資通安全法律案例宣導彙編

第四輯

編者序

資訊科技發達，網路及通信環境蓬勃發展，不但帶給人類急速而巨大的衝擊，也改變了人類生活模式，然而隨著資訊科技所帶來的便利，也引發不少令人擔憂的資通安全問題。民眾在享受資訊網路所帶來便利性的同時，開始遭受各類網路不安全事件的困擾與威脅：病毒蠕蟲、阻斷服務式攻擊、駭客入侵、網路釣魚、垃圾郵件及間諜軟體等各式各樣的威脅在網際網路上層出不窮，平均每幾秒鐘世界上就有一起資安事故發生。除了入侵性犯罪外，因爲個人資料外洩並進而引發的新興詐欺手法，近年來也困擾著各國執法單位。這些威脅，小則使網路服務中斷，影響民眾個人權

益，大則影響國家安全，破壞社會安定與金融交易秩序。

我國在 2004 年增訂刑法第 36 章「妨害電腦使用」罪章，將網路入侵犯罪正式納入刑罰體系；而賦予民眾個人資料自主權的個人資料保護法（原電腦處理個人資料保護法），目前亦在立法院審議中。法制的修正是有效打擊犯罪的第一步。然而，法律制裁即便再有效，犯罪本身已經造成社會危害，國家仍需動用大量司法資源去調查犯罪、矯正犯罪人等，整體社會付出成本相當可觀。

網際網路具有匿名性、傳輸環境開放性及作業系統安全維護不易等特質。在檢討各式各樣的資安問題後，吾人可發現，民眾對資通安全意識的淡薄是讓有心人士有可趁之機的主要因素。因此，如何加強民眾對資通安全重要性之認識，以全民之力護衛網路環境已成爲各國政府努力的目標。透過對相關案例的分析與學習，建立網路環境應有的法治概念，應是凝聚民眾資訊安全意識，預防網路犯罪的重要關鍵。

爲落實資通安全法制教育，提供社會大眾對於資通安全有更進一步的認識，行政院研考會特別委託財團法人資訊工業策進會科技法律中心，摘錄近年來廣受媒體矚目的國內外相關法律案例，進行說明與分析。考量實務應用層面，除針對各案例說明相關司法實務見解外，亦將網路安全管理建議、我國政府資訊通信安全基礎建設工作等內容一併納入，供各界參考。誠摯希望透過這本案例手冊，爲

我國資通訊環境之法制建設盡一份心力。

財團法人資訊工業策進會科技法律中心 撰稿
行政院國家資通安全會報技術服務中心 謹誌

目 錄

壹、病毒與駭客的威脅

一、癱瘓服務式犯罪

資料來源：2005.02.15.聯合新聞網

事件：MSN 遭病毒攻擊 檔案傳送要小心

事件描述：

2004 年 2 月，微軟即時通訊 MSN Messenger 遭到嚴重病毒攻擊，一張被剝光毛的火雞性感圖片，內藏著不懷好意的病毒，從韓國開始陸續散布到亞洲各地區，包括台灣、日本、大陸等都傳出嚴重災情，並逐步擴大到全球。其主要表現爲當 MSN 用戶上線時，會接到好友一個「傳送檔案」的訊息（包括 new_webcam、LMAO.pif、hot.pif、rofl.pif 等檔案），如果用戶接收後執行開啓，該病毒就會悄

悄進駐電腦中，除可能造成電腦當機、執行速度變慢或使得某些執行動作不能進行外，同時也會再度透過 MSN 通訊錄繼續散播病毒。

法律意見：

隨著網路的普及化，包括 MSN Messenger、Yahoo!奇摩即時通、YamQQ 及 Skype 等提供即時通訊的軟體，都已成爲網路玩家的必備通訊工具。由於此類即時通訊軟體多半提供檔案傳輸的功能，因此不少玩家便紛紛放棄使用電子郵件傳遞檔案，而改將檔案或在網路上看到好玩的程式或圖片等利用此功能直接傳遞給好友或同事，因此也讓即時通訊成爲新興的電腦病毒傳染管道。

對於此種傳送病毒檔案癱瘓他人電腦或網路的行爲，我國刑法第 360 條規定：「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。」本條主要是在處理故意癱瘓電腦設備的網路攻擊行爲，例如：分散式阻斷攻擊（DDoS）或封包洪流（Ping Flood）等，當然也包括影響電腦設備的正常運作。不過，由於事件中的行爲是透過病毒自動發起而傳送的，所以對於無心的玩家來說，應屬欠缺故意，而爲法所不罰。但使用者們應注意，若是明知該程式或圖片檔案等會造成他人電腦無法正常運作，即使只是單純爲了好玩而將該病毒檔案傳送給他人，仍有可能會觸犯上述之罪。

其實對於使用者來說，最好不要隨便接收來歷不明的檔案。要接受檔

案前，應先確認對方是否有要傳送檔案。同時，若不幸中毒，最好也應主動刪除該檔或解毒，千萬別用來惡作劇，以免害人害己。

資料來源：2004.05.27.中時電子報、2004.05.28.自由新聞網

事件：木馬無心 駭客有意

事件描述：

2004 年 5 月 27 日，刑事局偵九隊偵破一起國內公民營機構上千台電腦遭中國駭客植入 Peep.exe 及 PeepBrowser.exe 惡意木馬程式一案，經追查後發現，木馬程式的原始作者竟然是我國籍王姓軟體工程師。該王姓男子所自行研發的這個 peep 木馬程式功能強大，能夠避開防火牆、防毒軟體的偵測，其將原始碼公開在網站上，結果遭大陸情治駭客利用，攻擊入侵我國上百家企業及政府網站，造成企業財產損害，並危及國家安全。

法律意見：

近年有越來越多的木馬程式被發展製作出來，而這些木馬程式常循正當管道進入個人電腦，舉凡電子郵件的夾檔、瀏覽網頁的自動下載、即時聊天或者是點對點的檔案傳輸等，都是後門程式散播的途徑，因此也常讓人防不勝防。後門程式的特性在於，當電腦遭受攻擊後，此程式將會開啓一個可以遠端遙控的後門，而利用這道後門，駭客將可以輕易入侵他人電腦竊取檔案、密碼或者機密資料等，甚至是竊取網路頻寬資源，操控網路上爲數眾多的攻擊跳板去攻擊其他電腦目標，形成分散式阻斷攻擊（DDos）。由於木馬程式作者常公開其原始碼，這些程式只要被有心人士拿來修改，就可以換到不同的網路連接埠或是避開軟體偵測，其衍生的影響可謂甚大。

上述這些具備木馬、後門功能之電腦程式，可能嚴重影響電腦及網路的安全，造成重大財產損失，因此有必要對這些程式的設計者或製作者加以規範。我國刑法第 362 條規定，製作專供犯本章之罪（如利用這些惡意程式犯第 358 條之無故入侵電腦罪、第 359 條之無故取得刪除變更電磁紀錄罪、第 360 條之無故干擾電腦罪）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。是故，任何人設計惡意的木馬程式，不論是自用或是被他人所使用，只要造成第三人損害，均有可能會觸犯本罪，所以不可不慎！

二、入侵型犯罪

1.影響國家安全

資料來源：2004.08.18.中廣新聞網

事件:駭客攻擊 威脅我國防安全

事件描述：

我駐韓代表部辦公室電腦在2004年8月時，疑遭竊聽及盜截機密資料。據了解，我國駐韓代表部公室與外交部連線的電腦，在前幾個月，確實遭到「駭客」的攻擊，所以調查小組人員此次來韓，也將順道調查「駭客」入侵代表部辦公室電腦的事件，並加強安全上的管理。

法律意見：

台灣網路普及率居全球第二，僅次韓國。根據聯合國統計資料顯示，台灣網路系統遭駭客攻擊次數，一年1,173次，高居全球第六名。網路資訊的蓬勃發展，加上常面臨中國駭客的威脅，如何防範網路不速之客，實爲科技產業及國防界的重要課題。

就駭客攻擊或入侵電腦的行爲而言，可能會觸犯刑法第358條之無故入侵電腦罪及第360條之無故干擾電腦罪。考量公務機關的電腦系統被入侵，將造成國家機密外洩，有危及國家安全之虞,我國刑法於2003年6月修正時，特參考美國法律之規定，區別入侵政府之電腦系統與一般個人使用之電腦系統，對於入侵公務機關電腦或其相關設備的行爲加重處罰。故刑法第361規定：「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。」

其次，就網路駭客進一步竊取資料的行爲而言，除成立刑法第 359 條之無故取得電磁紀錄罪，依其資料內容是否涉及到國防機密，還可能成立刑法第 111 條或國家機密保護法第 34 條之刺探收集國防秘密罪。

此外，我國刑法採屬地主義爲原則，因此對於隔地犯，其犯罪之行爲或結果，有一在我國領域內者，即爲在我國領域內犯罪。故一般認爲利用網際網路犯罪之情形，其設站地、發送地、通訊地、可連結地，其中有一在我國領域內者，即爲在我國領域內犯罪，我國即有審判權，司法機關得追訴處罰。惟如何調查跨境犯罪，實有賴國際司法互助。

至於公務機關在資安管理上，目前行政院頒有「行政院及所屬各機關資訊安全管理要點」、「各級行政機關電腦處理個人資料保護要點」等相關法令，規定各機關相關人員負有一定權責，研議資訊安全政策及規範、管理保護資料、資訊系統安全及辦理資訊機密維護及安全稽核等事項。是故，若有人員發生違反要點之情事，將可能依情節遭受處分；更甚者，還有可能觸犯刑法，被移送偵辦，所以對於相關負責人來說，實不可不注意。

2. 損害組織形象

資料來源：2004.07.23.東森新聞報

事件：中國駭客入侵賦稅署網站

事件描述：

2004 年 7 月，財政部賦稅署網站遭中國駭客入侵，不但五星旗在首頁上飄揚，還以簡體字寫上「祖國統一，打擊一切分裂，打擊台獨」等字眼，引起外界注意。相關單位指出，沒有安全漏洞與個人資料外洩的問題。

法律意見：

近年來，網路駭客入侵事件層出不窮。導因於駭客技術日益增進以及網際網路的普及化，使得資通安全威脅從封閉的內部網路轉而面臨開放性高且無限範圍的外界威脅。網路駭客非法入侵電腦的方式及目的非常多，常見利用作業系統通訊協定之漏洞、網站服務設定不當或是網站本身缺乏防火牆等安全防範措施，藉由網路監聽或是類似木馬之程式，侵入網站系統竊取或是損毀資料。

現今我國政府及企業電子化腳步相當快速，惟與先進國家同樣地面臨到電腦駭客危害資通安全的問題。雖然我國刑法已立有妨害電腦使用罪章，用以遏阻網路駭客的各種非法行為，但是在警方追查多起駭客入侵網站案件過程中發現，不少是屬於國外駭客入侵案件，由於通常無法確認來源，因此要追查起來也相當困難。所以真正防範的辦法還是得靠政府機關及企業方面，在主機端設置防火牆等，做好資安措施，不讓駭客有

輕易入侵的機會。

就本案例而言，我國政府機關網站遭駭客入侵竄改首頁，雖無導致個人資料外洩，但已突顯出國家資通安全的重要性。隨著政府積極推動國家資通安全基礎建設工作，爲促使政府機關及重要民間業者重視資通安全並予因應，行政院已於 2001 年 1 月通過「建立我國通資訊基礎建設安全機制計畫」，3 月成立「國家資通安全會報」，並建立起政府機關資通訊系統通報及應變機制，以協助政府機關及重要民間業者之資通訊及網路系統，一旦遭受外來因素破壞或不當使用等緊急事故發生時，能迅速作必要之通報及緊急應變處置，並在最短時間回復正常運作，以降低該事故可能帶來之損害。

在網路開放的環境下，機構團體對於自身網路的防護，必須更加謹慎。除了軟硬體的防護設備外，也需要隨時檢查整個網路是否有漏洞，藉助於入侵偵測系統，是一個可行的方法。而未來任何機構也應將防範駭客視爲最重要的課題之一，以避免發生資料外洩事件。

3. 破壞交易秩序

資料來源：2004.05.04.中央日報、2004.04.14.民生報

事件：網路銀行遭駭客盜領

事件描述：

刑事局於2004年5月初提出嚴重警訊，國內許多金融機構、科技公司等百大企業，遭到駭客大規模以木馬程式入侵，竊取機密文件，且查知至少造成數十家網路銀行近三千萬元盜領轉帳損失。對於習慣使用網路銀行的民眾來說，如果是遭駭客入侵，導致存款遭到盜領，或者其他無法歸因於銀行的情況，民眾可能得自行承擔損失。

法律意見：

網路犯罪問題層出不窮，特別是近年來發生多起網路金融犯罪案件，且手法不斷翻新、花招百出。繼2003年11月某網路銀行客戶資料外洩後，又傳出國內有多家大型銀行之網路銀行遭駭客入侵盜領存款案；接著又發生某銀行現金卡密碼遭人竊取後透過網路連結至聯合信用卡中心的盜領事件，網路金融犯罪案件頻傳，也突顯出網路金融問題的嚴重性如滾雪球般越演越烈。

雖然針對網路駭客的這些行為，可分別以刑法「妨害電腦使用罪章」中之各罪，及偽造文書罪、詐欺罪等來處罰。然而就網路交易所生損失而言，依據「個人電腦銀行業務及網路銀行業務服務契約範本」，對於駭客破解授權者代號或密碼而入侵網路系統所導致之損失，是由銀行來負責；但若是使用者代號、密碼或憑

證等被第三人冒用或盜用時，客戶仍須負舉證責任。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，加上消費者個人電腦的安全防護機制水準不一；因此，如果疏失並不在於銀行，銀行將不會理賠，所以對消費者使用來說，實應小心注意。

在消費者端應防範及注意的事情有：1、常檢查固定使用的網路交易信用卡（建議使用固定的一張信用卡當作網路交易卡，並且限定信用額度）紀錄是否異常。2、避免開啓來路不明的電子郵件及檔案，並且安裝防毒軟體以避免駭客入侵。3、安裝防火牆以偵測駭客入侵竊取機密資料。4、不要在不明的地下網站做線上交易。5、不要在網咖或公用電腦上做線上交易或轉帳。6、切勿用懶人密碼，例如以生日、身份證字號…等，以免輕易被破解。

資料來源：2005.02.17.中時晚報

事件：破解線上付費網站機制

事件描述：

2005 年 2 月刑事局偵九隊查獲一詐騙盜刷集團，該集團嫌犯以盜取的被害人資料，冒名向發卡銀行申辦信用卡，還開通發卡銀行的網路銀行服務功能，在 ezPay 及 PayPal 線上付費網站上網註冊，取得授權碼後，立刻刷卡儲值。其後嫌犯再以被害人信用卡資料向拍賣網站購物，消費盜刷信用卡儲值的虛擬貨幣，向賣家購買高價的 3C 產品，或者直接把儲值的虛擬貨幣轉匯到另外一個人頭虛擬帳戶，並轉匯到銀行的人頭戶，從 ATM 提款機領走現金。

法律意見：

隨著網路購物、網路銀行日漸發達，網路交易的安全問題也日趨受到重視。在 C2C（個人對個人）交易部分，由於傳統轉帳方式的不便，因此多透過「線上付費網站」來進行。目前各「線上付費網站」在民眾申請會員資格後，可利用個人信用卡至該「線上付費網站」的虛擬帳戶內「刷卡儲值」，並據以付費給他人、代繳費用或是至各拍賣網站向他人購買商品，是一種非常方便的金融服務。然而這些線上金流服務雖爲現代人帶來了不少方便，但網路的特性也使得許多不肖之徒有機可乘。

根據刑法，關於案例中嫌犯以盜取的被害人資料，僞填信用卡申請書後向發卡銀行冒名申辦信用卡的行爲，乃將構成僞造署押及僞造文書

罪。其次，嫌犯以他人名義申請取得發卡銀行核發之信用卡後，開通網路銀行服務功能，在各線上付費網站註冊，盜刷獲取虛擬貨幣等行為，並造成發卡銀行及線上付費網站損失，則可構成詐欺罪及偽造文書等罪。其後，嫌犯持虛擬貨幣至購物網站向賣家購買高價的 3C 產品，或把虛擬帳戶內的儲值現金，轉匯到另外一個人頭虛擬帳戶，並轉匯到銀行的人頭存摺中，從 ATM 提款機盜領現金的行為，並造成網路賣家及銀行受損，將可再構成數個詐欺罪。

從資安觀點而言，如何加強信用卡代辦的安全管理，重新檢視網路銀行的作業程序，以及加強「線上付費網站」的審核制度，以避免成為詐騙集團的洗錢管道，將是未來線上金流服務的重要課題。

4. 危害個人權益

資料來源：2004.10.07.民視新聞

事件：線上遊戲 玩家帳號寶物失竊

事件描述：

2004 年 10 月初，多達 400 萬會員的天堂網路遊戲服務驚爆遊戲公司網站疑似遭到駭客攻擊事件，傳出許多玩家的帳號遭盜、寶物遭竊。有線上遊戲玩家投訴這波駭客入侵讓他們的個人資料被偷，而且虛擬寶物及金幣也被盜走，他們希望業者正視玩家的權益。

法律意見：

現今網路幾乎已成爲現代人在日常生活中的一個必需品，而不少網路玩家更是熱衷於網路遊戲。不過以網路遊戲「天堂」爲例，其中寶物、天幣（虛擬貨幣）遭竊或帳號遭盜用之情形，使得網路遊戲不僅只是遊戲，已有不法之徒藉著遊戲之名，行犯罪之事實。由於在「天堂」遊戲中，玩家必須耗費許多時間、金錢與精神埋首於所謂的「練功」，所以一些初學者爲省去練功時間，便會向技術高明或遊戲人物等級高的玩家購買寶物、天幣等，從而便有人藉由販賣寶物或虛擬貨幣來牟利，也因此衍生出許多法律問題。

就犯罪層面而言，關於線上遊戲的玩家帳號遭盜或寶物遭竊，在過去是以竊盜罪論處。在刑法於 2003 年 6 月增訂第 359 條「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」後，竊取他人帳號或虛擬寶物電磁紀錄之行爲，應論以第 359 條之無故取得電磁紀錄罪，不再以竊盜罪論處。

此外，刑法第 358 條另規定「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。」故針對線上遊戲來說，只要是未經過帳號所有人的同意，私自輸入帳號密碼進入遊戲網站，就要負起 3 年以下的刑責；如果進入後還把寶物拿走或丟掉，或者是變更密碼等，可就要負起 5 年以下的刑責。又這兩條之罪均需告訴乃

論，也就是被害的遊戲玩家必須報案，司法才能發動偵查。

貳、其他電腦犯罪的威脅

1. 網路詐騙

資料來源：2004.10.13.中國時報

事件：網釣詐騙 小心上鉤

事件描述：

2004 年 10 月，一名大學肄業黃姓男子，利用「網路釣魚」（phishing）的變種手法「網路豬籠草」，涉嫌架設虛假的「中國信託」與「中華商業銀行」的網路銀行網頁，利用相似的網址，以魚目混珠的方式，誘騙兩家網路銀行的客戶誤信點選登入，從而套取其帳號、密碼，再憑此將被害人存款轉至人頭帳戶，被害人多達六百多人。

法律意見：

除手機簡訊詐財、電話詐財外，現在還有一種網路詐財手法「phishing」，意即「網路釣魚」。其手法目的是在騙取受害人之個人金融資料，如帳號、密碼、身分證號碼及一些可藉以盜用受害人存款或信用卡等資料。當歹徒取得資料後，甚至使用受害人之名義去貸款、申用信用卡及駕照等，讓受害人信用破產。

典型案例通常爲受害人會收到發自知名且平日有來往金融機構或公司之電子郵件(例如往來銀行)，信上可能警告收信者因發生某些問題，若不立即處理，將可能產生嚴重後果。信末通常提供網址，引誘收信人直接點選進入其僞設網站。該網站與正確的銀行網站相似度極高，往往令人難分，待進入網站後常會跳出另一視窗，要求收信人鍵入個人金融資料以利身分確認，如帳號、密碼及一些足以佐證個人身分之資料等，一旦回應，受害人的資料即落入歹徒手中。

關於此類詐騙行爲，由於歹徒常利用虛假的電子郵件或銀行網站來引誘被害人進入，故就前階段編輯電子郵件或虛設銀行網站而言，係屬僞造電磁紀錄之行爲，應成立刑法上僞造準文書罪（按刑法第220條規定，電磁紀錄足以爲表示其用意之證明者，以文書論）。其次就後階段歹徒取得被害人所輸入的個人相關資料後，進一步利用他人帳號密碼，進入銀行網站更改其密碼之行爲，則應成立刑法第359條之無故變更電磁紀錄罪；其將被害人的帳戶存款轉走之行爲，則應

另成立第 339-3 條之電腦詐欺罪。

至於在自我保護方面，切勿應不明人士要求以電話或其他網路方式提供個人資料予他人，惟若相信對方是真正要接觸之對象，應主動親自確認或檢查該網站之正確性。而平常應有檢視個人戶頭內來往紀錄之習慣，以確認每筆紀錄皆爲正確，若不幸成爲受害人時，應立即通知往來銀行，告知已被騙之訊息，並向財團法人金融聯合徵信中心查詢。

2. 妨害電信秩序

資料來源：2004.04.12.趨勢科技

事件：手機病毒 蠢蠢欲動

事件描述：

自 2004 年 6 月全球出現第一隻以行動電話爲攻擊目標的食人魚病毒（Cabir）後，具有無線網路功能的智慧型手機便開始成爲駭客及病毒作者的新戰場。在 2005 年首季，更陸續出現第一隻會讓電腦與手機產生連鎖中毒效應的「雙響砲病毒」（PE_Vlasco.A），使電腦及部份手機應用程式無法運作；還有會利用 MMS 多媒體簡訊主動散播給通訊錄上朋友的「武士病毒」（SymbOS_Commwarrior）；以及能

摧毀手機作業系統的木馬病毒（Fontal.A）等。

法律意見：

隨著提供多功能的智慧型手機發展，駭客及病毒作者也開始轉向以手機爲攻擊目標。由於智慧型手機一般多內建行事曆、電子郵件、即時傳訊、辦公室應用軟體等功能，以及藍芽、Wi-Fi 等無線網路傳輸功能。因此透過無線網路途徑，駭客便可輕易入侵，取得使用者的行事曆、聯絡人名單和其他敏感資料；或是將行動電話變成一具竊聽裝置，暗地裡傾聽對話，甚至以病毒完全癱瘓手機，引發安全漏洞等。以目前智慧型手機成長快速來看，這類令人頭痛的新案例將可能會層出不窮。

對於製作病毒的行爲，刑法第 362 條規定，製作專供犯罪（例如利用病毒程式干擾電腦）之程式，而供自己或他人使用，致生損害於公眾或他人時，處 5 年以下有期徒刑、或科 20 萬元以下罰金。但刑法妨害電腦使用罪章中之條文大多以「電腦及其相關設備」爲犯罪客體，然而手機並非電腦，亦非電腦的相關設備，則未必能類推適用而予以相繩。惟在刑法解釋上，若智慧型手機具有與電腦相同類似之構造、處理功能或可以上網等，可視爲小型的掌上電腦，或可透過解釋有成立本章各罪的可能。

其實對於使用者來說，接到來路不明簡訊最好直接刪除，不明手機程式更不要任意安裝；同時，下載手機鈴聲或手機遊戲，也一定要

到官方網站進行；如果不慎中毒，最好暫時關閉手機上的藍芽接收功能，以免繼續搜尋感染目標。

3. 個人資料外洩

資料來源：2004.06.02.自由新聞網

事件：個人資料外洩 資安問題嚴重

事件描述：

2004 年 6 月，台北市檢調偵破歷來筆數最龐大的個人資料外洩暨販售案，查知三家民間公司，疑勾結公務機關或特定民營公司不肖人員，長期不法蒐集、販售上千萬筆國內企業及個人資料。這個以劉嫌爲首的集團，堪稱國內盜賣個人資料始祖，3 個集團掌握的資料超過 2000 萬筆，經調查發現，資料外洩的單位包括政府機關、電信事業以及金融事業單位等。

法律意見：

近年來不法販售個人資料集團橫行，已成「全民公害」，由於個人資料外洩的新聞事件層出不窮，而遭詐欺集團利用的案例也不斷發生，令人防不勝防，使得個人資料保護的問題再受爭議。經追查發現，包括金融單位、電信事業、公務機關、醫療院所、各級學校等都是個人資料的外洩管道，其中以行動電話申請用戶遭洩密的最多，估計全部已超過二千萬筆。

對於公務機關或企業內部人員洩漏個人資料的行爲，在普通刑法方面，可能觸犯的有背信罪、洩漏工商秘密罪及洩漏電腦秘密罪等；而在特別法方面，則可能觸犯「電腦處理個人資料保護法」第 34 條：「意圖爲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爲非法輸出、干擾、變更、刪除或以其他非法方法妨害個人資料檔案之正確，致生損害於他人者，處 3 年以下有期徒刑、拘役或科新台幣 5 萬元以下罰金。」此外，對於不法集團蒐集及盜賣個人資料的行爲，則屬違反同法第 19 條之規定，依同法第 33 條，得處以 2 年以下有期徒刑、拘役或科新台幣 4 萬元以下罰金。

關於個人資料的保護，我國雖訂有「電腦處理個人資料保護法」，但前提是個人資料必須是透過「電腦」處理的，才符合構成要件，因此在這種情形下，凡是沒有經過電腦輸入存檔的個人資料即使外洩，法律上也不會構成犯罪。爲貫徹對

個人資料之保護，在 2005 年的修正草案中，已把「電腦處理個人資料保護法」的名稱改爲「個人資料保護法」，擴大個人資料的保護範圍，而不再只以經電腦處理的個人資料爲限。同時，鑑於這類侵害個人隱私權益的犯罪問題日趨影響嚴重，爲加強對個人資料的保護，遏阻盜賣個人資料的行爲，在草案中也針對意圖營利不法者，將刑罰提高到 5 年以下有期徒刑，得併科新台幣 100 萬元以下罰金，並取消告訴乃論，以期加強打擊此類不法行爲。

4. 網站提供違法用途

資料來源：2005.02.01.法源法律網

事件：網路賭博 不是國內網站就沒事?

事件描述：

根據統計，台灣目前網路上找得到的賭博網站，就高達 6 萬多個，其中包括百家樂、21 點、俄羅斯輪盤、麻將、賭馬、職棒、職籃、美式足球、英超聯賽等應有盡有，只要刷卡買點數就可下注，贏了輸入銀行帳號，錢就會匯到戶頭，可謂最方便的賭博方法。

法律意見：

近年來，台灣已逐步開放因特定目的而設立的博奕制度(如政府允許之彩券)，但未經允許的賭博，還是屬於犯罪之行爲。本案中，提供網站者是否有違反刑法第 268 條意圖供給賭場或聚眾賭博罪：「意圖營利，供給賭博場所或聚眾賭博者，處三年以下有期徒刑，得併科三千元以下罰金。」之適用，解釋上有正反兩面之爭議，但就業者同時供不特定的多數網友進入該網站爲賭博行爲，適用聚眾賭博的概念，應無爭議。因此，只要業者藉由網路設備提供大眾於該網站進行賭博以獲利，就應適用本條的圖利提供賭場罪。

有些網站業者可能認爲，只要網站不設在台灣地區，便可以規避相關的刑責問題，但依據刑法第 4 條規定：「犯罪之行爲或結果，有一在中華民國領域內者，爲在中華民國領域內犯罪。」所以縱使網站位於國外，但使用者或網站操作者在我國領域內上站從事犯罪行爲，司法機關一樣可以主張管轄權。

至於民眾透過該網站進行賭博行爲，有無違反刑法第 266 條普通賭博罪：「在公共場所或公眾得出入之場所賭博財物者，處一千元以下罰金。」，由於網路乃依虛擬之空間是否符合「公共場所」或「公眾得出入之場所」，仍有爭議。但若就同法第 267 條規定：「以賭博爲常業者，處二年以下有期徒刑，得併科一千元以下罰金。」，使用者若網路賭博成癮，甚至以之爲職業，那麼就較無爭論的空間，依法要負刑事責任。

5. 有害內容防制

資料來源：2004.04.27.星報、2004.11.23.蕃薯藤新聞網

事件：網路分級 保護兒童及少年

事件描述：

行政院新聞局於 2004 年 9 月 26 日發布「電腦網路內容分級處理辦法」，明訂網路內容分級之標準，希望建立網際網路秩序，保護兒童及少年，避免接觸不適合其年紀的網頁內容。包括中華電信 Hinet、數位聯合、亞太線上、速博、雅虎奇摩、網路家庭、新浪網、蕃薯藤、和信超媒體等，均已於 2003 年 3 月 29 日簽下自律公約，積極配合網站內容分級制度的推動，並針對網域的內容進行自律控管。

法律意見：

依據兒童及少年福利法第 27 條規定:「出版品、電腦軟體、電腦網路應予分級；其他有害兒童及少年身心健康之物品經目的事業主管機關認定應予分級者，亦同。前項物品列爲限制級者，禁止對兒童及少年爲租售、散布、播送或公然陳列。第一項物品之分級辦法，由目的事業主管機關定之。」行政院於 2004 年 4 月 26 日公布「電腦網路內容分級處理辦法」，並於第 10 條要求電腦網路服務提供者，應自施行之日起十八個月內，完成電腦網路分級之相關準備措施，並進行分級。爲繼日本之後，第 2 個實施

網路分級之國家。

該辦法第 4 條將網路區分 4 級，分別爲：一般人皆可瀏覽的「普遍級」、未滿 6 歲兒童不宜瀏覽的「保護級」、未滿 12 歲兒童不宜瀏覽，12 歲以上未滿 18 歲的少年需父母或師長輔導瀏覽的「輔導級」、未滿 18 歲不得瀏覽的「限制級」。平臺提供者與內容提供者需就其內容標示分級標誌，並應標示是否設有管理員。而若發現內容違法或違反分級規定者，依據同法第 8 條，政府機關應爲其他限制兒童及少年接取、瀏覽之措施，或先行移除之措施，以保護使用者。

雖說網路內容分級處理辦法的實施成效仍有待觀察，但欲透過網路分級制度，以減少兒童或青少年透過網路接觸到危害身心健康之圖文，需透過家長的主動配合，隨時關心小孩的上網情形，才可以給兒童及青少年一個無害的網路空間。

參、網路安全管理

1. 垃圾郵件管理

資料來源：2004.12.08.中時電子報

事件：垃圾郵件 癱瘓電腦系統

事件描述：

刑事警察局偵九隊在 2004 年 9 月接獲一家軟體公司黃姓負責人報案，指稱該公司所營運維護的網站遭不明人士入侵，經查爲某男子爲了替自己經營的網站行銷，竟利用網路發信軟體系統，侵入該軟體公司主機，大舉發送廣告郵件，造成該公司所管理之戶政機關網路系統癱瘓，嚴重影響民眾權益。

法律意見：

垃圾郵件之氾濫，已是各國所重視之重要課題，依據 Spamhaus 於

2004 年 11 月公佈的 2004 年 10 月全球垃圾郵件量前十大國家中，我國垃圾郵件量已躍居全球第四大國家。垃圾郵件（Spam）的濫發，不但會造成網路資源的浪費，更對個人隱私與正常使用造成危害。

目前我國尚未有正式的反垃圾郵件法，亦未針對大量寄發垃圾郵件訂定任何懲罰規定，所以針對大量發送電子郵件之行爲，並無直接法律依據予以懲處。但本案中「造成軟體公司客戶電腦主機嚴重當機和癱瘓」之行爲，已違反了刑法第 360 條，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，須處 3 年以下有期徒刑、拘役或科或併科般 10 萬元以下罰金；而受損害者，由於包含公務機關電腦主機，符合第 361 條之加重要件，得加重其刑至二分之一。該男子爲了大量寄發電子郵件，以吸引消費者購買其商品，誤觸刑法之規定，實得不償失。

垃圾郵件的問題，已對電腦使用者造成不小的困擾，目前各國已展開立法行動，希望加以規範。我國之「濫發商業電子郵件管理條例」目前正在審議當中，相信法案通過後，透過政府的介入與法律的保護，將有助於減少垃圾郵件的網路亂象。

2. 軟體漏洞補強

資料來源：2005.01.13.聯合新聞網

事件：軟體漏洞 盜版遭殃

事件描述：

微軟於 2005 年 1 月 12 日公布 3 項新的「漏洞」，並呼籲大眾儘速下載修補程式。不過此一消息之發佈，對大補帖用戶而言，是一大惡耗。依照微軟過去公布重大「漏洞」的經驗，往往變相替駭客指引一條攻擊捷徑，使用盜版軟體者因無法下載更新修補程式，被「駭」的機率相對提高。

法律意見：

當系統業者發現其提供之程式有漏洞時，往往會透過網路傳輸的方式，提醒消費者儘快上網站下載更新檔案，以免遭受損害，但當系統業者公佈消息時，對使用盜版軟體或是大補帖的用戶，則是一大惡耗。

依據我國著作權法規定，就重製、散佈、以公開放映方式侵害著作財產權、侵害著作人格權等行為，均有相關的刑罰規定。使用者除適用重製之刑罰規定外，尚需負同法第 88 條「因故意或過失不法侵害他人著作財產權或製版權」之責任。

除法律風險外，盜版使用者須額外負擔相當大的技術風險；也就是，當軟體發現有漏洞或是需更新病毒碼時，盜版使用者無法及時更新系統資料，而容易導致電腦遭受病毒侵害或是損害的情事發生。所以使用者在貪小便宜享受盜版軟體之優惠時，不可不注意其背後可能帶來莫大的損

失與傷害。

3. 內部人員管理

資料來源：2003.07.21.中時電子報

事件：國軍洩密嚴重 危害國家安全

事件描述：

根據監察院內部調查研究報告發現，部分承包國軍重要武器的製造商，竟將零件轉往大陸生產，再運返台組裝，嚴重衝擊我國防安全。該報告在檢討我國防制軍情外洩的部分指出，除了長期存在的網路駭客威脅之外，中共對我情蒐滲透威脅日甚，並積極強化成計畫性竊密、情蒐活動。

法律意見：

我國「國家機密保護法」於 2003 年 2 月 6 日公佈實施，該法中第 4 條將國家機密區分爲「絕對機密」、「極機密」、「極密」三個等級，並在第 2 章中明確規範國家機密核定之權責、保密與解密之條件等。國防部爲了配合國家機密保護法的制定與陸海空軍刑法第 78 條之規定，於同年 4 月 25 日修訂「軍事機密與國防秘密種類範圍等級劃分準則」，以處理軍事及國防機密。

國軍之重要武器，依據「軍事機密與國防秘密種類範圍等級劃分準則」第 8 條第 1 項之規定，屬於軍備類軍事機密；軍事武器之零件，依據同規則第 15 條第 2 項之規定，屬於軍備類國防秘密。而同法第 2 條則規定：「軍事機密與國防秘密種類、範圍及等級劃分等，依本準則規定，本準則未規定者，適用國家機密保護法及其有關法令之規定。」而機密等級之劃分與核定，則依「國家機密保護法」第 4 條及第 7 條之規定辦理。

本案中之武器，經核定機密等級並告知製造商後，依據「國家機密保護法」第 2 條及第 3 條之規定，承辦之政府單位與製造商，均受到國家機密保護法的規範，一旦從事第 5 章所規定之違反國家機密保護法之行爲，均會受到刑罰之制裁。值得注意的是，同法第 26 條更特別規定，國家機密核定人員、辦理國家機密事項業務人員及前 2 款退、離職或移交國家機密未滿 3 年之人員之出境，須經應經其（原）服務機關或委託機關首長或其授權之人核准後，始可出境。

4. 離職員工管理

資料來源：2004.03.25.中國時報、2004.11.19.聯合新聞網

事件：離職員工扮演駭客 造成公司損失

事件描述：

具有美國電腦碩士學位的張姓男子，因不滿遭美國知名網站購物公司開除，爲求報復，竟上網扮演駭客，利用先前預留後門，先後 6 次入侵網路伺服器主機，移除該網站伺服器內 1830 餘家電子商店網站之商業資料，導致這些電子商店無法繼續從事交易，嚴重干擾公司網站伺服器主機及該電子商店之交易紀錄處理。

法律意見：

目前網路犯罪中最常見的手法包含網路釣魚、架設外掛程式、挾怨報復、癱瘓對手等等，本案即屬於挾怨報復型的案例，而此類案例也是台灣比較常見之電腦犯罪案例。

本案中，張某於離職後，在無合法權限之情形下，入侵伺服器主機之行爲，已違反刑法第 358 條，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，得處以 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金；而移除電腦伺服器中之電磁紀錄，則違反刑法第 359 條無故取得、刪除或變更他人電腦或相關設備之電磁紀錄罪，依法得處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。惟此兩條罪均爲告訴

乃論，須由被害者提出告訴後始爲受理。

當前社會，公司企業仰賴電腦作業的比重越來越重，而人員流動則在所難免。如何避免因爲人員的流動，而造成公司資料的外洩或是惡意的破壞，需要企業或公司制定一套安全機制因應，以減少無謂之損失。

肆、其他

1. 網友的責任

資料來源：2005.03.03.中國時報

事件：公開他人資料 害人害己

事件描述：

某校研究生，與學妹有曖昧關係，引來女方男友的不滿，上網公佈他們魚水之歡的過程，沒想到短短數小時，引來 5 千篇的回應，事後校方緊急關閉 BBS 站。但當事人的照片和課表已經被公開，校方緊急介入，由相關單位負責保護學生的安全，並透過心理諮商中心，對學生進行輔導。

法律意見：

網路是一個匿名的虛擬空間，在 BBS 站上，經常可以看到網友們留言

互打「筆戰」，甚至於涉及人身攻擊、辱罵或誹謗他人；或是傳播子虛烏有的事情，造成他人的名譽受損。而這些行爲，均有可能觸犯刑法。

關於上網公佈他人隱私活動之行爲，依據刑法第 310 條規定：「意圖散布於眾，而指摘或傳述足以毀損他人名譽之事者，爲誹謗罪，處一年以下有期徒刑、拘役或五百元以下罰金。散布文字、圖畫犯前項之罪者，處二年以下有期徒刑、拘役或一千元以下罰金。」本案女學生之男友透過文字公佈他人魚水之歡之言論，實觸犯了本罪，若其公布之內容爲不實，得處以 2 年以下有期徒刑。

此外，在網站上附和之人，若發表不當言論評述當事人，也可能成立毀謗罪或公然侮辱罪。除此之外，若網友有上傳一些關於他人隱私的照片，還可能涉及刑法第 315-1 條：「有下列行爲之一者，處三年以下有期徒刑、拘役或三萬元以下罰金：二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者」。

2. 新興科技的安全

資料來源：2004.07.16.工商時報

事件：無線駭客 隔空刷卡

事件描述：

刑事警察局偵九隊破獲國內首宗「無線駭客」盜用企業無線上網資源，向加油站員工購買客戶信用卡號等個人資料，再上網盜刷信用卡案。由於警方及時查獲嫌犯，未造成金融機構及民眾太大損失，但這種新的金融犯罪手法，已對市場秩序構成極大威脅。

法律意見：

網路盜刷信用卡爲一新興之犯罪行爲，犯罪人通常利用事先取得之他人卡號及有效期限，再上網蒐尋可以刷卡購物之網站，僞冒他人名義進行交易，達到詐騙之目的。

本案行爲人破解密碼而盜用企業無線上網資源之行爲，已違反刑法妨害電腦使用罪章第 358 條之規定，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之規定，得處以 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。其次，行爲人上網盜刷信用卡之行爲，則違反了刑法第 339-3 條，意圖爲自己或第三人不法之所有，以不正方法將虛僞資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更紀錄，而取得他人財產，得處以 7 年以下有期徒刑。

至於加油站員工爲一己之利益，盜賣信用卡之相關資料，依「電

腦處理個人資料保護法」第 34 條規定，意圖爲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爲非法輸出…妨害個人資料檔案之正確，致生損害於他人，得處以 3 年以下有期徒刑、拘役或科新臺幣 5 萬元以下罰金。

3. 個人電腦的維護

資料來源：2004.02.18.CNET

事件：飆網前 先做好防護

事件描述：

網際網路風暴中心（Internet Storm Center）最新研究發現，沒有裝上修補程式的 Windows 電腦在連上網際網路 20 分鐘內就可遭惡意軟體（malware）攻破，2003 年同樣的情況則約需 40 分鐘。這意味著用戶的平均「存活期」越來越短，用戶可能來不及下載所需修補程式來保護電腦免於網際網路的威脅。

法律意見：

隨著電腦使用的普及化，惡意破壞電腦資訊的病毒也越來越多，並在網路上伺機而動，找尋最適合破壞的電腦，而剛組裝完成，未及裝設任何防毒或防護程式的新電腦，最容易成爲攻擊之標的。據研究顯示，未設安全防護的電腦，被受入侵的時間已由以往之 40 分鐘縮短爲 20 分鐘，整整縮短了一半時間。

實務上，電腦製造商在新設備出廠時，其初始設定多將安全功能關閉。針對用戶存活期越來越短的趨勢，目前已有要求廠商在設備出廠時

即啓動安全設定的討論，但廠商態度仍有保留。

雖然目前刑法「妨害電腦使用罪章」已針對散佈病毒、製作惡性程式之行爲有所規範，但單以法律來防範網路駭客顯然是有所不足。網路安全的維護，相當程度仍須靠電腦使用者的注意。在使用上，於個人電腦加裝防毒軟體、並隨時更新病毒碼；不執行來路不明之軟體；套用較安全的模式來使用軟體；多注意電腦病毒之防制訊息；及裝設個人電腦防火牆或網路防火牆等，都可以保護自己電腦不致暴露於危害當中；另外在保密部份，不要輕易的洩露自己的密碼，並隨時更新密碼、提高密碼的複雜度、時時更新系統軟體及使用保密軟體等，都可以讓自己的電腦資料免於被偷竊。

4. 以牙還牙正當性

資料來源：2005.02.03.中國時報

事件：網路廖添丁 誤觸法網

事件描述：

高市刑大破獲一宗「騙中騙案」，以阿志爲首的詐騙集團，利用網路轉帳功能「詐騙」詐騙集團，在得款後，自稱還將部份金額幫助遊民及老人，並自詡是「義賊」。據了解，阿志因曾遭詐騙，對詐騙集團痛恨至極，於是開始吸收身邊需要錢的人及流浪漢，代辦銀行人頭帳戶，再向網路銀行申辦轉帳，然後透過報紙廣告將該人頭帳戶的「誘餌」賣給一般詐騙集團，造成其他詐騙集團損失慘重。

法律意見：

本案實屬特殊之案例，案例中阿志因不滿遭受詐騙集團之詐騙，又聽說住家附近有一殘障戶也被詐騙集團騙了五萬元，所以他對詐騙集團深惡痛絕，發誓一定要報復討回來。因工作之緣故接觸到網路銀行方面的業務，尤其是「轉帳」。透過網路銀行的漏洞，對詐騙集團實施「反詐騙」之行動。

本案行爲人利用人頭帳戶網路轉帳詐騙之行爲，已觸犯刑法第 339-3 條之電腦詐欺罪，若其犯罪所得達新臺幣 1 億元以上，則另觸犯銀行法第 125-3 條，意圖爲自己或第三人不法之所有，以詐術使銀行將銀行或第三人之財物交付，或以不正方法將虛僞資料或不正指令輸入銀行電腦或其相關設備，製作財產權之得喪、變更紀錄而取得他人財產，得處 3 年以上 10 年以下有期徒刑，併科新臺幣 1000 萬元以上 2 億元以下罰金。

案例中阿志透過自力救濟的方式，對犯罪集團實行「反詐騙」，並將獲取之利益，分送給有需要之民眾，在現今法治社會中並不接受。要討回公道，仍須遵循法律規定，故阿志之行爲仍須遭受到法律的制裁。

爲防制詐騙集團常透過人頭帳戶轉帳，詐騙民眾金錢，立法院已於 2005 年 5 月 4 日通過銀行法修正案，增列「人頭帳戶處理條款」（第 45-2 條），明定銀行對存款戶應負善良第三人管理責任，並賦予銀行對疑似不法或顯屬異常交易之存款帳戶，得予暫停存入或提領、匯出款項之權力。