編者序

不論是政府或是民間，我國對於資訊化的推動近年來可說是斐然有成。以網際網路而言，依據瑞士世界經濟論壇公布的 2002 年至 2003 年「全球資訊科技報告」指出，我國網路整備度排名全球第 9，其中「政府整備度」與「政府使用度」更分別高居全球第 2 及第 4 位。隨著數位台灣計劃的持續推動，e 化的腳步仍將不斷向前邁進。

在快速成長之際，部份資訊通信網路因安全整備不足而遭他人侵害的事實也時有所聞，例如透過電腦病毒破壞電腦及網路系統的正常運作、駭客入侵他人電腦從事不法行為、以及利用網路為犯罪工具或場所等行為。由於網路應用範圍逐漸廣泛，類似的糾紛隨著數位匯流在各個領域發生的可能性，值得全民加以重視。由於體認到整備資通安全環境的重要性，政府正對現有法制積極從事改革。立法院於今（民國 92）年 6 月 3 日三讀通過刑法關於電腦及網路犯罪的增修條文，即為一例。

資通安全觀念的推展，重點在於建立全民對於共同協助減低資通安全事件的發生，及對於在妨害資通安全秩序法律責任的認知基礎。為維護資訊通信環境的安全，並且讓社會大眾對於資通安全法制有基本的認識，這裡特別選

資通安全法律案例宣導彙編

擇了 20 個案例供各界參考。這些案例，有的是採自司法實務上曾經處理過的案件，有的則是摘取自近年來受到新聞媒體矚目的事件。誠摯希望這本配合最近刑法對於電腦及網路犯罪的增修規定的手冊，能藉由生活化的實例與精要的解說，對建立國民正確的資通安全法制觀念有所助益。

行政院國家資通安全會報技術服務中心　謹誌

目錄

資通安全法律案例宣導彙編

一、電腦病毒的威脅

電腦病毒對於資通安全秩序所造成的傷害，自數年前於我國發生大學生製作並散佈 CIH 病毒，導致世界各國電腦系統因而受損的事件開始，已逐漸引起社會各界重視。電腦病毒的製作，屬於高科技的「智慧型」犯罪，以下介紹兩則實例，分別由法律面及事實面提供讀者相關因應方式的參考。

資料來源：2002 年 10 月 4 日中國時報社會綜合版

事件：「熊熊」病毒肆虐

事件描述：

2002 年 10 月，「熊熊」病毒（BugBear.B）在歐美地區造成數百萬台電腦中毒。這個被美國國土安全局(Department of Homeland security)列為高危險性的病毒，除了會透過電子郵件散播外，還會自動啟動印表機亂印程式碼，甚至關閉電腦中的防毒軟體，即使電腦已經中毒，掃毒程式也會產生「正常」的回報訊息。更讓人防不勝防的是，病毒中內含木馬程式，可讓駭客從遠端截取密碼及其他包括信用卡資料等的機密資料。

法律意見：

「熊熊」病毒在我國雖未傳出重大災情，但由於「熊熊」的攻擊手法，綜合了目前已知的各類病毒行為特徵，此類混合型病毒撰寫的趨勢，讓網路環境倍增威脅。以我國現行刑法而言，相關條文對於散布病毒的過失犯並無處罰規定，仍限於故意的情形才會受到刑法的處罰，且須視散播者的目的為何，適用不同規範。以上述案例而言，故意散布熊熊病毒者，其散布的行為可能構成刑法第 360 條干擾他人處理電磁紀錄罪；利用內含的木馬程式截取他人

機密資料的行為，可能構成刑法第 359 條無故取得電磁紀錄罪，以及刑法第 318 條之 1、之 2 的利用電腦妨害秘密罪。相關行為視個案情況，最高可以處 5 年有期徒刑。

資料來源：2003 年 1 月 27 日中國時報社會綜合版

事件：軟體缺陷讓「監牢」病毒有機可乘

事件描述：

一隻攻擊威力與「紅色警戒」病毒相較之下有過之而無不及的監牢電腦病毒（Slammer），看準微軟公司的軟體漏洞，攻擊微軟關連式資料庫伺服器(SQL Server 2000)。此病毒除了會自行對外建立連線，產生一傳十、十傳百的效應外，部分遭 SQL Slammer 病毒感染的主機會瞬間產生將近巨量的攻擊封包，造成企業網路壅塞甚至中斷。

綜合國內外新聞報導，「監牢」病毒造成美國、加拿大銀行超過 13000 部提款機無法正常提供提領服務；韓國與台灣數家電信業者、線上遊戲服務業者的服務幾乎癱瘓，並造成亞洲股市一陣緊張。

法律意見：

為了逃避掃毒程式的檢查，利用系統安全漏洞的混合型病毒不斷改變其行為模式。多樣、複合式的繁殖方式與寬頻環境，讓此類惡性程式其得以迅速的擴散；而日常生活中各類基礎建設對電腦網路的倚賴增加，更使此類資安事故的影響層面日益擴大。根據 2002 年某網際網路安全防護公司發表的一份調查報告，2002 年下半年的企業電腦病

毒與駭客攻擊活動，已較前年同期激增五成。其中，電腦軟體瑕疵與企業網路漏洞激增，是促成攻擊活動日益活躍的主因；而遭到攻擊頻率最高的兩個產業，為電力能源業與金融服務業。

由於監牢病毒具有利用系統漏洞入侵電腦，再讓受害電腦系統發出大量封包壅塞網路、阻斷正常服務之特性。若依我國新修正之刑法條文，前段入侵行為可能成立第 358 條的入侵電腦系統罪，而後段行為可能成立第 360 條的干擾他人處理電磁紀錄罪；本病毒可被認定屬於專供犯罪之惡性程式無疑。且由於此病毒已造成社會上巨大的經濟財產損失，製作本程式者將可能成立第 362 條的製作專供犯罪之電腦程式罪，最高可處 5 年以下有期徒刑。本條規定為此次修法新增，且刑度甚重，目的即在遏阻惡性程式的撰寫。

軟體缺陷對資安的威脅不容小覷。系統軟體設計業者雖多已將「安全」作為設計應用的最優先考量，然而目前仍以系統管理者即時下載修補程式為此類資安事故主要的因應方式。我政府與資安業者也開始合作，由國家資通安全會報技術服務中心不定期發布相關新聞、提供教育訓練與技術支援，提醒各界重視網路安全的重要性。

二、電腦駭客的威脅

一般人經常從大眾傳播媒體上看到駭客這個名詞，但是大多數人對於駭客行為在法律上需負的責任為何可能並不了解。駭客的行為方式，雖可說是變化多端，就法律的觀點，大體上可區分為「癱瘓服務」與「入侵」兩大類。以下將介紹 9 則案例，具體說明不同型態的駭客行為責任。

1.癱瘓服務式犯罪

資料來源：2002 年 10 月 24 日中國時報社會綜合版

事件：駭客入侵根伺服器

事件描述：

被形容為網際網路問世以來手法最先進、規模最大的分散式阻斷服務攻擊（DDOS），發生在美東時間 2002 年 10 月 21 日下午 5 時（台灣時間 22 日上午 5 時）。全球 13 個管理網際網路網址系統的根伺服器遭到阻斷服務攻擊，導致其中 9 台暫時癱瘓，雖未造成重大災情，但聯邦調查局與白宮已著手調查始末。

法律意見：

網際網路上的網址如同電腦的門牌，也是電腦與電腦之間聯繫與辨識的線索，使用者上網輸入網址後，必須由根伺服器指導電腦如何到達其他網址或位址，少了它們，網路瀏覽者將無法順利進行連線。而 DDOS 攻擊，即為利用大量且分散的使用者佔用系統共用資源，造成服務阻斷之結果。

駭客利用 DDOS 攻擊，足以生所損害於公眾或他人時，依我國現行刑法，將構成第 360 條之「干擾他人電磁紀錄

處理」罪，最高可處 3 年以下有期徒刑。

資料來源：2002 年 1 月 10 日中國時報社會綜合版

事件：駭客組織「借道」我國網站進行跳板攻擊

事件描述：

美國 911 事件發生後，刑事局即接獲美國 FBI 的通報，要求我方協助調查中東國家駭客疑透過我國電腦，攻擊美國本土重要機構電腦設備。刑事局偵九隊在調查後發現，一個中東親「基地」的駭客組織「GFORCE」，成功入侵我國某 ISP 業者主機，再以跳板方式入侵美國本土電腦。刑事局將相關資料與偵查結果知會美方，建立雙方共同打擊電腦犯罪良好合作模式。

法律意見：

由於網路特殊的匿名性與可遠端遙控性，資料封包的來源位址(source IP)成為網路攻擊事件追緝的重要線索，也因此駭客會無所不用其極地利用不實的 IP 來抹去行跡。施放後門程式，利用不知情的網站跳板攻擊來誤導執法人員的追查方向，遂成為網路攻擊行為模式中常見的型態之一。而國內一些頻寬大、使用少、服務多、安全低的電腦主機，正好給予國際駭客可趁之機。

對於這類跳板攻擊事件，由於被當作跳板之網站本身也是被害者，且在無故意之情況下，現階段通說皆不以為

有任何法律責任。為防範網路犯罪，各國均有修正法制，加重網站管理者責任的趨勢。因此，已有部分美國學者主張，若被當作跳板之網站可被認定具有一定維護社會安全的注意義務時，可以成立民事賠償責任。惟此論點，仍待法院案例之支持。

無論如何，跳板網站攻擊事件也點出網路安全管理的重要性。不論是電腦使用者或電腦管理者，均應提高對電腦安全維護的警覺性，加強對電腦安全的認知，隨時注意下載更新各種系統漏洞修補程式，避免因為管理不善或疏失，淪為駭客攻擊的幫兇，遭到受害國家的抨擊與批評，害人又害己。

2.入侵型犯罪

資料來源：2003 年 5 月 19 日中央社

事件：北韓每年培訓百名駭客

事件描述：

根據南韓軍方情報當局透露，北韓每年訓練培養 100 名電腦專才，以提升北韓在虛擬空間的恐怖活動能力，南韓國防官員因此強調，必須加強電腦虛擬空間的備戰能力，方能遏制平壤當局的駭客任務。若他國駭客攻擊我國的網路基礎設施，我國法制應如何規範。

法律意見：

資訊科技於國家安全領域扮演的角色日益重要。除了各國政府積極研究以資訊科技提升整體軍事戰力外，恐怖組織或團體也紛紛以網路作為另一個遂行恐怖主義的戰場，以收攻敵於不備之效。有感於此，美伊戰爭時，布希總統下令擬定網路作戰計畫，高度防範恐怖集團利用網路攻擊美國國家基礎設施。易言之，網路時代的資訊安全不只關乎個人利益，更涉及社會秩序與國家安全。

依據我國刑法第 5 條到第 8 條，外國人，即使在我國領域外，若觸犯我國刑法內亂罪、外患罪章內的各項罪名，

以及其他最輕本刑 3 年以上有期徒刑之罪，且犯罪地的法律有處罰規定者，都可以適用我國刑法加以處罰。因此，他國駭客的行為若對我國造成侵害，我國仍得視情況對其主張管轄權。

而我國人民如因參與或幫助而涉入其中，則為共同正犯或幫助犯；若其具有公務員身份，並假借職務上之權力、機會或方法協助犯案時，更可依刑法第 134 條規定，加重其刑至二分之一。相關罪名涉及國家安全，刑責甚重，民眾不可不慎。

資料來源：2003 年 5 月 19 日中國時報政治新聞版

事件：疑似大陸駭客入侵我國政府網站

事件描述：

行政院國家資通安全會報從 4 月底至 5 月 20 日前，一連接獲 7 起政府網站遭駭客入侵，或因電腦系統感染病毒而受損的資安事件通報。部分攻擊手法與大陸駭客網站之前策劃的某攻擊行動類似，但因駭客大都以第三國為跳板對台灣發動攻擊，逃避我方以位址 IP 追查攻擊源頭，資安單位無法百分之百肯定攻擊者來自對岸。

法律意見：

資安事件的法律責任，可以分兩個部分論之。其一，是駭客行為對電腦系統安全性的破壞。此部分根據新修正的刑法「妨害電腦使用」罪章，若行為人係以公務機關之電腦作為攻擊對象，進行入侵或干擾設備使用之行為時，將各依其行為態樣之罪責，根據第 361 條加重其刑至二分之一。

此外，建立資安防護機制的重要目的，在維護電腦設備內所儲存資料之安全性、機密性與完整性。若入侵行為對系統內的資料有進一步之行為時，將視其情節，可能構成刑法第 111 條刺探國防秘密罪、第 138 條毀損或隱匿公

務員職務上掌管文書罪、第 211 條偽造或變造公文書罪、第 359 條無故取得電磁紀錄罪、或第 360 條干擾他人電磁紀錄處理罪等等。若攻擊者為大陸駭客，我國刑法不但有管轄權，且依台灣地區與大陸地區人民關係條例第 75 條規定，在大陸地區犯罪者，雖在大陸地區曾受處罰，仍得依法處斷。

資料來源：2002 年 9 月 18 日工商時報焦點新聞版

事件：財金公司資訊外洩案

事件描述：

財金公司員工涉嫌販售消費者信用卡資料資料約 6 萬多筆，可能影響消費者 170 萬張信用卡。由於資料外洩的期間可能長達 1 年，直到 2002 年 9 月間才被發現，引發消費者憂慮。相關新聞並被消基會評選為 91 年度十大消費新聞之第 9 名。

法律意見：

財金公司員工洩密案，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」）。

上述出賣個人資料之行為，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 年以下有期徒刑、拘役或科新臺幣 5 萬元以下罰金。

此外，根據個資法第 17 條與第 26 條規定，公務機關、非公務機關對於保有個人資料檔案者，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」的義務。若民眾的個人資料外洩是因

該機關安全控管不當，致其權益受損害時，被害民眾得依個資法第 30 條規定向該機關請求損害賠償。

總而言之，為了防範資安事件，各金融機構莫不以高標準的軟硬體設備來建構安全的網路環境。然而，所謂家賊難防，面對高科技金融犯罪的猖獗，金融界實應更加重視對內部人員的安全控管。否則，小則侵害客戶隱私權，大則影響交易金融秩序及信心，其影響層面將難以估算。

資料來源：2002 年 5 月 17 日 91 年度上訴字第 689 號判決

事件：電信公司員工入侵機房盜用電信牟利

事件描述：

某甲任職於某電信公司，其工作內容是為公司處理有關客戶無法收發話等技術障礙問題，因此得以隨時進入交換機系統更改客戶資料以解決客戶問題。但甲竟趁職務上的機會，進入公司話務與帳務系統，利用話務系統及帳務系統間漏洞，使其所使用的門號電磁紀錄受干擾而未予計費，並以此方式多次為自己及其家人牟取不法利益。

法律意見：

某甲的行為已觸犯刑法第 360 條干擾他人電磁紀錄處理罪，以及電信法第 56 條第 1 項以電磁方式違法盜接電信設備罪，最高可處 5 年以下有期徒刑。

本案彰顯了企業資安維護的重點，在人員的管理與密碼的保護。甲任職之電信公司雖然有依相關規定，對員工使用系統的權限進行區分，卻由於對人員的安全控管和密碼保護不周，致使甲有機可乘，進而入侵系統得逞。由此可知對人員的安全控管實在是資安防護工作最重要的一環。

資料來源：2003 年 2 月 13 日中時晚報焦點新聞版

事件：大學講師扮駭客

事件描述：

某甲曾為與軟體公司合作開發程式之工程師，後擔任某大學講師。自 2002 年 9 月起，該公司開發的遠距教學電腦系統持續遭入侵，資料並被毀損刪除，造成公司無法正常營運，專業形象受質疑，損失達約 1000 萬元。經警方追查後發現是某甲所為。

法律意見：

針對目前發現的入侵型犯罪，警方發現大多源於熟知內部電腦系統運作細節的資訊人員，而這些資訊人員一旦產生危害，往往比外來的駭客更切中要害。相關企業機構主管，實需要多加注意內部人員與合作伙伴的忠誠與溝通問題。以上述事件而言，根據新修正的刑法，甲已觸犯第 358 條無故入侵他人電腦罪及第 359 條刪除他人電磁紀錄罪，最高可處 5 年有期徒刑。並應依民法負侵權行為損害賠償責任。

資料來源：2003 年 3 月 25 日 92 年度上訴字第 133 號判決

事件：離職員工入侵公司郵件伺服器

事件描述：

某甲曾在 A 公司擔任業務部經理一職，因職務關係而知悉 A 公司所設置使用的數個電子郵件信箱密碼。甲於離職後，利用 A 公司郵件伺服器，將他人寄給 A 公司的電子郵件，偽造為內容足以毀損他人名譽的郵件，再冒用 A 公司名義寄發給客戶。A 公司因客戶反應，始發覺報警處理。

法律意見：

甲明知電子郵件帳號是作為網際網路上表明郵件使用者名義之用，竟冒用足以表彰 A 公司名義之電子郵件帳號，偽造電子郵件之內容後，再將偽造之電子郵件寄給他人，已觸犯犯刑法第 210 條之偽造私文書罪，及第 216 條的行使偽造私文書罪。而涉嫌誹謗之部份，實已觸犯刑法第 310 條第 2 項的誹謗罪。須注意者是，在刑法增訂妨害電腦使用罪章後，甲的行為更將違反第 358 條無故入侵他人電腦罪。綜而言之，對甲最高可處 5 年有期徒刑。

本案充分反應出企業對離職人員安全控管的重要性。當員工因衝突而離職時，容易產生報復之心態。此時，公司平日若已做好資料分級機制，避免讓職級不夠的員工接

觸到過多的資訊，對郵件伺服器之連線密碼設定與安全管控亦能即時反應人事變動之情形時，則應能有效降低員工對公司報復舉動的影響性。而當具有影響力之員工離職時，企業更應做好一定的安全機制，以避免損及公司利益。

資料來源：2002 年 5 月 3 日 91 年度易字第 8 號判決

事件：好友入侵竄改密碼

事件描述：

G 與 W 是某工業專科學校同學及室友，因曾一同使用電腦上網，使 G 得知 W 登錄使用之網路電子郵件帳號及密碼。由於 G 認為 W 在網路上散布其為同性戀之言論，心生不滿，便在住處使用撥接帳號上網，進入 W 在某大學的電子佈告欄、以及某網站經營業者的網路帳號，將 W 在上述網路登錄使用的原密碼 xxx 竄改為 ooo，以致 W 以原網路密碼無法進入相關網站，經 W 報案後，警方循線偵知上情。

法律意見：

根據新修正之刑法，G 未經過 W 授權，擅自利用網際網路進入 W 帳戶之行為，可能成立刑法第 358 條之入侵電腦系統罪；而其進一步竄改 W 登錄密碼，致使 W 以原網路密碼無法進入相關網站，則可能成立第 359 條變更他人電磁紀錄罪。由於前述各罪屬告訴乃論，W 可在發現上述情事後，就 G 之行為造成之損害提起告訴。

三、其他電腦犯罪之威脅

資通安全的維護，除了須防止病毒及駭客破壞電腦及網路系統本身的正常運作之外，更包含建立健全資通環境在內。為達成此目標，有必要提供參與網路環境者對於安全事項的行為規範。然而由於行為型態與法律種類繁多，此處僅以 9 個實例，對常見的重要犯罪類型加以介紹。

1.妨害電信秩序

資料來源：2001 年 11 月 20 日 90 年訴字第 1083 號判決

事件：以他人名義申辦行動電話儲值卡

事件描述：

某甲於購買 A 電信公司的儲值卡後，因儲值卡須向 A 公司客戶服務中心登錄使用者個人資料後，才能繼續通話使用，甲不願留下自己資料，在撥打客服專線時，利用不知情的 A 公司客服人員，將某乙個人資料輸入該公司電腦系統處理並存檔。經乙報案指稱遭人冒名，才循線破案。

法律意見：

所謂「電磁紀錄」，依據刑法第 220 條第 3 項規定，是指以電子、磁性或其他無法以人之知覺直接認識之方式所製成之紀錄，而供電腦處理之用者。甲未經乙授權同意，而以電話利用不知情之 A 公司客服人員將乙的個人資料輸入該公司電腦系統處理並存檔為電磁紀錄，實已觸犯刑法第 210 條之偽造準私文書罪。

資料來源：2001 年 3 月 28 日 90 年台上字第 1802 號判決

事件：盜拷他人行動電話內碼

事件描述：

T 先生為了盜拷行動電話使用，在收受他人盜拷自某立法委員所有號碼行動電話機一支後，委由不知情之通信行，以盜拷方式製造行動電話機供自用。在持有前開盜拷的行動電話機後，更利用該行動電話，連續多次在不特定處所，以無線方式盜用該立法委員承租的行動電話號碼對外通信，而免繳行動電話通信費用。

法律分析：

行動電話手機（話機）之電子序號及內碼等，是手機製造廠商及行動電話通信業者有權自行製作或授權他人製作，將之輸錄於行動電話手機的電腦電磁紀錄內，供行動電話通信業者的電腦網路交換控制中心比對查核，以決定是否准許該手機使用者通信之用，屬於刑法第 220 條第 2 項的準私文書。行為人明知行動電話手機的電子序號及內碼是盜拷(偽造)自他人行動電話的序號、內碼，為圖自己或第三人不法利益，持以使用，除犯電信法第 56 條第 1 項之罪外，尚成立刑法第 210 條偽造準私文書罪及第 216 條的行使偽造準私文書罪。

2.個人資料外洩

資料來源：2002 年 10 月 21 日中國時報焦點新聞版

事件：刑事局警官涉盜賣通聯紀錄

事件描述：

任職刑事局 A 警官，涉嫌與民間徵信社業者掛勾，連續利用本身職權，取得民間電信公司客戶電話通聯資料，再交給徵信業者，換取鉅額酬勞。據估計，經由 A 警官之手流向徵信社業者的電話通聯資料多達數百筆。

法律意見：

電信公司客戶通聯資料，屬於電腦處理個人資料保護法（以下簡稱「個資法」）所保障的個人資料。依個資法第 3 條第 7 款規定，電信業應受拘束。因此，在前述案例，該電信公司將客戶資料無故洩漏給 A 警官，可能須依個資法第 28 條，對權益受損害者負損害賠償責任。至於 A 警官與徵信業者，則可能成立個資法第 33 條「非法輸出、干擾、變更、刪除、妨害正確罪」之共同正犯；又因 A 具有公務員身分，應依個資法第 35 條，加重其刑至二分之一。

資料來源：2003 年 3 月 14 日中國時報社會綜合版

事件：電信資料外洩引發騷擾

事件描述：

在某電信公司任職的某 A，以自己的名義申請手機門號後，供親友使用。但其親友不慎與人結怨，對方（某 B）透過管道追查其親友使用之手機號碼，誤認 A 為該名親友，除駕車跟監，作勢衝撞以為警告外，更在其住處外擲石騷擾，讓 A 精神受到莫大威脅。A 利用其上班場所的電腦系統回查其名下手機門號的被查詢記錄，始查出本案係其個人電信資料被該公司內部員工 C 不當外洩所致。

法律意見：

電信業須受電腦處理個人資料保護法（以下簡稱「個資法」）規範。依個資法第 18 條及第 23 條意旨，未經當事人同意，原則上不得從事特定目的外之利用。C 不當將資料外洩的行為，可能違反個資法第 33 條及第 34 條而須受刑事制裁，且須依民法相關規定對 A 負侵權行為損害賠償責任。

B 除了可能成為 C 之教唆犯或共同正犯，與 C 就民事賠償連帶負責之外，尚觸犯刑法第 305 條恐嚇罪等罪名。至於 C 所屬之電信公司，除須就受僱人 C 之侵權行為連帶

負責之外，依個資法第 38 條規定，目的事業主管機關更得對公司負責人科以罰鍰。

3.妨害秘密

資料來源：2001 年 12 月 31 日 90 年度上易字第 4014 號判決；2002 年 8 月 21 日 91 年度上易字第 1945 號判決

事件：離職員工刪除電腦檔案

事件描述：

案例 1：某公司業務經理甲，因職務關係持有公司所有之「相關客戶往來文件及儲存於電腦內之檔案資料」。因故離職後，被公司控告不當清除電腦檔案資料。被告甲否認犯行並辯稱，公司並無規定使用電腦後均應存檔，而甲使用電腦的習慣是列印後並不存檔；相關書面資料更在離職前全部辦理移交完畢。公司所舉證人所言都只是推測之詞云云。甲最後獲判無罪。

案例 2：乙在某科技公司上班，負責電腦設計繪圖。在離職前乙不聽同仁勸阻，將任職公司期間所繪製之設計圖電腦圖檔從電腦中刪除，並在交接時拒絕交出儲存在電腦裡的設計圖軟體部分，且不為示範操作。乙被控觸犯刑法第 352 條第 1 項之毀損文書罪成立。

法律意見：

前述案例中，被告甲獲判無罪，乙則獲判有罪。兩者

的差異，除了乙任職的公司能充分舉證，證明乙有刪除相關圖檔、電磁紀錄的行為外，公司對員工使用電腦的行為是否有明確的作業規範、有否定期對員工電腦中的資料進行備份等，是兩案判決差異的關鍵。

在案例 1 中，因為甲任職的公司並無規定員工應就所有相關資料存檔，亦無定期將員工電腦內資料備份的習慣，因此無從證明甲離職當時，其電腦中究竟有何資料，致法官無從認定甲是否如公司指控，有積極毀損、干擾公司電磁紀錄之行為。因此採信甲「無將資料儲存習慣」之辯詞。

而在案例 2 中，由於乙負責業務即是電腦繪圖。根據刑法第 220 條第 2 項，電磁紀錄為準私文書之一種。則電腦圖檔在遭刪除時，因足生損害於乙任職之公司，因此其刪除行為即觸犯刑法第 352 條第 1 項之毀損文書罪。

資料來源：2002 年 9 月 10 日中時晚報政治新聞版

事件：調查局調查員疑似洩密

事件描述：

調查局某調查員涉嫌將調查局內部對於法輪功部分報告內容，透過電腦網路傳送到大陸，後經法務部考績會決議記 2 大過免職。

法律意見：

國家之機密資料，事涉公共利益與民眾安全，關係重大，其處理應依法定程序為之。因此我國特於 2003 年 2 月 6 日制定「國家機密保護法」，其中第 32 條以下對於洩密之處罰設有明確規定，其行為型態可大抵分為「刺探或收集機密」、「洩漏或交付機密」及「毀損或隱匿機密」三大類型。爾後若出現類似上開案例之洩漏國家機密行為，將違反國家機密保護法之相關規定，最高可處以 7 年有期徒刑。

4.網路詐騙

資料來源：2001 年 4 月 18 日 89 年訴字第 928 號判決

事件：線上購物詐欺

事件描述：

甲藉著在西餐廳擔任服務生的機會，私自抄錄顧客的信用卡卡號及有效期間等資料。在取得上述資料後，自各網咖連線到不同的購物網站，以他人名義輸入虛偽身分證字號及上述信用卡卡號及有效期間等資料以訂購物品，甲並偽刻印章，通知業者將訂購貨物交付至連線上網購物的網咖後，請不知情之店員協助領取。並在其他購物網站轉售贓物。

法律意見：

本案中，甲為訂購所作成的電磁紀錄及蓋有印文或簽有署名之出貨單，具有訂購單及收據的性質，屬於準私文書，因此已觸犯刑法第 210 條及第 216 條的行使偽造準私文書罪。至於上網詐取物品部分，則構成刑法第 339 條及第 340 條的詐欺罪。由於甲以連續犯意屢次犯罪，應依常業詐欺罪及連續行使偽造準私文書罪論處。

資料來源：2002 年 12 月 5 日 91 年台上字第 6909 號判決

事件：翻印正版說明供盜版物販賣案

事件描述：

經營電視遊樂器販賣之業者 L，基於概括之犯意，以低價購入仿冒任 X 堂公司所產製之電視遊樂器含燒錄電腦程式之「ＧＡＭＥＢＯＹ」、「超級任 X 堂遊戲」卡匣等物，且翻印正版說明黏貼其上，在所開設之電視遊樂器店內出售予不特定之人，以牟取利益。

法律意見：

前述案例，若從刑法角度觀之，電腦遊戲程式在性質上屬於刑法第 220 條第 2 項之準文書，偽造之行為人實構成第 210 條之偽造準私文書罪。因販賣而交付該盜版程式的情形，如販賣交付者與買受收受者，均明知其確為偽造，且均明知藉由機器或電腦處理即可使用該偽造程式時，因買受者已達於可隨時使用該程式之狀態，故販賣該偽造準文書者於交付時，即已構成第 216 條行使偽造準文書罪。

本實務判決中雖未提及，然本案另可依商標法論責。如 L 翻印正版說明之行為，可能構成商標法第 62 條侵害他人商標專用權；販賣、陳列仿冒物之行為，則觸犯第 63 條販賣仿冒商品罪。依商標法第 64 條，所有商品不問屬於犯

人與否，沒收之；而依第 67 條規定，L 更應與仿冒者負連帶損害賠償責任。

資料來源：2002 年 12 月 26 日台北地方法院 91 年訴緝字第 157 號判決

事件：偽造信用卡消費

事實描述：

某甲利用向他人購買盜錄得來的信用卡資料（即內碼）、卡號、持卡人姓名及使用期限等程式資料、燒錄軟體，及空白信用卡，用自備的筆記型電腦、燒錄機、燒錄光碟片，連續多次將內碼等程式輸入電腦，再以燒錄機將卡號等資料燒錄至空白信用卡，偽造了共計 50 餘張信用卡。並連續在臺北縣、市或日本等地之商店，刷卡偽造真正持卡人簽名消費。

法律分析：

科技技術的進步，讓金融偽造行為更加容易。根據現行刑法增訂第 201 條之 1 第 1 項：意圖供行使之用而偽造信用卡者，處 1 年以上 7 年以下有期徒刑，得併科 3 萬元以下罰金。同條第 2 項：行使前項偽造之信用卡者，處 5 年以下有期徒刑，得併科 3 萬元以下罰金，同法第 205 條並增加偽造之信用卡，不問屬於犯人與否均沒收等規定。被告行為時，若是在上開條文增訂之前，當時行使偽造信用卡的罪名通常以偽造私文書罪之型態呈現，修正後的獨

立罪名雖性質上屬於偽造有價證券罪，而與偽造私文書罪名不同，但新舊法均認定行使偽造信用卡有罪，則無疑問。