淡江大學

個人資料保護法帶來之衝擊與資訊管理因應作為

報告人：法務部資訊處長 陳泉錫

日　期：100年11月9日

簡報大綱

壹、近期的個資事件
貳、個人資料保護法修正重點
參、個人資料保護法細則草案重點
肆、行政與資訊部門之因應探討
- 人員安全管理及教育訓練
- 制度/法規
- 稽核

伍、結語

這是不是個資?

〔學　歷〕

- 國立臺灣大學政治研究所碩士
- 國立政治大學法律研究所碩士
- 法務部司法官訓練所司法官班第二十一期結業

〔經　歷〕

- 臺灣高雄地方法院檢察署候補檢察官、檢察官
- 臺灣臺北地方法院檢察署檢察官
- 臺灣高等法院花蓮分院檢察署檢察官
- 臺灣高等法院檢察署檢察官
- 法務部檢察司副司長
- 法務部檢察司司長
- 臺灣高等法院檢察署主任檢察官

甚麼是個人資料

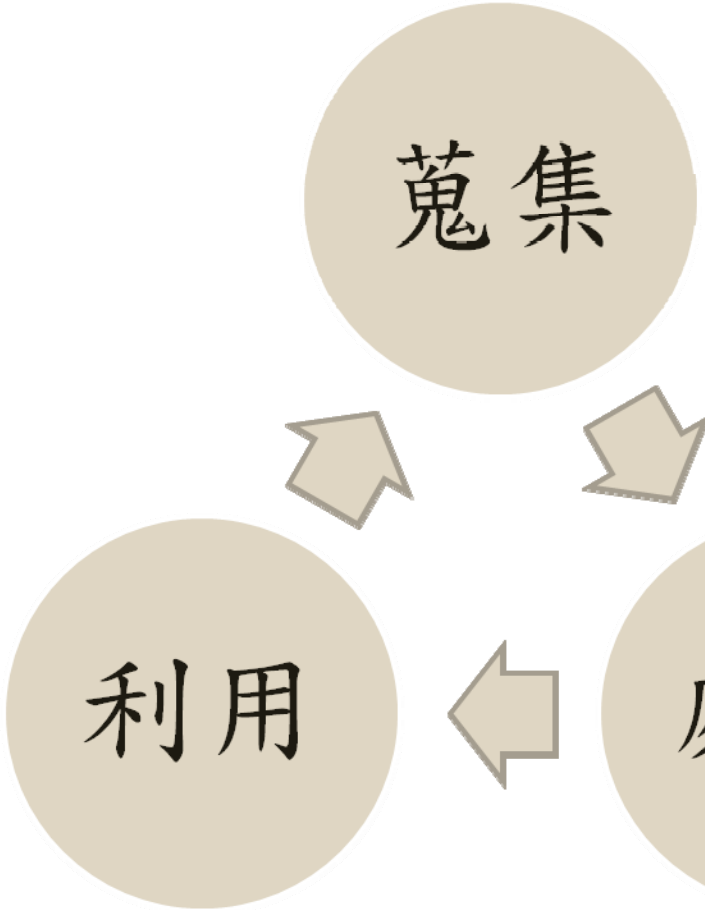
- 有形的型體—外貌長相
- 無形的內容：精神、心靈、個性、嗜好
- 個人資料：

  有形+無形=得以直接或間接方式識別該個人之資料。

  - 姓名、出生年月日、國民身分證統一編號、護照號碼、特徵(ex:性別)、指紋、婚姻、家庭(ex:家庭成員)、教育(ex:學歷)、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式(ex:電話、 e-mail)、財務情況(動產、不動產、 金融、保險、稅務資料)、社會活動(ex:組織會員)、其他(ex:經歷、宗教)。


站 - Windows Internet Explorer
/law.moj.gov.tw/LawClass/LawSearchNo.aspx?PC=I0050021&DF=&SNo=6
http--www.moj.gov.tw-...
建議的網站
升級您的瀏覽器
網站
全國法規資料庫
Laws & Regulations Database of The Republic of China
網站地圖
加入最愛
一般民眾
法規類別
法規檢索
司法判解
條約協定
兩岸協議
綜合查詢
跨機關檢索
置：首頁 > 法規 > 條號查詢結果
號查詢結果
稱
個人資料保護法
英
正日期
民國 99 年 05 月 26 日
效狀態
※本法規部分或全部條文尚未生效
連結舊法規內容
本法 99.05.26 修正公布之全文施行日期，由行政院定之。但現行條文第19～22、43 條之刪除，自公布日施行。
第 6 條
有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：
一、法律明文規定。
二、公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施。
三、當事人自行公開或其他已合法公開之個人資料。

個人資料保護三重點



以任何方式取得個人資料。

為建立或利用各人資料檔案所為資料之記錄、輸入、儲存、 編輯、更正、複製、檢索、刪除、輸出、連結、內部傳送。

將蒐集之個人資料為處理以外之使用。

幾個個人資料洩漏案事件

2009年06月11日新聞

http://tw.nextmedia.com/applenews/article/art_id/31700290/IssueID/20090611

網路販賣xx購物 8千筆個資

- 案情摘要
  - ■「阿哲」 賣東森購物 信用卡資料
  - ■2009年五月前每天均有絕無欺騙，預購來信表示購買日期及筆數。
  - ■8000筆資料試用(2008年八月十二日及十一月七日)

(source:葉奇鑫律師)

歹徒的網路留言

■ 15348@09:*阿哲* on 14:51:56 6/08/09IP=210.107.84.7 *輸錢賣*信用卡資料東森購物流出試用網址 http://www.megaupload.com/?d=OY3LKTU5 一筆0.5 瀏覽器編碼要改unicode才看的到 *ts8899@yeah.net來信詳談* **...**

(source:葉奇鑫律師)

事件二

麥當勞委外廠商遭入侵 客戶資料外洩,Information Security 資安人科技網 - Windows Internet Explorer

C:\Users\cchen7\Desktop\資安與委外\麥當勞委外廠商遭入侵 客戶資料外洩,Information Security 資安人科技網.mht

資安人 INFO SECURITY 領航資安・駕馭風險

資安MVP 等你來挑戰 即日起至2011年2月28日 觀看活動詳情

回首頁 | 資安直擊 | 話題大家談 | 最新活動 | 資安二手市集 | 資安知識庫 | 焦點話題 | 產業脈動 | 產品推薦 | 聯絡我們 | 資安人雜誌 | 資安人粉絲網 | 資安工作職缺

首頁 > 熱門新聞

麥當勞委外廠商遭入侵 客戶資料外洩

作者：張雒君 -12/13/2010

根據外電報導，連鎖速食業者麥當勞也傳出客戶資料外洩。上週，美國麥當勞總部透過電子郵件及其官方網站發布訊息，指出其行銷服務合作夥伴Arc Worldwide所委託管理麥當勞客戶資料的電子郵件公司，系統遭到入侵，包括姓名、電話號碼、電子郵件、地址等客戶資料很可能被未經授權的第三方存取。

一直以來，麥當勞委託行銷公司Arc Worldwide一一知名廣告公司李奧貝納（Leo Burnett）旗下互動行銷子公司進行宣傳、行銷活動，包括電子郵件促銷訊息的開發設計，而Arc則再委由另一家電子郵件發送

麥當勞於2010.12洩漏個資220萬筆

條規定：『受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。』因此，業者必須特別注意委外廠商對於客戶資料的處理過程及系統是否安全。由於委外廠商對於個人資料管理所應付的責任視同委託機關，因此業者必須特別留意在相關業務委外的合約上是否註明清楚的權利、義務。

本週新聞點閱排行

- 個資保護從政府資訊應用做起-2 全國地政資料庫在便民與隱私間平衡
- Sentinel AV 防病毒引擎推出! - Network Box
- 根據Network Box資料顯示印度和俄羅斯於八月份成為最主要的病毒來源
- 又是委外廠商惹的禍！美國Honda外洩490萬車主資料
- 輕忽系統異常現象 個資外洩5年不自覺
- 醫療詐騙與電話行銷 病人隱私安全嗎？
- 要玩真的不簡單！ 富邦機房燒出備援疑慮

Check Point DLP主動檢核並確認，確保機密不外洩

Info Security 2011

最新活動 +more

- 保護個資第一步，打造無縫防火牆
- 微軟資安面面俱到 (Microsoft

三、SONY個資外洩7700萬筆

- SONY Play Station(PS3) 於2011.4.20洩漏
  - • 7700萬筆資料
- 其中23,400為信用卡資料

事件4:監察院提案糾正本部資安管控

- 本(100) 4月監察院對於法務部提出糾正案要旨如下:

"…政風機構對於涉貪法官，未能積極處理，做有效之防制，核有違失。檢察官使用內部網路資料管理鬆散，亦乏有效稽查管考機制，核有嚴重違失，爰提案糾正。"

大法官釋字603號解釋明確宣示：

- 隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第22條保障。
- 大法官不僅認為「隱私權」為憲法第22條所保障之憲法權利，並且認為「隱私權」中之「資訊隱私權」(information privacy)亦屬憲法第22條所保障之憲法權利。

(引自湯德宗，臺灣大學國家發展研究所98學年度第1學期博碩士班(中)比較憲法專題研究課程大綱
ww.nd.ntu.edu.tw/download.php?filename=1335...doc..)

個人資料保護法修法進程

- 1995年，立法院三讀通過「電腦處理個人資料保護法」草案，同年總統公布施行
- 2005年，法務部研擬完成「電腦處理個人資料保護法」草案，並將法規名稱改為「個人資料保護法」，並送請立法院審議
- 2010年4月27日立法院三讀通過個人資料保護法
- 2010年5月26日總統府公布，施行日期尚待行政院訂之
- 施行細則草案法務部已經於網站預告，預計最快在2011年11月提行政院通過
- 新版個人資料保護法預計最快在2012年?月實施

現行「電腦處理個人資料保護法」主要問題

現行「電腦處理個人資料保護法」主要問題

- 適用範圍問題: §3本法用詞定義
  - 六、公務機關：指依法行使公權力之中央或地方機關
  - 七、非公務機關：指前款以外之左列事業、團體或個人：(一) 徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人。(二) 醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。(三) 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
- 限於電腦處理者，不包括人工處理之資訊在內。
- 訴訟程序與經費令當事人怯步

台灣舊個資法民事判決分析(source:達文西律師事務所)

裁判案號	被告行業別	請求權基礎	Brief	賠償金額
臺灣高等法院98年度上易字第1229號民事判決	銀行	電腦處理個人資料保護法第18條、第28條、民法第184條第1項前段、第188條第1項、第195條	原告未曾向被告申請信用卡，然被告於民國97年間誤向聯合徵信中心申報原告持用之信用卡遭強制停卡至原告之名譽、信用受有損害	250,000
臺灣板橋地方法院99年度重勞訴字第10號民事判決	證券商離職員工	民法第153條、第199條、第184條第1項前段、營業秘密第12條第1項前段	被告藉職務上之機會，取得原告未授權被告查閱之客戶資料後離職	214,500
臺灣臺南地方法院94年度訴字第121號民事判決	個人、電信業者及其員工	電腦處理個人資料保護法第28條、民法第184條第1項前段、第188條第1項、第195條	被告甲為利用職務之便，受被告乙之請託擅自進入電腦系統查詢電話使用人即原告之姓名、住址相關資料，並告知被告乙藉以確定原告之身分	個人:150,000 電信業者及其員工:80,000
臺灣臺北地方法院97年度訴字第1683號民事判決	網路書店	民法第184條第1項前段第195條、電腦處理個人資料保護法第28條適用第27條	原告等於被告網站購買台北金馬影展套票，因被告處理疏失，竟夾帶其餘477位註冊成功之會員資料含會員帳號、姓名、地址、電話、手機、電子信箱資料，外流到其他數百人之信箱之中，無法追回	137,900

台灣舊個資法民事判決分析(source:達文西律師事務所)

裁判案號	被告行業別	請求權基礎	Brief	賠償金額
臺灣臺中地方法院94年度重訴字第196號民事判決	銀行及其員工	電腦處理個人資料保護法第六條及第十八條、第二十八條及民法第一百八十八條之規定	被告甲利用任職被告公司業務之機會，取得原告申辦現金卡之個人資料，進而利用此一資料，冒用原告名義，辦理變更住址及掛失補發現金卡	100,000
臺灣臺北地方法院93年度訴字第2455號民事判決	徵信業者、資訊業者	電腦處理個人資料保護法第二十七、二十八條規定	被告乙違法蒐集將原告之個人資料，又與被告甲共同意圖營利，提供被告甲之付費會員，得透過網路超連結 方式，以每筆資料二百元之價格付費查詢	徵信業者:100,000 資訊業者:100,000
臺灣基隆地方法院九93年訴字第82號民事判決	證券商	電腦處理個人資料保護法第二十七、二十八條規定	未經原告同意蒐集其姓名、地址等資料並發送廣告信函	30,000
臺灣宜蘭地方法院羅東簡易庭99年度羅小第56號民事小額判決	網購賣家	民法第184條第1項前段、第195條及電腦處理個人資料保護法	原告於網拍上購買被告商品，被告於評價留言公開原告家中之系爭家用電話號碼，使原告之家用電話號碼遭第三者知悉	20,000
臺灣臺北地方法院簡易99年度北國簡字第16號民事判決	公務機關	國家賠償法第5 條、民法第195 條與電腦處理個人資料保護法	被告將原告之個人資料公布於薪給發放標準之陳情函並予以張貼	5,000

貳、個資法修正重點

個人資料保護法整體架構

第一章　總則

第二章
公務機關之資料處理對個人資料之蒐集、處理及利用

第三章
非公務機關之資料處理對個人資料之蒐集、處理及利用

第四章　損害賠償及團體訴訟

第五章　罰則

第六章　附則

22

立法意旨(一)

- 保護個人隱私(及個資自主權)
- 促進個人 資料之合理利用

第一條　為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人 資料之合理利用，特制定本法

立法意旨(二)

- 個人資料之蒐集、處理或利用原則:

  符合業務需要之最小範圍

  - 尊重當事人之權益
  - 不得逾越必要範圍
  - 與蒐集之目的具有正當合理之 關聯

> 第 5 條　個人資料之蒐集、處理或利用，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，並應與蒐集之目的具有正當合理之 關聯。

新個資法修正重點

一、擴大保護客體：

(一) 不再以經電腦處理之個人資料爲限，包含紙本之個人資料

(二) 增訂第 6 條「特種資料」蒐集之限制

◆ 第 6 條

有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、 處理或利用。但有下列情形之一者，不在此限：

一、法律明文規定。

二、公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當 安全維護措施。

三、當事人自行公開或其他已合法公開之個人資料。

四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，爲統計 或學術研究而有必要，且經一定程序所爲蒐集、處理或利用之個人資 料。

前項第四款個人資料蒐集、處理或利用之範圍、程序及其他應遵行事項之 辦法，由中央目的事業主管機關會同法務部定之。

新個資法修正重點

二、普遍適用主體：

刪除適用主體之限制，即**公務機關及非公務機關，均納入個資法適用之範疇**。但自然人為單純個人或家庭活動之目的者，或於公開場合或公開活動蒐集；處理或利用之未與其他個人資料結合之影音資料者，不適用本法。

公務機關：指依法行使公權力之中央或地方機關或行政法人
非公務機關：指前款以外之自然人、法人或其他團體（新法取消行業別之限制）
受委託者：受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關（§5；新§4）

- 第51條

  有下列情形之一者，不適用本法規定：

  一、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。

新個資法修正重點

三、個人資料定義大幅擴張:

舊法:足資識別

新法:直接或間接得以識別

- 舊法第3條第一項:

  個人資料：指自然人之姓名、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、社會活動 及其他足資識別該個人之資料。

- 新法第2條第一項:

  個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因 、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及 其他得以直接或間接方式識別該個人之資料。

四、增修行為規範

（一）增訂個人之醫療、基因、性生活、健康檢查及犯罪前科等5種資料為特種資料，應特別保護。§6

（二）不論直接或間接蒐集個人資料，均有告知當事人之義務。§8、§9

（三）資料外洩或被竊取時，資料持有者應於查明後以適當方式通知當事人。§12

（四）非公務機關特定目的外利用之條件變更(§20):

1.法律明文規定

4. 基於公共利益為統計或學術研究而有必要，且資料經過處理後無從識別特定當事人。(本款新增)

5. 經當事人書面同意。

非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。非公務機關應於首次行銷時，免費提供當事人表示拒絕之方式。

28

學校衛生法

- §8:學校應建立學生健康管理制度，定期辦理學生健康檢查；…前項學生健康檢查之對象、項目、方法及其他相關事項之實施辦法，由中 央主管機關會同中央衛生主管機關定之。
- §9:學校應將學生健康檢查及疾病檢查結果載入學生資料，併隨學籍轉移。 前項學生資料，應予保密，不得無故洩漏。但應教學、輔導、醫療之需要 ，經學生家長同意或依其他法律規定應予提供者，不在此限。

四、增修行為規範

（五）中央目的事業主管機關個資檢察權:中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護 ....認有必 要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查， 並得命相關人員為必要之說明、配合措施。

（六）非公務機關應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。 (§ 27)

30

四、增修行為規範

- （七）非公務機關有違反本法規定之情事者，中央目的事業主管機關或直轄市、縣（市）政府除依本法規定裁處罰鍰外，並得為下列處分(§25)：
  - 一、禁止蒐集、處理或利用個人資料。
  - 二、命令刪除經處理之個人資料檔案。
  - 三、沒入或命銷燬違法蒐集之個人資料。
  - 四、公布非公務機關之違法情形，及其姓名或名稱與負責人。

五、鼓勵民間公益團體能參與

為方便被害民眾行使本法規定之損害賠償請求，本法修正草案特規定符合一定要件之財團法人或公益社團法人，得代替當事人提起團體訴訟，以節省勞費並保護民眾權益。§32 -39

六、增加對非公務機關代表人之課責

非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三 條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰 之處罰§50

32

七、特種資料之應用

- 醫療、基因、性生活、健康檢查及犯罪前科等5種個人資料為特種資料，應特別保護。非有法“律”明文，執行法定職務且有適當安全措施，或當事人自行公開者，不得收集、處理、利用。
- 為統計或學術研究而有必要，且經一定程序得為蒐集、處理或利用之。但本款之程序、範圍須由中央目的事業主管機關會同法務部定之。違反本條規定者不但有民事賠償責任，更將受到刑法之追訴。§6

責任衝擊(個資法§28)

民事責任

額度-NTD	說　　明
500-20000	被害人“不易或不能證明”實際損害額，依侵害情節，每人每一事件計算。
200000000	同一原因事實造成多數當事人權利受侵害， 合計最高總額。
>200000000	因該原因事實所涉利益 超過2億元者，以該所涉利益為限。
回復名譽	

美國個資法對於個資外洩之罰則

- Model Privacy and Data Security Bill

  Section 10. Enforcement

  - Violation : ….Except that the amount of any civil penalty under such Act may not exceed $2,000,000 for all related violations by a single violator regardless of duration or the number of individuals affected.
  - Federal Trade Commission Act may be increased by up to tree times this amount if there is evidence that the defendant is found to have committed a violation willfully and knowingly

責任衝擊(個資法§42)--刑事責任

- 意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者
  - 處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以 下罰金。
  - 原則告訴乃論(§45)，例外§42，對公務機關犯此罪非告訴乃論。

日本早稻田個資案例

- 事件摘要:大陸領導人胡錦濤訪日，於早稻田大學演講。
- 日警方基於保護外國元首安全，要求學校提供學生名單
- 早稻田大學提供，但遭3學生依個資法告訴
- 法院判賠每位學生USD50(原告訴要求100)

日本早稻田個資案例在我國個資法之適用

- 第 20非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集 之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利 用：

  一、法律明文規定。

  二、為增進公共利益。

  三、為免除當事人之生命、身體、自由或財產上之危險。

  四、為防止他人權益之重大危害。

參、個資法施行細則草案重點

一、新增軌跡資料之概念

- 為保護個人資料之隱私權，個人資料檔案除了備份檔案之外，亦應包括軌跡資料
- 軌跡資料係指個人資料在蒐集、處理、利用過程中所產生非屬於原蒐集個資本體之衍生資訊（LOG FILES），包括（但不限於）資料存取人之代號、存取時間、使用設備代號、網路位址（IP）、經過之網路路徑.....等，可用於比對、查證資料存取之適當性。
  - 第五條　本法第二條第二款所稱個人資料檔案，包括備份檔案及軌跡資料。

二、增訂委託人適當監督義務之規定(細則8)

- 委託他人蒐集、處理或利用個人資料之全部或一部時，委託人應對受託人為適當之監督。
- 前項監督至少應包含下列事項：
  - 一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。
  - 二、受託人就第九條第二項應採取之必要措施。
- 委託人應定期確認受託人執行之狀況，並將確認結果記錄之。

三、修訂「刪除」定義(細則第6條)

- 本法第二條第四款所稱刪除，指使已儲存之個人資料自個人資料檔案中消失(原為消失而不復存在)。
- 前項規定，如為事後查核、比對或證明之需要而留存軌跡資料者，得不予刪除。

四、定義適當安全維護措施(細則第9條)

- 本法所稱適當安全維護措施、安全維護事項或適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之必要措施。

  前項必要措施，應包括下列事項：

  - 一、 成立管理組織，配置相當資源。
  - 二、 界定個人資料之範圍。
  - 三、 個人資料之風險評估及管理機制。
  - 四、 事故之預防、通報及應變機制。
  - 五、 個人資料蒐集、處理及利用之內部管理程序。
  - 六、 資料安全管理及人員管理。...

五、定義適當方式通知(細則第十八條)

- 本法第十二條所稱適當方式通知，係指即時以書面、電話等足以使當事人知悉之方式。但耗費過鉅者，得以網際網路或其他方式為之。
- 依本法第十二條通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施
- 查明:指知悉被侵害之事實

六、增訂專人之定義(細則第21條)

- 第二十一條　本法第十八條所稱專人，指具有管理及維護個人資料檔案之專業能力，且足以擔任機關檔案資料安全維護經常性工作之人員。
- 公務機關為使專人具有辦理安全維護事項之能力，應辦理或使專人接受相關專業之教育訓練。

肆、資訊與行政部門之因應探討

ISO27001的效用問題

- 16個通過ISO27001驗證的機關，經國家資通安全會報技服中心檢測:
  - 11個網站可取得主控權或資料。
  - 內部連至外部中繼站之阻擋比率僅約67.94%

source: 國家資通全會報技術服務中心 99.7.16 “政府資通安全檢測評鑑機制規劃報告”

Key Problem1: 主要的風險因子(技術能力、人力問題) 在調整”可接受風險值“ 下，被淹蓋。

Key Problem2: 通過ISO27001得否主張免除過失之責?

OWASP ASVS 4 Level Verification

(ASVS: Application Security Verification Standand)

- Level 1: Automated Verification
- Level 1A – Dynamic Scan (Partial Automated Verification)
- Level 1B – Source Code Scan (Partial Automated Verification)
- Level 2: Manual Verification
- Level 2A – Penetration Test (Partial Manual Verification)
- Level 2B – Code Review (Partial Manual Verification)
- Level 3: Design Verification
- Level 4: Internal Verification


C:\Users\cchen7\Desktop\資安與委外\委外資料外洩.mht
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
我的最愛
法務部內部網站
又是委外廠商惹的禍！...
網頁(P) 安全性(S) 工具(O)
資安人 INFO SECURITY 領航資安・駕馭風險
牽引國內資安能量 擴大單位防護力
高雄場：12月07日(二)
台中場：12月08日(三)
台北場：12月09日(四)
研討會活動詳情
加入會員 · 會員登入
請輸入您要查詢的關鍵字
搜尋
回首頁 | 資安直擊 | 話題大家談 | 最新活動 | 資安二手市集 | 資安知識庫 | 焦點話題 | 產業脈動 | 產品推薦 | 聯絡我們 | 資安人雜誌 | 資安人粉絲網 | 資安工作職缺
首頁 > 熱門新聞
分享
又是委外廠商惹的禍！美國Honda外洩490萬車主資料
作者：廖珮君整理 01/03/2011
美國接連傳出因為委外廠商安全漏洞導致客戶資料外洩的事件，首先是2010年12月中旬，美國麥當勞發表聲明證實客戶資料外洩一事，不到兩個禮拜，事件主角換成日本本田汽車的美國分公司(以下簡稱美國Honda)，駭客總共竊取了490萬筆車主資料，兩起事件的原因，同樣都是委外廠商系統漏洞所引起。
根據外電報導，駭客入侵美國Honda合作的第三方行銷團隊，成功竊取220萬名車主的登入資訊、電子郵件及車牌號碼，以及270萬名Acura車主的電子郵件，至於車主的社會安全碼、生日、銀行帳戶及其他資訊則未洩露。目前，Honda尚未公佈合作夥伴的名稱，僅告知其業務是發送「歡迎訊息」的電子郵件，給Honda Owner Link或My Acura的帳
知客戶後續該如何處理。
在之前的文章裡，《資安人科技網》探討了委外廠商安全對企業的影響，及委外發送電
本週新聞點閱排行
個資保護從政府資訊應用做起-2 全國地政資料庫在便民與隱私間平衡
Sentinel AV 防病毒引擎推出! - Network Box
根據Network Box資料顯示印度和俄羅斯於八月份成為最主要的病毒來源
又是委外廠商惹的禍！美國Honda外洩490萬車主資料
輕忽系統異常現象 個資外洩5年不自覺
醫療詐騙與電話行銷 病人隱私安全嗎？
要玩真的不簡單！ 富邦機房燒出備援疑慮
Check Point DLP主動檢核並確認，確保機密不外洩
最新活動 +more
保護個資第一步，打造無縫防火牆
微軟資安面面俱到 (Microsoft
本田(US廠)於2011.3洩漏個資470萬筆
完成
網際網路 | 受保護模式: 啟動
100%
文件
桌面
資安與委外
收件匣 - Win...
又是委外廠商...
Mail2000 Em...
No.100040收...
Microsoft Po...
上午 08:39
2011/4/1

新加坡李光耀學院公共政策研習心得摘要

“政策衡量通常以政績之立即呈現或媒體之快速回應為主。決策者鮮少費心思於長程的風險與不確定性問題的預防或規劃上。獎勵或重視過程之效率展現而忽視真正最後產生效果之衡量---華爾街之金融海嘯可為殷鑑”

(摘自受訓資料---動態管理 Prof. Neo Boon Siong)。

個資法第18/27條與BSI10012

- 個資法第18 條:

  公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人 資料被竊取、竄改、毀損、滅失或洩漏。 (非公務機關無專人規定)

  - BSI10012 第4章(Implementing PIMS):
    - 4.1:Key Appointment (Senior manager, and day to day compliance worker)
    - 4.2 Day to day responsibility for compliance with policy
  - 政府組改規定三四級機關不設資訊單位，似與個資法規定意旨相違

我國個資法第18/27條與德國立法例

- 德國個資法第4f,4g兩條共十款詳細界定各個公務機關設置資料保護專人之職掌、訓練、任用與保障等

(德國聯邦法律公報，2003):

- 德國個資法規定政府或民間機構若收集個資之人數達20人以上必須設置個資保護監察人。§4f.(1)
- 個資保護監察人之任命資格須依具備執行任務所需專業，併信用可靠為限。其專業程度依負責資料處理之範圍及資料應受保護程度決定之，並得設置輔佐人。§4f.(2)
- 個資保護監察人直屬於公務或非公務機關首長，其於資料保護監察之範圍執行職務時，不受其他指揮監督。§4f.(3)

德國立法例(2)

- 公務及非公務機關應協助個資保護監察人履行職務，在其職務必要範圍內，輔以人員、處所、設備、資源供其應用。§4f.(5)
- 其中令人印象深刻的為4g第1款:

  用以處理個人資料之程式，應確保其運用符合法令規定。任何處理個人資料之規畫，須知會個資保護監察人。

德國立法例(3)

- 德國個資法第29條另於聯邦設“資訊保護官”，由總理提名，經國會任命，相當我國政務委員
- 課責與賦權(資源、職掌)同時考量

國外資訊人力配置比率

	Employee under1000	Employee over 1000
Business services	3.7%	3.3%
Transportation and logistics	3.0%	2.5%
Professional services	4.4%	3.7%
Construction and engineering	2.0%	1.4%
Media, entertainment and leisure	3.3%	2.5%
Utilities and telecom	1.5%	4.3%
Utilities	2.1%	2.0%
Telecommunications	5.5%	4.9%
Finance and Insurance	7.7%	6.7%
Financial services	9.6%	8.5%
Insurance	3.7%	3.3%
Public sector	5.6%	5.1%
Public services	5.4%	5.0%
Government	4.7%	5.1%
Overall	4.0%	3.4%

Exhibit 3.9 IT Staff as a Percent of Total Staff by Company Size
(*Source:* Forrester.)

人員安全管理及教育訓練(一)

資訊系統安全之威脅：

- Threat from Environment : 15%-17%
- Threat from People :83%-85%
  - Internal People :70%-80%
  - External People :3%-15%

Source :Datapro Report 1995

人員安全管理及教育訓練

- 訓練資訊處人員
  - 強化資安攻防技巧基本能力 PM4:00-6:30
  - 全部人員共同研討委外合約及保密切結應訂定之內容(形成集體意識與可操作性)
- 所屬機關首長
  - 本部統一調訓
- 所屬機關資訊人員
  - 本部統一調訓

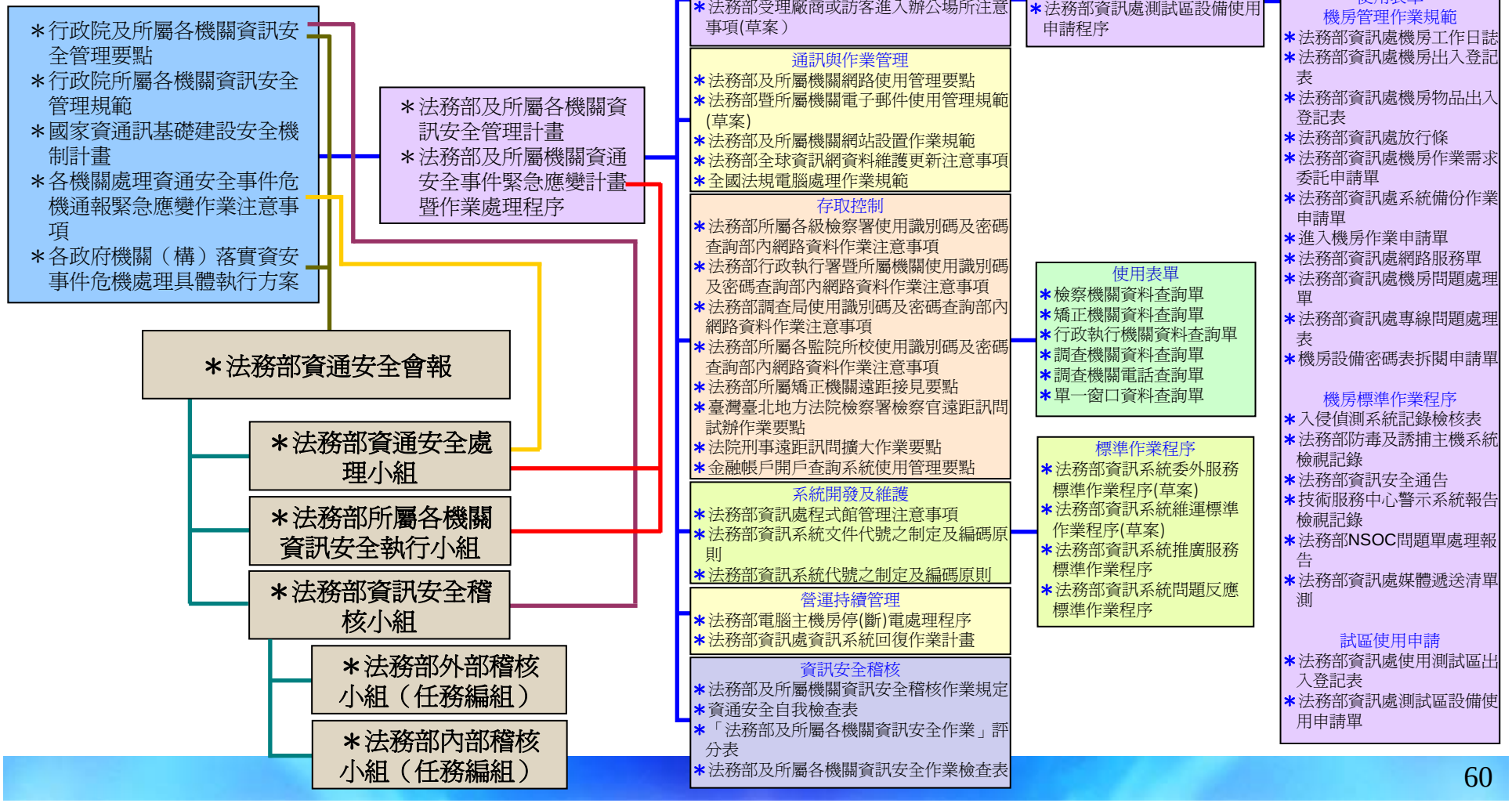
制度/法規(一)

- 國外資安管理法規:
  - US:
    - Information Technology Management Reform Act (ITMRA, Clinger Cohen ACT, 1996)
      §5123 (6),
      §5125 CIO Function and official designated
    - Federal Information Security Management Act (FISMA)

制度/法規(二)

- 國內資安管理法規
  - 法律/命令:
    - 直接以資安為主體之法律-無
    - 相關法律:電腦個人資料保護法、刑法、政府機密保護法等
  - 行政規則：
    - 行政院及所屬各機關資訊安全管理要點
    - 行政院及所屬各機關資訊安全管理規範
    - 各機關處理資通安全事件危機通報緊急應變作業注意事項
    - ● ● ●
  - 法務部資訊安全行政規則體系表

➢法務部資訊安全行政規則體系表



稽核

- 施行方式:
  - 資安外部稽核作業
    - 書面查核(全面)
    - 實地查核(每年擇定5-6個所屬機關)
  - 資安內部稽核作業(法務部各司處)
  - 定期/不定期
  - 程序查核/實質查核
  - 資訊處內部的資安內控機制

肆、結語

- 資安工作貴在實踐，技術面與管理面應並重。
- 資安雖然無法盡於美善，但我們在有限資源下作最大的努力。

簡報完畢
敬請指教