編　者　序

安全，可以說是現階段影響電子化政府、企業商務應用、或使用者信心最重要的因素。一談到資訊安全，外界普遍直接聯想到購買各類軟硬體設備、設置防火牆等。對安全產品的投資，無可置疑地對我們的網路應用環境提供了相當的保護作用，但是買了資安產品就認為安全無虞，卻是絕對錯誤的觀念。因為，「安全」是個動態的概念。這點，從國內外利用電腦系統漏洞的病毒不斷發威並造成損害，而網路安全產品也不斷推陳出新可以得証。而企業、組織在網路應用上的資安風險，不僅來自外部，來自內部因為管理不當而產生的資料盜賣、機密外洩等的資安事件，對組織可能造成更大的損害。

如何提升各界網路安全意識、落實使用者的法制教育，是國家資通安全會報念茲在茲的重點工作項目。本案例集特別委託資訊工業策進會科技法律中心，摘錄近一、二年國內外受到新聞媒體矚目的十餘則案例，參酌司法實務見解進行說明與分析。除針對電腦病毒、駭客與其他電腦犯罪威脅（如妨害電信秩序、侵害智慧財產權等）等議題進行撰擬外，同時考量各級公務人員在實務層面需求，論及網路安全管理與我國政府資訊安全檢測工作的實施，以供各界參考。誠摯希望能藉由這本手冊生活化的實例與精要的解說，為我國的資訊安全法制教育略盡棉薄之力。

行政院國家資通安全會報

技術服務中心　謹誌

目　錄

壹、 電腦病毒的威脅

資料來源：綜合國內外媒體報導

事件：駭客互槓 網路世界混亂

事件描述：

2004 年 4 月 21 日網路安全廠商針對「天網病毒」(WORM_NETSKY.Y)發佈病毒警訊。病毒中心在解碼天網病毒後赫然發現如「Hey, bagle what’ s up?」、「2004 年 4 月 19 日於俄羅斯」等字樣，顯示天網病毒極有可能來自俄羅斯，並且挑釁焙果病毒（PE_BAGLE.N)。據了解，這一場混戰，始於兩隻病毒都想移除於 1 月間出現的悲慘命運（MyDoom）病毒，後來才相互咬上。培果變種病毒出現的第二天就被天網的變種病毒追打，而培果另一隻變種病毒也立即還以顏色；病毒變種速度之快，打破過往案例。

法律意見：

從 2003 年下半年的疾風（MSBlast)、到 2004 年 1 月的悲慘命運、3 月的培果和天網、4 月的殺手病毒(Sasser）等，利用作業系統安全漏洞的混合型病毒不斷改變其行為

模式，小則干擾個人電腦的應用（如殺手病毒僅造成電腦不斷重複開機，不會造成永久性傷害)，大則影響網路傳輸效率，造成網站癱瘓（如 DoS 阻斷式攻擊)。這些病毒傳播速度加快、變種迅速，又由於日常生活中各類基礎建設對電腦網路的倚賴增加，此類資安事故的影響層面日益擴大。

針對駭客製作病毒的行為，我國刑法於 2003 年 6 月增訂第 362 條製作專供犯罪電腦程式罪：「製作專供犯本章之罪（包括§358 無故入侵、§359 無故取得刪除變更、§360 無故干擾）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 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」本條立法目的在嚇阻有心人士撰寫惡性程式進行犯罪，處罰的對象因此針對程式的製作行為；為避免引發產業界及軟體研究者恐慌，本條規定同時以「專供犯罪」、「致生損害」的結果作為本罪構成要件。

案例中駭客相互挑釁，程式製作者的故意顯而易見，並已造成相當規模的損害，應有本條規定之適用；又本罪屬「非告訴乃論」之罪，執法者應主動偵察。惟網路犯罪具有遠端遙控性，如何找到程式製作者並繩之以法，實有賴國際間的司法互助。

資料來源：2003/9/25 **中廣新聞網、**

2004/4/13 **自由時報**

事件：公務電腦大當機

事件描述：

掌管美國入出境的領事電腦系統，於 2003 年 9 月遭到不明電腦病毒入侵，使美國入出境管理局核發簽證出現問題。據了解，這套領事電腦系統至少包含 1 千多萬筆資料，包括對外國申請簽證人士之安全資料。

在國內，花蓮縣警察局、及北市警局若干分局的電腦主機，於 2004 年 4 月分別傳出病毒入侵。花蓮警方僅能確定資料無外洩之虞；而北市警局電腦主機所感染的病毒，據瞭解會自動解除如密碼、防火牆等的安全防護措施，開放資源共享，有可能導致資料外洩。

法律意見：

資訊時代下，各國無不致力發展電子化政府，建置各

類資料庫以促進政府效能，讓政府成為最大的資訊收集者。也由於政府資料庫內資料均攸關民眾權益，隨著病毒結合入侵攻擊對網路環境造成的威脅增加，其功能越強大，組織所需承擔的資安風險也越大。

政府有責任維護公務資料、檔案的正確性、完整性與可用性，不論其係以紙本或電磁紀錄的型態存在。行政院於 1999 年頒佈了「行政院及所屬各機關資訊安全管理要點」，協助政府各級機關建立安全的網路應用環境。現行法制另有電腦處理個人資料保護法（以下簡稱「個資法」），針對公務與非公務機關的電子資料安全進行規範。

根據個資法第 17 條，公務機關有「指定專人依相關法令辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏」之責。因違反規定致當事人權益受損害時，應負賠償責任，並適用國家賠償法規定。此外，雖然電腦病毒防不勝防，但各該公務人員若因違反注意義務，怠於維護資料庫安全，因此洩漏國防（或國防以外）應秘密之文書時，可能成立刑法第 110 條、第 132 條第 2 項的過失洩密罪；也可能依國家機密保護法各相關罪責論之。

貳、 電腦駭客的威脅

一、 癱瘓服務式犯罪

資料來源：2003/10/28 聯合報

事件：大學生試圖擠爆政府網站

事件描述：

某大學學生為抗議政府開闢道路將經過校園，發動網路快閃游擊行動，號召同學上網擠爆政府信箱。不過由於政府網管人員防堵得宜，幸未造成損害。

法律意見：

本案若此次事件真如媒體所載，且造成政府網站癱瘓，相關涉案人之刑責分述如下：

首先就號召他人擠爆信箱者而言，若號召者係以不特定人為對象，恐將觸犯刑法第 153 條「煽惑他人犯罪」罪。若是以特定人為對象，則將觸犯教唆無故入侵電腦罪及教唆無故干擾電腦罪等罪，由於教唆犯罪的對象為公務機關

網站，更將加重其刑至二分之一。最高可處 4.5 年有期徒刑，並可併科 15 萬元罰金。

其次就實際參與擠爆政府網站者而言，將觸犯刑法第 358 條無故入侵電腦罪及第 360 條無故干擾電腦罪等罪。又由於以公務機關網站為對象，依刑法第 361 條規定，得加重其刑至二分之一。最高可處 4.5 年有期徒刑，並可併科 15 萬元罰金。

附帶說明者，若網管人員因廢弛其維護安全之任務而造成網站被癱瘓的結果，則視其具體情況為何，有可能觸犯刑法第 130 條廢弛職務釀成災害罪，最高可處 10 年有期徒刑。

二、 入侵型犯罪

1、妨礙國家安全

資料來源：2004/5/3 中時晚報

事件：駭客大規模以木馬程式竊密案

事件描述：

刑事局偵九隊先後接獲多家企業機構及個人報案表示，電腦出現異常、CPU 使用量激增及帳號密碼無端遭竊等問題，在相關受害人協助下，初步證實國內政府機關、百大企業、竹科園區、學校或個人電腦已大規模遭駭客入侵，並遭植入多種惡意木馬程式，遭流失、竊取的機密資料無法估計。由於事態嚴重，警方特別發佈新聞稿，呼籲各電腦使用者儘速清查、移除可疑程式。

法律意見：

駭客行為中最令人防不勝防的，就是利用如電腦病毒或免費遊戲軟體下載等方式，在當事人不知情的情況下，於使用者系統中植入木馬程式，讓駭客得從遠端為所欲為。除非程式被執行、干擾到系統或電腦的正常運作，否則電腦使用者或管理者並不容易發現，也甚難提防。

從法律觀點，駭客植入木馬和其後續的操控行為主要構成我國刑法第 359 條的無故取得、刪除、變更他人電磁紀錄罪，與第 360 條的無故以電腦程式干擾他人電腦或相關設備罪，分別是 5 年與 3 年的刑責。然而前述之罪，原則上屬告訴乃論之罪。也就是說，除了公務機關以外的被害人，在發生損害後都需要自行提出告訴。至於「竊取」資料的行為，另依其資料內容是否涉及到機密，可成立國家機密保護法或刑法上的刺探收集國防秘密罪。

從資安管理觀點，這類事件真正危害之處，在於犯罪者可藉此隱匿行蹤，讓正常的網路管理行為無法有效運作；而在被當作跳板網站的當事人本身也是受害者的情況下，損害賠償責任的歸屬也殊難明確。所謂「明槍易躲、暗箭難防」，使用者在下載各類應用程式時不可不慎。

2、影響交易秩序

資料來源：2004/4/14 民生報

事件：遭植入木馬 網路銀行不賠

事件描述：

國內發生詐騙集團偽設銀行網站，並發出電子郵件誘使民眾連絡，騙取民眾存款帳號及密碼，或者趁機在民眾電腦中植入木馬程式，盜領民眾存款等情事，造成民眾的財產損失。 然民眾在發現盜領情事後，向銀行主張賠償損失，卻遭銀行以個人疏失為由拒絕。

法律意見：

客戶因電腦遭木馬程式入侵，導致資料及存款遭到盜領，因金額不大，銀行大多同意先行墊付，但並不代表銀行需承擔損失。財政部金融局在發上上述事件後曾表示，由於網路是開放性系統，與自動櫃員機屬於封閉性系統的情形不同，加上個人電腦等安全防護機制的水準不一，因

此除非可確認屬銀行的疏失，否則銀行不會理賠。

根據「個人電腦銀行業務及網路銀行業務服務契約」範本內容，駭客行為所導致之損失，客戶須就「第三人破解授權者代號或密碼而入侵網路」負舉證責任。亦即，依前述契約範本約定，消費者利用網路銀行進行交易需承擔較大之交易風險與責任。所以類似案件中，如果疏失並不在於銀行，銀行最後還是會向民眾追回墊付的款項。

3、損害組織與企業形象

資料來源：2004/3/22 民視新聞

事件：政府網站出現五星旗

事件描述：

總統大選後，疑似來自中國大陸的駭客組織，因不滿選舉結果，在選舉結果揭曉次日即對我方政府網站發動攻擊。包括財政部國庫署等官方網站被置換網頁，及出現五星旗圖樣。我方網站維護人員在發現遭受攻擊後，已經立刻恢復網站正常運作。

法律意見：

由於網路的可匿名性及遠端遙控的特性，使得近年來利用不實 IP 位址及跳板攻擊的事件頻傳。基於政治因素，來自對岸的攻擊也有逐年增加的趨勢。

從所報導的行為描述，駭客的攻擊行為，包括利用電

腦系統漏洞入侵政府網站，及變更相關電磁紀錄。依我國刑法規定，顯然已觸犯刑法第 358 條入侵他人電腦罪及第 359 條未經許可取得、刪除、變更他人電腦罪。由於攻擊對象為政府機關的電腦系統，依第 361 條規定得加重其刑至二分之一。

資料來源：2003/7/8 中國時報社會綜合版

事件：替代役男駭客倉儲案

事件描述：

警方破獲某北縣某替代役男，利用駭客程式入侵公務機關及國立大學電腦，並利用電腦主機中的空間，將盜版 MTV 及電影等資訊儲存其中，並對外招收會員，提供需要販售影音光碟的相關業者下載資訊，牟取利益。

法律意見：

前述案例可從著作權法與刑法兩個層面加以探討該役男可能應負之刑責。

首先在著作權法部份，該役男未經授權而重製他人著作，並儲存於電腦主機中以營利，顯已觸犯著作權法第 91 條第 1 項、第 92 條及第 94 條第 1 項之罪，須論以意圖營利常業重製罪。最高可處 7 年有期徒刑，併科新台幣 300 萬元罰金。

至於刑法部份，該役男雖可能因職務關係得利用服務機關的電腦，但並不表示即可用以入侵他人電腦以從事不法。因此仍構成刑法第 358 條無故入侵他人電腦罪，並得依同法第 361 條加重其刑至二分之一，最高可處 4.5 年有期徒刑，併科 15 萬元罰金。

由於該役男先以入侵他人電腦為手段，方能達成重製盜版資訊於他人電腦主機以營利的目的，在刑法上屬於牽連犯，因此須以較重的意圖營利常業重製罪處斷。

4、損及個人權益

資料來源：2004/3/16 自由時報證券理財版

事件： 人力銀行資料庫遭同業入侵

事件描述：

國內某知名人力銀行在 2002 年 10 月間，發現有大量異常之查詢。經追查 IP 位址後，發現為同業擅自盜用付費客戶的帳號密碼，登入該人力銀行專屬 VIP 資料庫為查詢、下載，因而向法院提出控告。被告業者表示係員工私人行為，雖與公司無關，但該公司仍願意為其行為道歉並概括承受相關損失。

法律意見：

本案例首先需釐清者，由於求職者的個人資料為人力銀行業者獲利之憑藉，人力銀行符合電腦處理個人資料保護法（以下簡稱「個資法」）第三條第七項「以蒐集或電腦處理個人資料為主要業務」之「非公務機關」之定義。本

案應有個資法之適用。

根據個資法第 18 條對非公務機關蒐集個人資料之要求包括：需有特定目的；經當事人書面同意；與當事人有契約或類似契約之關係而對當事人權益無侵害之虞；已公開之資料且無害於當事人之重大利益。被告員工如在未取得求職者同意的情形下蒐集個人資料，有可能觸犯個資法第 33 條規定，得處 2 年以下有期徒刑；其盜用他人帳號、密碼進入資料庫的行為，將可另成立刑法第 358 條的入侵電腦罪。

至於被告企業，根據民法第 188 條，應對受僱員工因執行職務不法侵害他人權利之行為，負連帶之民事損害賠償責任。此外，主管機關得根據第 38 條規定，就企業違法蒐集個人資料的行為，科處企業負責人罰鍰。

最後，由於原告與被告所經營的人力銀行間存在市場競爭關係。本案除了可能涉及企業不當蒐集個人資料行為外，還可能涉及公平交易法不當影響交易秩序的規定。具體的法律責任，仍須視被告網站是否有進一步實質影響競爭的行為而定。

參、 其他電腦犯罪威脅

一、 妨害電信秩序

資料來源：2003/8/14 中時電子報

事件：電話遙控轉接成為犯罪新管道

事件描述：

一名許姓男子向警方報案，指其電話莫名其妙被轉接，讓他的電話只能發話，不能接收，朋友找他找不到，打自己的號碼卻總是打到另一間公司，帳單還無端多了數萬元。警方接獲報案後，逮捕紀嫌等四人，他們涉嫌利用電信公司提供的電話遙控轉接功能的系統漏洞，及部分電話業主沒有變更預設密碼的特性，將他人室內電話成功轉接到手機，再賣給其他犯罪集團使用。

法律意見：

嫌犯非法以有線、無線方式盜接、盜用他人電信設備通信的行為，主要成立電信法第 56 條第 1 項的「盜接盜用他人電信設備通信罪」，可處 5 年以下有期徒刑。此外，由

於涉及常業，可另成立刑法第 340 條的常業詐欺罪，得處 1 年以上 7 年以下有期徒刑。二者從一重處斷。

近來各類新興詐欺案件頻傳，歹徒以電信科技設備為工具，騙誘或恐嚇民眾至自動提款機轉帳匯款，影響社會治安甚鉅。而電信盜接，讓民眾在不知情的情況下，或協助犯罪者逃避檢警追查，或被警方列入人頭資料庫而強制斷話；除此之外，可能還要替偷轉接的電話負擔電話費。這類案件對民眾權益的侵害、對整體電信秩序的危害性可見一斑。

二、 妨害秘密

資料來源：台北地方法院 91 年勞訴字第 139 號判決

事件：企業監看員工電子郵件的法律爭議

事件描述：

某電信公司以員工轉寄公司調薪決定的電子郵件，違反保密的工作規則而逕行開除員工。針對公司涉及監看員工電子郵件部分，被開除員工向法院主張隱私權被侵害。

法律意見：

近來企業與員工之間由於監看電子郵件問題所導致的爭訟，通常是因員工不服僱主的解僱行為，依據僱傭契約及民法與勞動基準法等相關法律起訴而生。由於我國對於監看員工電子郵件的行為，並無直接明文規範，因此司法實務上的相關見解更顯重要。

2003 年 12 月 8 日台北地方法院所作成的 91 年勞訴字

第 139 號判決，對於企業監看員工電子郵件問題，即提出簡明原則可資依循。該判決認為，公司監看員工之電子郵件，是否侵害員工之言論自由、秘密通訊自由或隱私權等基本權利，應視員工是否能對其在公司中電子郵件通訊之隱私有合理期待。若公司對於員工電子郵件之監看政策有明確宣示，或是員工有簽署同意監看之同意書，則難以推論員工對於自身電子郵件隱私有合理期待可能性。易言之，若企業與員工間對於監看電子郵件有所約定，或曾以工作規則明確宣示企業的電子郵件管理政策，則企業監看員工電子郵件應非違法。

然而須注意的是，上述見解僅針對有無監看權限而為說明。至於企業合法監看員工之電子郵件後，更進而解僱員工時，解僱行為合法與否，自須就該行為本身所須符合的規範加以判斷，不可與監看的合法性混為一談。

三、 網路詐騙

資料來源：2004/3/23 FindLaw

事件：「網路釣魚」詐欺 全球知名網站遭假冒

事件描述：

美國德州一名青年涉嫌偽稱美國線上（AOL）或 Paypal 公司帳務處理中心名義，發送電子郵件給會員，聲稱帳戶條款更動，要求收信者到郵件鏈結的網站上「弄清楚」並「同意」這些更動，否則其帳戶將被「凍結」云云。不疑有他的消費者連結到看似官方網站的假網站後，被要求輸入一些個人帳戶資訊。該名青年藉此取得將近 600 名使用者的個人資料，隨後利用以進行其他的金融犯罪獲利。

法律意見：

這類結合傳統詐欺、大量電子郵件和虛設網站誘使民眾主動提供個人身份資料的犯罪，在駭客界稱為釣魚詐欺（Phishing）。犯罪者計畫性地取得民眾個人資料後，偽造證件或上網轉帳，進行所謂的「身份竊盜」犯罪（Identify

Theft Scam）。以下根據網路釣魚行為各階段之違法性，說明其在我國刑法上可能之評價：

「灑網階段」：偽造商家名義散發郵件，並虛設網站。此時可能構成我國刑法第 210 條的偽造文書罪，與商標法第 61 條的侵害商標權。

「魚兒上鉤階段」：蒐集民眾個人資料。由於個人資料（如帳號、密碼）並不構成我國刑法中「動產」的概念（2003 年 6 月刑法修正草案說明參照），行為人蒐集個人資料的行為，無法該當刑法第 339 條之詐欺罪。惟可能得以第 359 條的無故取得他人電磁紀錄罪論之。

「獲利階段」：行為人利用所取得的個人資料，為其他利用行為。如用以製作偽卡，可構成刑法第 201 條之 1 的偽造支付工具罪，可處 7 年以下有期徒刑；用以上網，進行電子轉帳、更改他人財務紀錄時，即可能構成第 339 條之 3 的製作他人財產得喪變更紀錄詐欺罪，可處 3 年以下有期徒刑；若其行為涉及到常業時，可加重其刑至 7 年。

資料來源：2003/12/8 PC Home

事件：天堂盜寶 有法可管

事件描述：

22 歲王姓男子冒用友人帳號、密碼，進入線上遊戲「天堂」，竊取網友市價達 4 萬元虛擬寶物。經網友報警處理後，被檢察官依竊盜等罪起訴。但承審法官認為，刑法於 2003 年 6 月修正後，盜寶案件已不構成公訴的竊盜罪。在雙方當事人達成和解，原告及遊戲公司未提告訴情況下，最後判決無罪。

法律意見：

須強調的是，刑法於 2003 年 6 月修正後，對於網路遊戲玩家的盜寶行為仍然加以處罰，僅規範的基礎不同而已。

以本案例而言，行為人仍將構成刑法第 358 條的無故入侵他人電腦罪以及第 359 條的無故取得他人電磁紀錄罪。然而應注意的是，依據同法第 363 條，上述二罪均屬告訴乃論，若欠缺告訴權人之告訴，則案件將遭到不起訴

處分或不受理判決的命運。本案例判決結果即是一例。因此建議遊戲玩家，若發現自己遭不肖玩家侵害，除向警方報案之外，仍應積極請求遊戲公司出面協助解決，以保障自己權益。

四、 網路販賣違禁物

資料來源：2004/2/18 中國時報社會綜合版

事件：軍人網路盜賣槍枝零件

事件描述：

刑事局偵九隊查獲網路販售改造槍枝集團案，其中並發現有現役軍人涉案。據了解，該集團利用服役共犯在部隊中從事軍品補給職務之便，私藏槍械零件，再交由其他共犯加以組裝成堪用槍枝後，利用封閉式家族網站找尋買主，並高價出售圖利。

法律意見：

本案因有現役軍人涉案，相關人等的刑責將涉及陸海空軍刑法與刑法兩個層面。

首先就現役軍人私藏槍械零件的行為，已觸犯陸海空軍刑法第 64 條第 3 項之侵占軍用武器彈藥以外軍用物品

罪，最高可處 7 年有期徒刑。此外尚觸犯該法第 65 條之未經許可製造、販賣、運輸軍用武器彈藥之主要零件罪，最高可處無期徒刑。

就涉案人等私自組裝槍枝的行為，除觸犯刑法第 186 條的製造販賣單純危險物罪，最高可處 2 年有期徒刑之外，更可能觸犯同法第 187 條的加重危險物罪，最高可處 5 年有期徒刑。而渠等在網路上尋找買主，涉及教唆他人觸犯「持有單純危險物」罪，最高同樣可處 2 年有期徒刑。

上述各罪因有手段目的關係，屬於刑法上的牽連犯，故應從一重罪處刑，亦即最高可處以無期徒刑。

肆、 網路安全管理

一、 業務委外安全控管

資料來源：2004/4/26 **聯合新聞網**

事件：個人資料外洩　疑似業務委外肇禍

事件描述：

高雄市刑警大隊破獲一個專門販賣個人資料給詐欺集團的「優 x 國際行銷公司」，發現將近 2,000 萬筆銀行客戶的個人資料被這家號稱是「詐欺集團資料庫」的公司非法取得，並以每筆 1 到 10 元賣給詐欺集團作案。據判斷，整起事件可能導因於銀行將其資訊業務委外所致。

法律意見：

這起資料外洩案涉及到對個人資料的侵害，原則上適用電腦處理個人資料保護法（以下簡稱「個資法」）。以下分述相關人等的法律責任。

首先是受託處理資料人員的責任。依個資法第 34 條規

定，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輸出，致生損害於他人者，可處 3 年有期徒刑。根據同法第 5 條，受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。因此，即使涉案人非銀行行員，受託處理業務人員與委託銀行，均無法免除個資法責任。

此外，受託處理業務人員亦可能依刑法第 317 條洩漏業務上知悉工商秘密罪處罰，並根據第 318 條之 2，加重其刑至二分之一。

在銀行的責任方面，除了銀行仍必須對外包業務人員所造成的損害負民事上的賠償責任外，個資法對於保有個人資料檔案之公務、非公務機關，另規定有「應指定專人依相關法令辦理安全維護事項，防止個人資料被洩漏」的義務（個資法第 26 條參照）。業者違反義務時，目的事業主管機關得限期改正，並得按次處罰負責人罰鍰。

資料來源：2004/5/7 中國時報

事件：專裝人頭電話 電信公司包商爆弊端

事件描述：

警方查獲郭嫌等 11 人，涉嫌勾結電信公司外包施工人員，利用假證件、空戶申辦電話，再轉接其他地方，供詐欺集團使用。同時，為配合詐騙集團以假冒警察及銀行的新手法，電話裝機人員甚至在偏遠的縣市鎖定當地銀行、警局電話直接掛線，從分機轉接出去。目前正擴大偵辦中。

法律意見：

詐欺集團持用人頭電話轉接再轉接，遙控犯案，詐欺取財的案件層出不窮，影響社會治安甚鉅。針對人頭電話犯濫、阻礙警方查緝工作，內政部警政署已積極建置人頭資料庫，對可疑的人頭電話、帳戶，建立斷話、警示通報系統。各電信公司業者也配合政府，對客戶身份加強核對。但前述案例顯示，所謂家賊難防，業者更應注意執行人員的安全控管。因為歹徒在申裝電話時，施工人員在現場裝

機施工時應能馬上得知異狀，可即時避免歹徒申裝得逞。

案例中，涉案人等利用假證件申辦電話，主要涉及到刑法第 210 條的偽造文書罪。而電話裝機人員在電信設備中掛線、轉接分機的行為，涉及電信法第 56 條的違法盜接電信設備罪，處 5 年以下有期徒刑，得併科新台幣 150 萬元以下罰金。值得注意者，根據電信法第 59 條，法人之代理人、受僱人犯第 56 條之罪者，除處罰行為人外，對該法人亦科以各該條罰金。因此，該電信業者並不會因為業務委外而免責，法院可就本案科業者新台幣 150 萬元以下之罰金。

二、 內部人員管理

資料來源：2004/5/26 **聯合新聞網**

事件：公務員涉資料盜賣 游揆指示懲處

事件描述：

檢調破獲個人資料盜賣集團，涉案人涵蓋刑事局警官、海巡署隊員和中華電信、民營電信員工。游錫堃院長震怒，要求提報懲處名單，並強調不可官官相護。

法律意見：

不論國內、國外的經驗都顯示，政府蒐集的個人資料，由於有公權力背書，具備相當精準性，是最被外界覬覦的資料來源。而政府各類資料庫中，最具敏感性者，非警政系統的資料庫莫屬。這類資料庫因為可在案件發生時提供及時性的背景資料，是協助執法人員辦案的利器，但這類資料庫的安全維護若稍有不當時，極可能嚴重侵害人民權益，打擊公權力威信。

現行法令對政府資料庫的資料應用議題，其實已有相當多規範，如刑法、個人資料保護法等；而通訊保障及監察法、電信法更嚴格禁止非法的通訊監察行為。然而，所謂家賊難防。機關內部人員的安全控管問題，實非單獨之法律規範能盡其功。如何兼顧內部人員資料取用效能，同時保障民眾的資訊隱私，是各政府機關在規劃建置功能強大的資料庫時必須深思的議題。

三、 軟體漏洞公開的安全議題

資料來源：2003/12/11 CNeT **新聞專區**

事件：軟體漏洞資訊公開機制

事件描述：

微軟公司 12 月 9 日表示，其正在調查有關 IE 瀏覽器中存在的一個潛在漏洞。此漏洞，根據丹麥 X 安全公司的通報，有可能幫助不肖駭客創建以假亂真的虛假網站來進行詐騙活動。X 公司在微軟公司發表聲明前，已經對外公布上述漏洞，並展示了駭客會如何利用此一漏洞的過程。

微軟對此發佈聲明，指責 X 公司不應過早公開上述漏洞，暗示這樣做使得微軟沒有足夠的時間來發佈修補程式。

法律意見：

利用系統設計上的缺陷進行攻擊，已成為近一年來資安事件主要的行為模式。資安業者的資料也顯示，近來駭客的攻擊行動與安全漏洞公告的時間差距已經越來越短，從過去的記錄保持者，第 26 天就開始攻擊的疾風病毒

（BLASTER），到 2004 年 5 月的殺手病毒，已大幅縮短到 10 天之內。讓程式漏洞是否應該公開，成為指引駭客明路的議題，開始在國內引發討論。

此議題，各方見解不一。但建立標準化處理程序來縮短事件處理所需時間、降低企業風險，可說是被各方廣泛接受的觀念。在美國，由數家業者成立的網路安全組織 OIS（Organization for Internet Safety）即在 2003 年 6 月 28 日發布了「安全瑕疵公布準則」，希望以推動業者聯盟的方式，建立安全漏洞公開的共通標準。根據準則建議，各社群研究者在將新發現的軟體漏洞訊息公諸於世之前，應先給軟體公司至少 30 天的時間提出修補程式；在進一步公布其細節前，再給予 30 天的緩衝因應期。以免有心人士利用安全漏洞攻擊他人的系統。

從法律層面，利用電腦漏洞進行攻擊的行為，主要成立我國刑法第 36 章的妨害電腦使用罪章。具體罪責，仍依其攻擊態樣而異。

四、 垃圾郵件管理

資料來源：2004/3/11 民視、2004/5/14 工商時報

事件：知名網路商聯名控告散播垃圾郵件

事件描述：

美國的「反垃圾郵件法」（CAN-SPAM Act of 2003）在 2004 年 1 月生效之後，包括微軟和雅虎、美國線上等知名網路商首度在美聯名對數百名散播垃圾郵件者提出六項罪名的控告，罪行嚴重者，最高可能會被判 20 年刑期。

法律意見：

自美國於 2003 年底通過反垃圾郵件法，以刑罰對付濫發垃圾郵件業者後，世界各國可說陸續對垃圾郵件宣戰。

在科技的推波助瀾下，濫發廣告信函的行為，開始在使用者端與 ISP 業者端造成許多困擾。除了使用者隱私權有被侵犯之虞、或信箱因此被塞爆而阻斷正常通訊困擾

外，垃圾郵件在傳輸過程中霸佔頻寬的行為就如同常見的駭客分散式阻斷攻擊行為般，不當加重 ISP 業者提供正常服務的困難。

一般而言，垃圾郵件分為兩種：一種是蒐集消費者個人資料後，不請自來的推銷郵件；另一種是惡性程式，如利用郵件地址產生器，隨機產生郵址後發送。依現行法制，前述二種行為只有在涉及不當干擾他人電腦或其相關設備之使用，並造成損害時，才可能有刑法第 360 條之適用；易言之，垃圾郵件雖然惱人，但除非已造成收信人的實質損害，否則並不構成刑罰。

針對第一類不當蒐集個人資料行銷的行為，法務部已在「電腦處理個人資料保護法」修正草案中增訂保護規定，要求業者首次寄發行銷郵件時，須主動告知收件人如何取得其個人資料，並提供表達拒絕或退件的免費途徑。不過受限於該法保護對象只針對「足以識別個人的資料」，相關規定預料無法適用於第二種類型的垃圾郵件。對此，相關單位已研擬濫用商業電子郵件管理條例草案，希望能健全國內的網路應用環境。

伍、 政府資安檢測實錄

資料來源：國家資通安全會報資安季刊 2003 年夏季號

事件：我國政府機關資通安全檢驗

事件描述：

國家資通安全會報在經過總召集人行政院林信義副院長核定後，於 2003 年 4 月 22 日至 4 月 28 日，針對 525 個 A、B 級政府機關機構、3,347 個 IP，展開為期 7 天之「92 年度政府機關機構資通安全攻防演練實施計畫」模擬駭客攻擊。這是我國首次舉辦的模擬駭客資安攻防演練，目的在不影響各單位正常運作的情況下，檢驗重要政府機關機構資安防護的弱點。

法律意見：

這類模擬駭客進行安全演練，最需要關注者，為擔任假想敵之安全檢測人員（以下簡稱「檢測者」）之身分與可信賴度，從而據以有效掌控參與活動者行為，避免對政府機關機構網站、資料庫的效能與安全產生負面影響。此次檢測活動，因此由官、學、研推薦安全無虞之資訊安全專

業人員，實施甄選合格、簽訂演練作業規定保密切結書後，在限定的模擬環境中進行。

若各該政府機關機構網站因此次演練作業不慎，導致資安事件時，試析各相關人等的法律責任如下：

首先是參與者的責任。若檢測者惡意入侵網站，導致機關機構機密資料外洩時，此時參與規劃、執行之公務員，仍可能因此成立刑法第 109 條或第 132 條的洩漏國防（國防以外）秘密罪；不具公務員身份之參與者，可能仍須依刑法第 132 條第 3 項之非公務員洩漏國防秘密罪負責。

若檢測者未獲授權或逾越授權，對政府機關機構網站實施類似駭客入侵之行為，原則上仍可該當刑法第 358 條無故入侵電腦罪、第 359 條無故取得變更電磁紀錄罪、或第 360 條的干擾罪，並依第 361 條對公務機關實施，加重處罰規定。

另由於多數政府機關機構網站內資料與民眾息息相關，若檢測者逾越權限非法取得民眾資料時，受害民眾仍可依電腦處理個人資料保護法向政府提出告訴。公務機關係採無過失賠償責任。

最後，根據國家機密保護法第 32 條，洩漏或交付經依本法核定之國家機密者，處 1 年以上 7 年以下有期徒刑。因過失犯前項之罪者，處 2 年以下有期徒刑、拘役或科或併科新臺幣 20 萬元以下罰金。第 1 項之未遂犯罰之。各參與人員實應注意此次計畫核定之密等，在保密期限內恪遵保密義務，以落實資訊安全維護工作。