學術網路系統	較適用於行政資訊系統
ISO 27001:2005(E)	11	39		
教育體系管理規範	11	36	33(除A.10.5,A.12.1, A.12.2之外)	35(除A.10.6之外)

規範名稱	控制項		稽核項	
ISO 27001:2005(E)	133		至少424項 (行政院版本)	
教育體系管理規範	(1)100	(2)69	(1)約323	(2)約215

(1) 較適用於第一群項目(B、C級)
(2) 較適用於第二群項目(D級)

國內大學建置 ISMS 概況

- 已通過 ISO27001認證
  - 逢甲大學
  - 東海大學
  - 高雄第一科技大學
  - 靜宜大學
  - 淡江大學
  - 中興大學
  - 清雲科技大學
  - 大葉大學
  - 勤益科技大學
  - 暨南大學
  - 弘光科技大學
  - 嶺東科技大學
- 建置ISO 27001中
  - 台灣大學
  - 台北大學
  - 龍華科技大學
  - 高雄空中大學
  - 樹德科技大學
  - 屏東科技大學
  - 中國醫藥大學
  - 明治科技大學
  - 陽明大學
  - 台北護理學院
- 建置教育版ISMS
  - 中山醫學大學
  - 萬能科技大學
  - 彰化師範大學
  - 明道大學
  - 聯合大學
  - 崑山科技大學
  - 正修科技大學
  - 南台科技大學
  - 長榮大學
  - 立德大學
  - 致遠管理學院
  - 35區、縣網路中心

ISO27001驗證現況

2007/12/13　資料來源：
http://www.iso27001certificates.com/

Japan	2317*	Switzerland	12	Lithuania	2
UK	363	Turkey	12	Oman	2
India	347	Saudi Arabia	10	Peru	2
Taiwan	149	UAE	9	Portugal	2
Germany	87	Slovenia	8	Qatar	2
China	74	Sweden	8	Slovak Republic	2
Hungary	58	Iceland	7	Sri Lanka	2
USA	54	Kuwait	6	Vietnam	2
Australia	53	Pakistan	6	Armenia	1
Korea	51	Russian Federation	6	Bulgaria	1
Italy	45	France	5	Chile	1
Netherlands	32	Greece	5	Egypt	1
Hong Kong	30	Thailand	5	Gibraltar	1
Czech Republic	28	Bahrain	4	Lebanon	1
Singapore	28	Canada	4	Luxemburg	1
Malaysia	21	Indonesia	4	Macedonia	1
Brazil	20	Argentina	3	Moldova	1
Austria	17	Colombia	3	Morocco	1
Ireland	17	Isle of Man	3	New Zealand	1
Poland	16	Macau	3	Ukraine	1
Finland	14	Romania	3	Uruguay	1
Norway	14	South Africa	3	Yugoslavia	1
Mexico	12	Belgium	2		
Philippines	12	Croatia	2	**Relative Total**	**4047**
Spain	12	Denmark	2	**Absolute Total**	**4036***

ISO27001驗證現況

2008/11/16 資料來源：
http://www.iso27001certificates.com/

Japan	2863*	Netherlands	11	Bulgaria	2
India	433	Singapore	11	Canada	2
UK	368	Philippines	10	Gibraltar	2
Taiwan	202	Saudi Arabia	10	Isle of Man	2
China	174	Pakistan	10	Morocco	2
Germany	108	Russian Federation	10	Oman	2
USA	82	France	9	Qatar	2
Hungary	74	Colombia	7	Yemen	2
Korea	71	Slovenia	7	Armenia	1
Czech Republic	66	Sweden	7	Bangladesh	1
Italy	54	Slovakia	6	Belgium	1
Hong Kong	38	Croatia	5	Egypt	1
Poland	36	Greece	5	Iran	1
Australia	28	South Africa	5	Kazakhstan	1
Austria	26	Bahrain	4	Kyrgyzstan	1
Ireland	26	Indonesia	4	Lebanon	1
Malaysia	26	Kuwait	4	Lithuania	1
Spain	26	Norway	4	Luxembourg	1
Brazil	20	Sri Lanka	4	Macedonia	1
Mexico	20	Switzerland	4	Moldova	1
Thailand	17	Chile	3	New Zealand	1
Romania	16	Macau	3	Ukraine	1
Turkey	15	Peru	3	Uruguay	1
UAE	14	Portugal	3	Relative Total	4997
Iceland	11	Vietnam	3	**Absolute Total**	**4987**

國中小學資通安全管理制度實施原則

NII財團法人中華民國國家資訊基本建設產業發展協進會

發展背景

- 配合行政院針對各級機關資訊安全要求之政策，在教育部指導下，94年度由 NII 產業發展協進會、及產官學資安領域專家，共同針對國中、小學校的資訊環境需求與體質，規劃出學校單位較容易落實之資通安全作業。
- 設計理念
  - 以 CNS 17800的 10 個領域為基礎，挑選出國中小學校容易落實之項目。
  - 提供學校查檢表，便於學校檢核與評估落實狀況。
  - 規劃合適之資訊安全管理概念教育訓練課程教材，提升人員資訊安全觀念與認知。

適合國中小環境的資安控制項目

CNS 17800
資訊安全政策
安全組織
資產分類與控制
人員安全
實體與環境安全
通訊與作業管理
存取控制
系統開發與維護
營運維持管理
遵守法規要求

篩選與
重新分類

國中小學資安管理系統實施原則
1. 網路安全
2. 系統安全
3.人員安全管理
4.實體安全管理

實施原則之內涵－網路安全

- 網路控制措施
  - 學校與外界連線，應僅限於經由縣網中心之管控，以符合一致性與單一性之安全要求。
  - 學校內特殊系統（例如會計系統、學生學籍、成績原始資料系統等）之資料，當有必要透過網路進行傳輸時，建議透過虛擬私有網路（Virtual Private Network, VPN）或同等連線方式進行；若無透過網路進行傳輸需求，則建議區隔於網路之外。
  - 應禁止以電話線連結主機電腦或網路設備。
- 網路安全管理服務委外廠商合約之安全要求
  - 委外開發或維護廠商必須簽訂安全保密切結書（提供切結書範本）。

實施原則之內涵－系統安全

- 職責區隔
  - 學校主機電腦可依個別應用系統之需要，設置專屬電腦，例如網路服務主機（電子郵件、網站主機）、教學系統主機（例如隨選視訊主機）。
  - 學校的行政系統主機（例如財務、人事、公文系統等）電腦，建議由各個縣（市）教育網路中心或教育局等單位統籌管理。
- 對抗惡意軟體、隱密通道及特洛依木馬程式
  - 學校內的個人電腦應：
    - 裝置防毒軟體，將軟體設定為自動定期更新病毒碼；或由伺服器端進行病毒碼更新的管理
    - 定期（至少每個月）進行如「Windows Update」之程式更新作業，以防範作業系統之漏洞
  - 學校內個人電腦所使用的軟體應有授權。
  - 新系統啟用前，應經過掃毒與更新系統密碼程序，以防範可能隱藏的病毒或後門程式。

實施原則之內涵－系統安全（續）

- 資料備份
  - 學校(或委託)系統管理人員需針對學校重要系統（例如系統檔案、應用系統、資料庫等）定期進行備份工作，或採用自動備份機制；建議週期為每週進行一次。
- 操作員日誌
  - 學校(或委託)系統管理人員需針對敏感度高、或包含特殊資訊的電腦系統進行檢查、維護、更新等動作時，應針對這些活動填寫日誌予以紀錄，作為未來需要時之檢查。
  - 日誌內容可包含以下各項：
    - 系統例行檢查、維護、更新活動的起始時間
    - 系統錯誤內容和採取的改正措施。
    - 紀錄日誌項目人員姓名與簽名欄。

實施原則之內涵－系統安全（續）

- 資訊存取限制
  - 學校內所共用的個人電腦應以特定功能為目的，並設定特定安全管控機制（例如限制從網路非法下載檔案行為、限制自行安裝軟體行為、限制特定資料的存取等）。
- 使用者註冊
  - 學校應制定電腦系統使用的使用者註冊及註銷程序，透過該註冊及註銷程序來控制使用者資訊服務的存取，該作業應包括以下內容：
    - 使用唯一的使用者識別碼(ID)。
    - 檢查使用者是否經過系統管理單位之授權使用資訊系統或服務。
    - 保存一份包含所有識別碼註冊的記錄。
    - 使用者調職或離職後，應移除其識別碼的存取權限。
    - 定期（建議每學期）檢查並取消多餘的使用者識別碼和帳號。
- 定期（建議每學期）檢查新增之帳號，若有莫名帳號產生，應關閉帳號權限，並依通報程序請求處理。

實施原則之內涵－系統安全（續）

- 特權管理
  - 學校的電腦與網路系統資訊具有存取特權人員清單、及其所持有的權限說明，應予以文件化記錄備查。
- 通行碼之使用
  - 管制使用者第一次登入系統時，必須立即更改預設通行碼，預設通行碼應設定有效期限。
  - 資訊系統與服務應避免使用共同帳號及通行碼。
  - 由學校發佈通行碼（Password）制定與使用規則給使用者，內容應包含以下各項：
    - 使用者應該對其個人所持有通行碼盡保密責任
    - 要求使用者的通行碼設定避免使用易於猜測之數字或文字，如生日、名字、鍵盤上連續的字母與數字、及過多的重複字元等。或建議通行碼應該包含英文字大小寫、數字、特殊符號等四種設定中的三種。
  - 因特殊需要擁有多個帳號時，可考慮使用一組複雜但相同的通行碼。

實施原則之內涵－系統安全（續）

- 原始程式庫之存取控制
  - 學校與系統廠商間的合約應加註對原始程式庫安全之要求，並防範資料庫隱碼(SQL-injection)問題，針對存取資料庫程式碼之輸入欄位進行字元合理性檢查。
- 通報安全事件與處理
  - 資訊安全事件包括：任何來自網路的駭客攻擊、病毒感染、垃圾郵件、資料或網頁遭竄改、以及通訊中斷等。
  - 學校應建立資訊安全事件通報程序以及安全事件通報單；通報程序應包括學校內部通報，以及學校與所屬縣市教育網路中心的通報。
  - 當學校內部無法處理之資安事件，應通報其所屬縣市網路中心。
  - 所訂出資訊安全事件通報程序應公布於校園內使用電腦與網路之場所，提供使用者瞭解。

實施原則之內涵－實體安全

- 設備安置及保護
  - 學校重要的資訊設備（如主機機房）應置於設有空調空間。
  - 學校資訊設備主機機房、電腦教室區域，應設置滅火設備，並禁止擺放易燃物、或飲食。
  - 學校資訊設備主機機房、電腦教室區域內的電源線插頭應有接地的連結、或有避雷針等裝置，避免如雷擊事件所造成損害情況。
  - 學校資訊設備主機機房、電腦教室區域，應至少於入出口處加裝門鎖或其他同等裝置。
  - 電源供應。
  - 學校重要的資訊設備（如主機機房）應有適當的電力設施，例如設置UPS、電源保護措施，以免斷電或過負載而造成損失。
- 纜線安全
  - 學校資訊設備主機機房、電腦教室區域內應避免明佈線。

實施原則之內涵－實體安全（續）

- 設備與儲存媒體之安全報廢或再使用
  - 所有包括儲存媒體的設備項目，在報廢前，應先確保已將任何敏感資料和授權軟體刪除或覆寫。
- 設備維護
  - 應與設備廠商建立維護合約。
  - 廠商進入安全區域需簽訂安全保密切結書。
- 財產攜出
  - 未經授權不應將學校的資訊設備、資訊或軟體攜出所在地。
  - 當將設備移出，應檢視相關授權，並實施登記與歸還記錄。
  - 相關財產之攜出應依教育部或學校既有之相關規定處理。
- 桌面淨空與螢幕淨空政策
  - 結束工作時，所有學校教職員工應將其所經辦或使用具有機密或敏感特性的資料（如公文、學籍資料等）及資料的儲存媒體（如USB 隨身碟、磁碟片、光碟等），妥善存放。
  - 學校提供教職員工或學生使用的個人電腦應設定保護裝置，如個人鑰匙、個人密碼以及螢幕保護。

實施原則之內涵 –人員安全

- 將安全列入工作執掌中
  - 應將資訊安全納入教職員手冊說明中，以強化工作上之資訊安全意識。
- 資訊安全教育與訓練
  - 使學校(或委託)系統管理人員有足夠能力執行日常基礎之資安管理系統維護工作，並使其瞭解資安事件通報之程序。
  - 學校鼓勵或安排資訊組長/老師/系統管理人員、以及所有教職員參與資訊安全教育訓練或宣導活動，以提昇資訊安全認知。

實施原則之內涵－法令認知

- 智慧財產權
- 電腦處理個人資料保護法
- 電子簽章法

國中小學資安自我檢測表

- 以「國中小學資通安全管理系統實施原則」文件為依據所擬定，作為國中小學就其資通安全管理系統之實施現況，進行自我評量之用途。

NO	檢測項目	符合與否	補充說明
網路安全			
	本校對外的網際網路連線只透過縣網中心進行。	□是 □否	
	學校自行管理的資訊應用系統包括？	□ 會計系統 □人事系統 □ 學籍系統 □網站服務 □ 電子郵件 □教學系統 □ 視訊系統	
	所勾選之系統所儲存的資訊當有必要和縣(市)網路中心進行網路傳輸時，傳輸連線是否為透過專屬線路完成？如VPN或GSN等。	□是 □否	

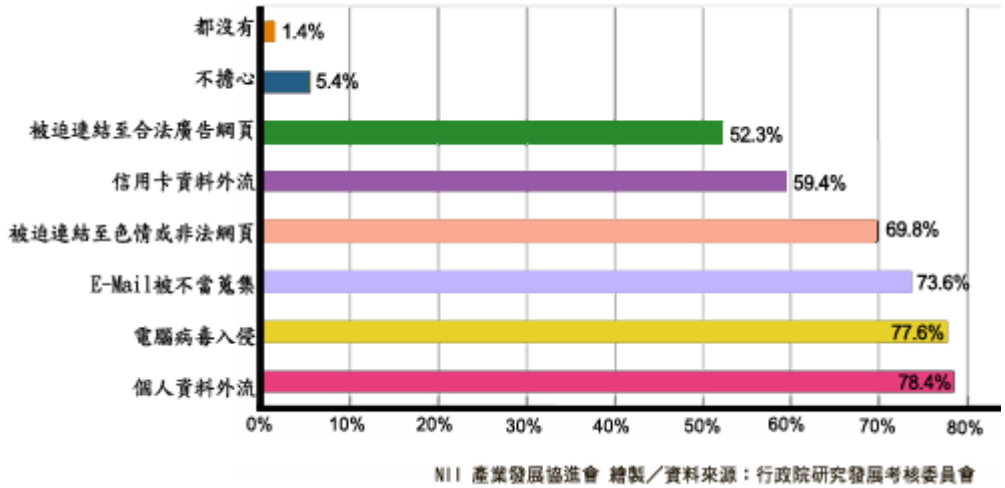
課程大綱

- 使用者作業安全管理

網路安全議題

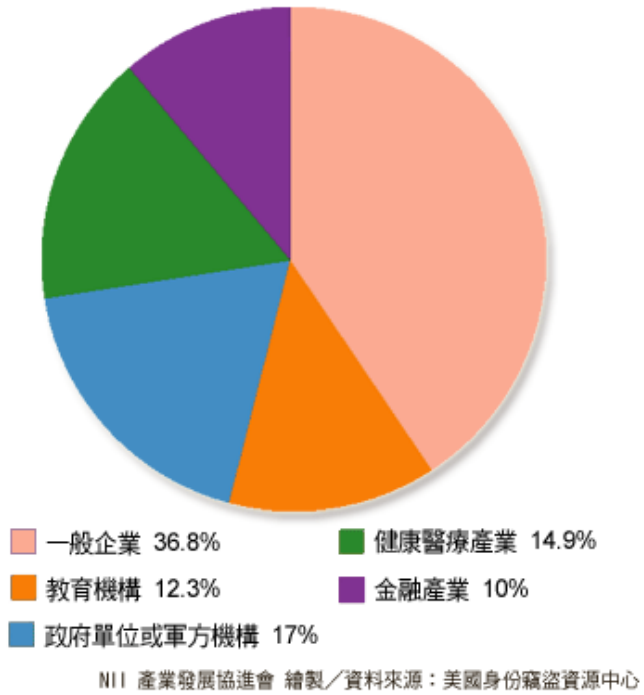
- 78.4% 網路使用者在上網時最擔心個人資料外流的問題

網路使用者在使用網路時的困擾與擔憂，在可複選的情形下，調查發現，網路使用者在上網時最擔心個人資料外流的問題，比率接近八成 (78.4%)，其次依序是擔心電腦病毒的入侵(77.6%)、E-Mail 被不當蒐集利用或常收到垃圾、廣告信件等(73.6%)、被迫連結至色情或非法網頁(69.8%)、信用卡資料外流(59.4%)及被迫連結至合法廣告網頁(52.3%)等，只有5.4%的網路使用者沒有上述這些網路使用困擾或擔憂，由此顯示，網路資訊安全已成為許多網路使用者相當擔憂且須嚴肅面對的問題。
資料來源：行政院研究發展考核委員會
公布日期：2008年1月7日



身分資料遺失

- 2008年1~8月美國身份資料遺失案件達449件



- 美國身份竊盜資源中心（Identity Theft Resource Center，ITRC）近日公布一項統計指出，截至8月22日為止，今年的資料外洩件數達到449件，已超越去年整年的446件
- ITRC所列出的身份資料外洩管道包含筆電或電腦等儲存裝置的遺失、備份磁帶的遺失、駭客入侵、內部員工偷竊或受到木馬、病毒程式的入侵等。在今年的資料外洩案件中，有36.8%是屬於一般企業、12.3%為教育機構、17%為政府單位或軍方機構、14.9%為健康醫療產業，以及10%為金融產業。

使用者責任

- 使用者的態度，在於有效防止非法(未經授權)的使用者存取，以保障安全的工作環境
- 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，應使用相關安全控制措施，以防止他人非法使用；抑或考慮汰除

桌面淨空與螢幕淨空政策

- 桌面淨空
  - 重要/機密文件(資料)不置於桌上
  - 重要/機密文件(資料)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

- 與網路服務的連線如果不安全，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(鍵盤測錄)

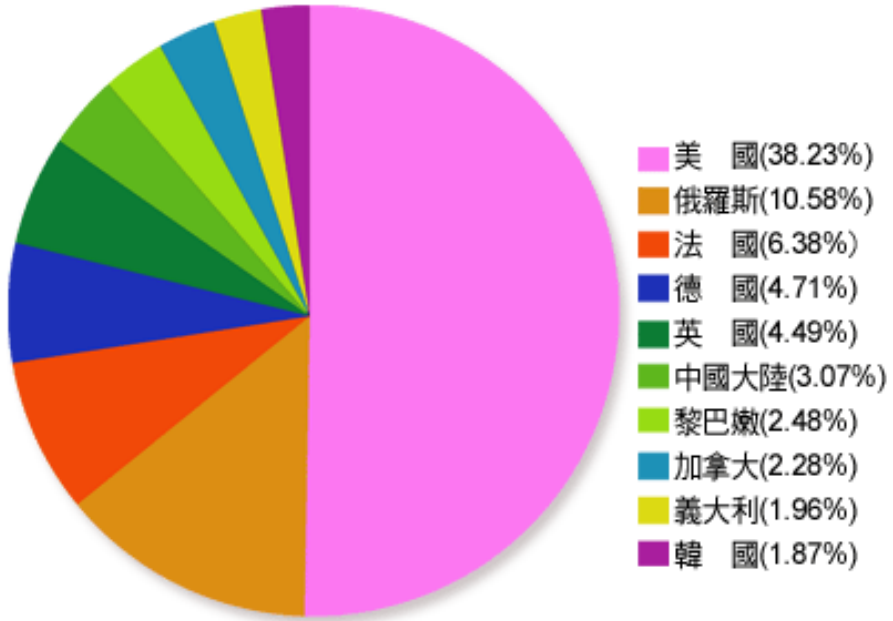
網路內容安全風險

- 惡性程式/廣告
  - 假冒輸入畫面
  - Pop-Up廣告
  - ADware(廣告軟體)
- 首頁綁架(Brower Hijacking)
- 間諜軟體(Spy Ware)
- 瀏覽器控制項(Browser Helper Object)

惡意程式網站

- 每十個網站就有一個是惡意網站

APWG: 全球藏有惡意程式網站的前三名國家
2008年3月：美國、俄羅斯、法國
資料來源：反網路釣魚工作小組(APWG)
公布日期： 2008年8月29日



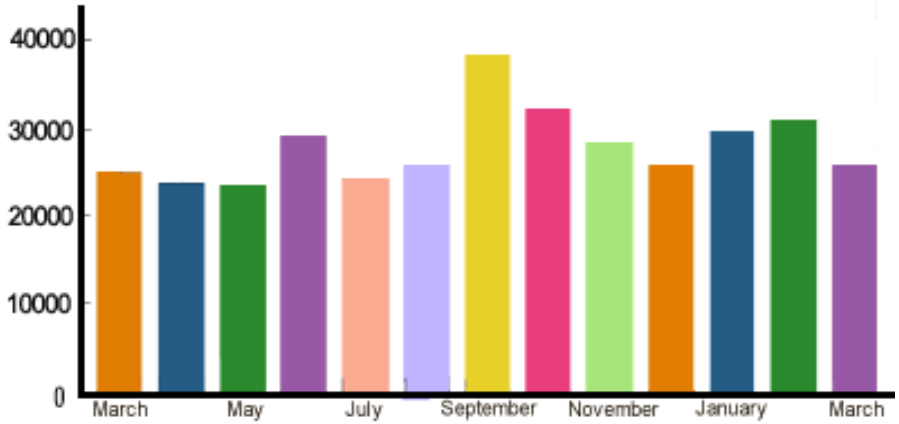
NII 產業發展協進會 繪製／資料來源：資料來源：APWG

網路釣魚攻擊

- 全球超過120個企業品牌被駭客用來透過電子郵件進行網路釣魚詐騙活動

2008年3月全球網路釣魚攻擊通報數量約 25,630 件
資料來源：反網路釣魚工作小組(APWG)
公布日期：2008年8月29日
反網路釣魚工作小組(Anti-Phishing Working Group)
2008年3月全球網路釣魚趨勢調查報告：

- 全球網路釣魚攻擊通報數量約 25,630 件
- 全球釣魚網站數量達到 24,908個
- 釣魚網站最多的國家： 美國
- 未使用 Domain Name, 而是使用 IP 的釣魚網站比例：4%
- 未使用 80 port 的釣魚網站所佔比例： 0.49%
- 釣魚網站在線最長的天數： 31 天 。



NII 產業發展協進會 繪製／資料來源：反網路釣魚工作小組(APWG)

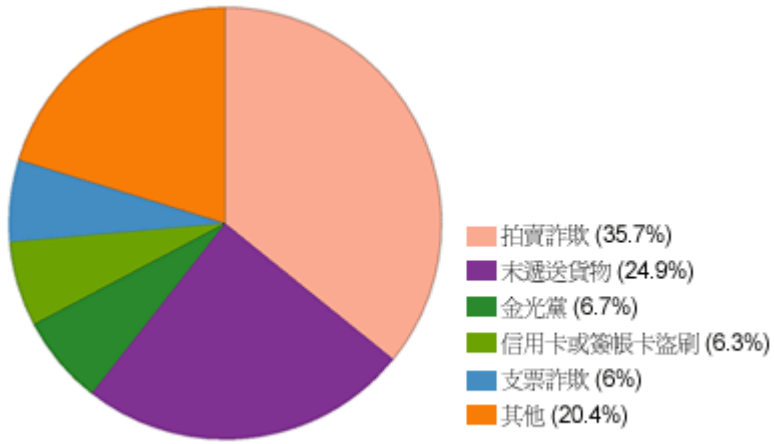
網路詐騙

- 2007年美國網路詐騙金額創2.39億美元新高

●2007年IC3總計接獲21.9萬個網路詐騙申訴案件，大多數調查的案件與拍賣或信用卡詐欺有關，這些詐欺案件所造成的損失總計為2.39億美元。

●IC3分析，詐欺佔去年申訴的最大比例，去年前五大網路犯罪申訴種類中，拍賣詐欺佔35.7%，未遞送貨物佔24.9%，金光黨佔6.7%，信用卡或簽帳卡盜刷佔6.3%、支票詐欺佔6.0%。去年因詐欺所損失的金額創下2.39億美元的新紀錄，比2006年的1.98億美元增加20%。

●至於歹徒與被害人接觸的管道主要為電子郵件，佔73.6%，其次是網頁的32.7%，以及電話的11.5%，即時傳訊亦佔了10.1%。



NII 產業發展協進會 繪製／資料來源：美國網路犯罪申訴中心

網路犯罪事件

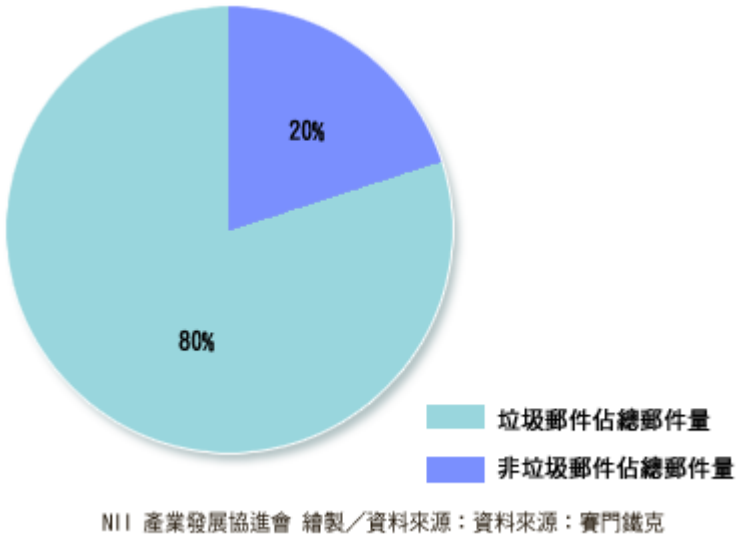
- 據警政署統計，2007年上半年電腦網路犯罪案件數高達一萬三六０八件
- 其中，攸關資料外洩的「網路詐欺」、「妨礙電腦使用」兩項案類，就分佔33%、27%
- 警政署預估，全台有三分之一電腦遭惡意程式入侵或被遠端駭客操縱而不自知

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

電子郵件風險

- 垃圾郵件量占整體電子郵件流量80%



NII 產業發展協進會 繪製／資料來源：資料來源：賽門鐵克

垃圾郵件發展出新的攻擊手法，隨著網路應用擴充到行動電話上，在日本出現垃圾郵件入侵手機竊取個資的案例，此外還有垃圾郵件中沒有出現連結，反而是要求收信者，利用信中指定的關鍵字去搜尋這些惡意網站。

資料來源：賽門鐵克垃圾郵件研究報告
公布日期：2008年07月22日

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。)
  - 要寄送重要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
    - 郵件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
  - 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

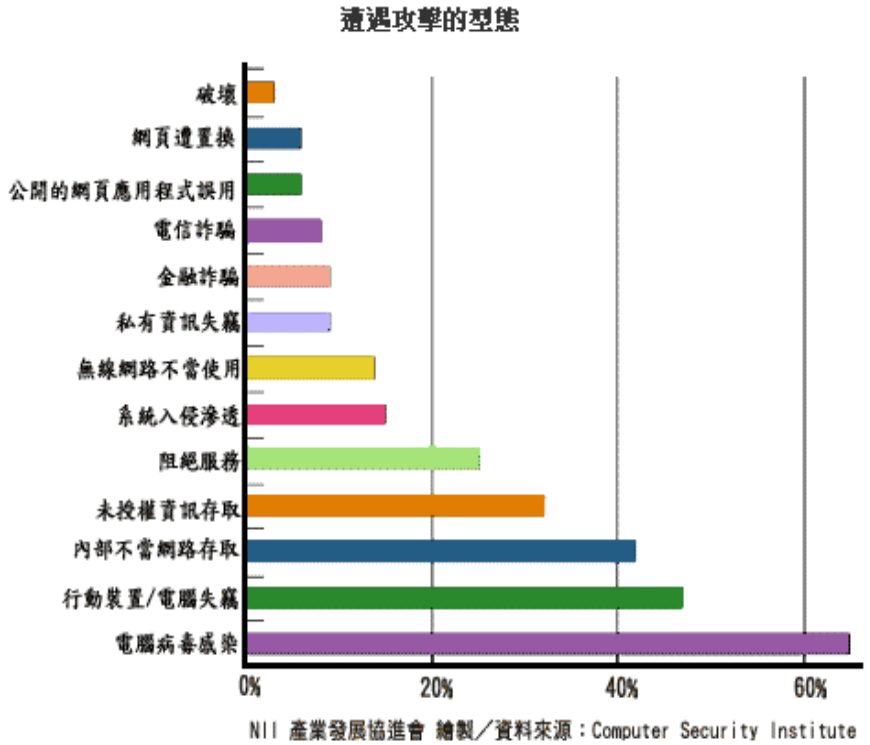
電腦作業威脅—電腦病毒

- 電腦病毒是最常見的攻擊形態

CSI/FBI 2006 Computer Crime and Security Survey：電腦病毒感染是最常見的攻擊形態

資料來源：Computer Security Institute
公布日期： 2006年

根據CSI/FBI 2006 Computer Crime and Security Survey，針對美國企業、政府、金融、醫療、學校等單位資訊安全從業人員調查「遭過攻擊的型態」，前三名分別是電腦病毒感染(65%)、行動裝置/電腦失竊(47%)、內部不當網路存取(42%)。



NII 產業發展協進會 繪製／資料來源：Computer Security Institute

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
  - 使用至少兩個反間諜軟體程式
- 刑事警察局木馬及鍵盤側錄惡意程式清除軟體「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

電腦作業威脅—駭客入侵

- 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

電腦作業威脅—駭客入侵

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

可攜式設備之安全管理要求(一)

- 使用可攜式設備（如筆記型電腦、掌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

可攜式設備之安全管理要求(二)

- 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

- 不論是紙本或電子檔的重要資料，皆應：
  - 定期備份
  - 存放在不同地方(異地備份)
- 資料備份原則
  - 資料價值較高時應優先備份
  - 選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）的管理辦法
  - 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

課程大綱

- 資訊安全法令宣導

資通安全相關法令

- 教育部所屬機關及各級公私立學校資通安全工作事項
- 私立學校及學術研究機構電腦處理個人資料管理辦法
- 台灣學術網路保護智慧財產權之相關措施
- 教育部校園網路使用規範
- 學術網路不法網站處理流程及智慧財產權疑似侵權處理程序
- 電腦處理個人資料保護法
- 執行電腦處理個人資料保護事項協調連繫辦法
- 著作權法
- 電子簽章法
- 電子簽章法施行細則
- 通訊保障及監察法
- 通訊保障及監察法施行細則
- 行政院及所屬各機關資訊安全管理要點
- 中華民國刑法（第三六章妨害電腦使用罪）
- 國家機密保護法
- 刑法防駭條款

案例(一)

- **案例描述** (資料來源:2007/10/10 天下雜誌)
- 多家知名電信公司、ISP廠商、學術網站等，**遭駭客入侵破解通行碼**，客戶個資遭盜竊合計近千萬筆，經查犯案者為苗栗某國立大學學生，該學生計畫以數百萬元代價販賣給犯罪組織。警政署呼籲電信、網路服務公司由於存放眾多客戶資料尤應加強資安防範，若本案未能即時查獲，其所造成之損害難以估計。

- 適用法條
  - 觸犯刑法第358條「**無故入侵電腦罪**」。
  - 觸犯刑法第359條「**無故取得、刪除或變更他人電磁紀錄罪**」。

案例(二)

- **案例描述** (資料來源:2007/11/16 中國時報)
- 電腦駭客蘇柏榕，涉嫌夥同林姓高二生，以**學術網站**為掩護，入侵各國中網站，竊取學籍資料，以每筆五元代價販售給補習班。他們將**跳板主機**隱藏在**台灣學術網路**內，利用木馬程式、網站漏洞，侵入網站取得資料，**存放在國外網站主機**，用以規避追查，於九月廿一日遭刑事局及桃園縣警局聯手查獲。

- 適用法條
  - 觸犯刑法第358條「**無故入侵電腦罪**」。
  - 觸犯刑法第359條「**無故取得、刪除或變更他人電磁紀錄罪**」。
  - 違反「**電腦處理個人資料保護法**」。

案例(三)

- **案例描述** (資料來源:2007/11/17 中國時報)
- 衛生署疾病管制局(ＣＤＣ)爆發電腦網路管控不當，致使1279名被限制搭機的結核病患者個人資料在網路曝光！民眾在知名網站「Google」(中文版)就可搜尋得到病人資料，從姓名、居住地，乃至身分證號碼、罹病狀況統統一目了然。ＣＤＣ十六日晚聲明認錯道歉，必要時將國家賠償。
- 全國25縣市、1279名經ＣＤＣ列管為「痰陽」之開放性結核病患（**不得搭乘航程八小時以上班機**），包含暫時不得搭機之多重抗藥性（ＭＤＲ）及超級抗藥性（ＸＤＲ）患者的姓名全名、設籍縣市及地區、照護院所代號、最近就醫日，甚至連英文字母在內十碼身分證字號...，竟然全都可以透過Google搜尋 。
- 適用法條
  - 依「**傳染病防治法**」受害當事人得提請國家賠償。
  - 違反「**電腦處理個人資料保護法**」

案例(四)

- **案例描述** (資料來源:2007/11/21 中國時報)
- 曾任職**銀行外包代辦現金卡公司**的男子翁文欽，離職後做起出售客戶個人資料的生意，詐欺及盜刷集團都向他買過資料。
- 警方調查，銀行外包代辦現金卡的常豐公司，前年十一月設立，去年四月停業，翁文欽藉此機會**留存客戶個資**，還上網利誘在賣場、加油站打工的工讀生側錄民眾信用卡卡號及背面檢核碼。翁文欽並將持有的民眾個資，以電子郵件**轉賣寄往詐欺或盜刷集團**。

- 適用法條
  - 觸犯刑法「**電腦詐欺罪**」、「**偽造文書罪**」以及「**電腦處理個人資料保護法**」等刑責。

刑法(第36章)

- 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**
  - **以網路作為犯罪場所–如色情、誹謗、賭博等**
- 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36章「妨害電腦使用罪」**

刑法(第36章)

- **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

刑法(第36章)

- 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

電腦處理個人資料保護法(一)

- 立法目的
  - 對公務與非公務機關蒐集、處理、與利用個人資料的情形，加以明文規範
  - 避免個人人格權（隱私權）遭受侵害，促進個人資料之合理利用，特此制定電腦處理個人資料保護法
- 保護客體
  - 本法保護客體限於經電腦處理的個人資料
  - 受本法保護之個人資料以現仍生存之自然人為限，已死亡之自然人與法人，不受本法之規範
  - 個人資料包含:自然人之姓名、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、社交活動、及其他足以識別該個人之資料

電腦處理個人資料保護法(二)

- 適用主體
  - 本法規範的對象有公務機關及非公務機關
  - 公務機關係指依法行使公權力之中央或地方機關
  - 非公務機關係指以下所列之事業、團體或個人
    - 徵信業、以蒐集或電腦處理個人資料為主要業務之團體或個人
    - 醫院、學校、電信業、金融業、證券業、保險業、大眾傳播業
    - 其他經法務部會同中央目的事業主管機關指定之事業、團體或個人
  - 受公務機關或非公務機關委託處理資料之團體或個人，於本法適用範圍內，其處理資料之人，視同委託機關之人

電腦處理個人資料保護法(三)

- 機關對個人資料之蒐集或利用的原則
  - 應尊重當事人之權益，依誠實及信用方法為之
  - 不得逾越特定目的之必要範圍，以確保當事人權益，避免人格權受到侵害
- 揭露個人資料，當事人是主要關鍵人物，當事人本身需審慎決定何者為提供給公務與非公務機關的必要個人資料

電腦處理個人資料保護法修訂草案

- 修法背景
  - 法務部為因應急速變遷之社會環境，特別彙整國內學界與實務界的相關修法建議，並參考其他國家之個人資料保護相關法令來針對本法進行修訂
- 修訂草案共有55條，預計將本法名稱修訂為「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
擴大保護客體	限經電腦處理之個人資料。	任何形式之個人資料。
普遍適用主體	公務機關、八大行業及指定適用之團體或個人。	1.任何自然人、法人、公務與非公務機關。 2.中華民國領域外，對中華民國人民蒐集、處理或利用個人資料者，亦適用。
增修行為規範(特種資料)	無規範。	醫療、基因、性生活、健康檢查及犯罪前科等五類資料，原則不得蒐集、處理或利用。
增修行為規範(通知義務)	僅規定公告機制無規定通知義務。	無論直接或間接蒐集個人資料均需告知當事人。

現行法與修正草案對照表(2/3)

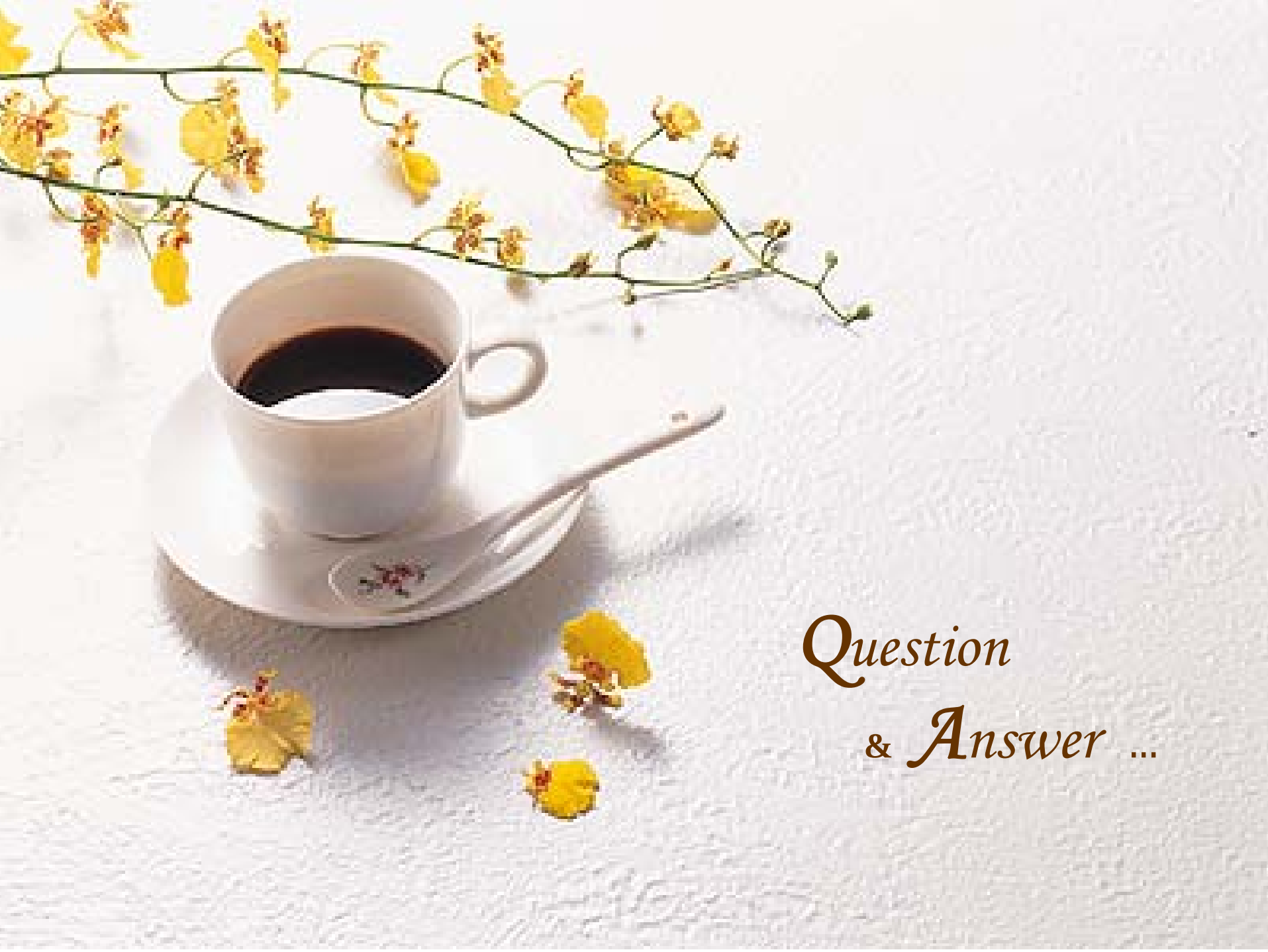
項　　目	現 行 法	修正草案
增修行為規範(書面同意)	無規範。	特定目的外利用個資需當事人書面同意方式。
增修行為規範(拒絕接受行銷權利)	無特別規定。	首次行銷應免費提供當事人表示拒絕之方式。
強化行政監督	無規範。	中央目的事業主管機關或直轄市、縣(市)政府，發現違反本法規定時，得派員進入檢查，並採取必要處分。
妥適調整罰則(刑罰規定)	僅處罰意圖營利侵害個資隱私權益者，刑期最高2年以下。	違反規定雖未意圖營利，刑期最高2年以下。 意圖營利者加重其刑最高5年以下。

現行法與修正草案對照表(3/3)

項　　目	現 行 法	修正草案
妥適調整罰則(民事損害賠償)	1.每人每一事件2萬元以上，10萬元以下。 2.同一原因事實最高2000萬元。	1.每人每一事件5000元以上，10萬元以下。 2.同一原因事實最高5000萬元。(待協商)
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。

結語

- 資訊安全的落實須高階主管的大力支持。
- 組織內的每一位成員都可能成為資訊安全漏洞。
- 資訊安全不只是軟/硬體設備或技術能力，還須輔以管理制度及持續運作與改進。
- 資訊安全不是資訊人員的責任，而是組織內全體人員的責任。
- 資訊安全須融入日常生活方能久遠維護。
  觀念認知 → 責任感建立 → 習慣養成


Question
& Answer ...