淡江大學高階主管資安講習
— 個資法通過後的資訊安全挑戰

電子化巨架構事業單位（Acer eDC）
宏碁公司 電子化服務事業群

副總經理 張 善 政
2010.6.18

一、引言：
個資洩漏不是只有台灣在頭痛

AT&T 也會被駭 (I)

- ☑ **2006.9.1 AT&T發佈消息**
  - Hackers accessed personal data, including credit card information, from several thousand customers who purchased DSL equipments through online Web store.
  - AT&T technicians discovered the security breach “within hours.” The online DSL store was immediately shut down.
  - AT&T quickly notified major credit card companies and is working with law enforcement to investigate the incident and pursue the perpetrators.
  - Individual customers were notified by (real) e-mail about the full scope of the scam

AT&T 也會被駭 (II)

- ☑ **AT&T 隱瞞的內容**
  - The stolen info of 19,000 customers was immediately put to use as part of an unusual deceptive phishing scam
  - The security breach occurred at an AT&T vendor that operates an order processing computer for the online DSL store
  - Stolen information included: name, address, e-mail, phone no., credit card no. and card expiration date
- ☑ **Phishing 作法**
  - 給客戶的 e-mail: we recently tried to charge your credit card for your SBCdslstore.com order and it was rejected by the bank because it has no complete information.
  - e-mail 中也包括原始的 DSL 設備 order number、客戶地址與信用卡最後四碼，製造真實來源的假象。
  - e-mail 又說: To update the credit card information details for your order, please select this link," the message instructed, directing people to a "spoof site" with an illegitimate sbcdslstore.org (not .com) Web address.

AT&T 又被駭了 (I)

- 2010.6.10: In what's being described as AT&T's worst security breach in recent history,
  - the wireless company went and left sensitive information on 114,067 owners of the iPad 3G exposed on the Web.
  - The subscriber data was obtained by a group calling itself Goatse Security, who then published the personal email addresses of the victims, including military officials, CEOs, prominent politicians, and celebrities.
- When provided with an ICC-ID as part of an HTTP request
  - the script (of AT&T web-site) would return the associated e-mail address, in what was apparently intended to be an AJAX-style response within a Web application.
  - The security researchers were able to guess a large swath of ICC IDs by looking at known iPad 3G ICC IDs, some of which are shown in pictures posted by gadget enthusiasts to Flickr and other internet sites, and which can also be obtained through friendly associates who own iPads and are willing to share their information, available within the iPad "Settings" application.

AT&T 又被駭了 (II)

- To make AT&T's servers respond,
  - the security group merely had to send an iPad-style "User agent" header in their Web request. Such header identify users' browser types to websites.
- AT&T, which has confirmed the breach, insists that
  - only email addresses were lifted, and that more sensitive data like credit cards and home addresses were not compromised.
- Famous users:
  - New York Mayor Michael Bloomberg,
  - anchorwoman Diane Sawyer of ABC News,
  - New York Times CEO Janet Robinson,
  - Col. William Eldredge, commander of the 28th Operations Group at Ellsworth Air Force Base in South Dakota

二、案例影片
（from YouTube）

三、個資法概要

個資保護八原則

- ☑ **OECD 1980之「隱私保護暨個人資料跨境流通指導綱要」**
  - 限制蒐集原則（Collection Limitation Principle）
  - 目的明確化原則（Purpose Specification Principle）
  - 資料內容完整正確原則（Data Quality Principle）
  - 限制利用原則（Use Limitation Principle ）
  - 個人參加原則（Individual Participation Principle）
  - 公開原則（Openness Principle）
  - 安全保護原則（Security Safeguards Principle）
  - 責任之原則（Accountability Principle）

個人資料保護法源起與發展

- ☑ 「電腦處理個人資料保護法」於民國 84 年 8 月 11 日公布施行
  - 保護對象僅限於「經電腦處理」之個人資料，其他人工資料不適用
  - 基於同一原因事實之侵權行為，最高損害賠償總額限新台幣二千萬
  - 適用對象僅限徵信業、醫院、學校、電信、金融、證券、保險、大眾傳播業等「八大行業」

- ☑ 法務部於民國九十年研擬「個人資料保護法」
  - 行政院會於 93 年 9 月審查通過「個人資料保護法草案」
  - 99 年 4 月 27 日正式立法，取代「電腦處理個人資料保護法」

個人資料保護法－範圍擴大

- ☑ 擴大適用行業
  - 原適用八大行業（徵信、醫院、學校、電信、金融、證券、保險及傳播業）
  - 適用範圍擴大至公務機關（含行政法人）與公務機關外的自然人、法人或其他團體
- ☑ 個資新定義與科技演進結合
  - 原個資定義：姓名、生日、身份證字號、特徵、指紋、婚姻、職業等
  - 增加了護照號碼、犯罪前科、聯絡方式，並原病歷擴大為需考量醫療、基因、性生活、健康檢查等
- ☑ 調整資料儲存型式
  - 原有對儲存於電磁紀錄物或其他類似媒體
  - 調整為以自動化機器或非自動化個人資料之集合

個人資料保護法
－加強個資保護及通報因應

- ☑ 加強個資保護
  - 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。（第2章第18條）
  - 非公務機關保有個人資料檔案者，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。（第3章第27條）
- ☑ 個資外洩時主動告知當事人
  - 公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。（第1章第12條）

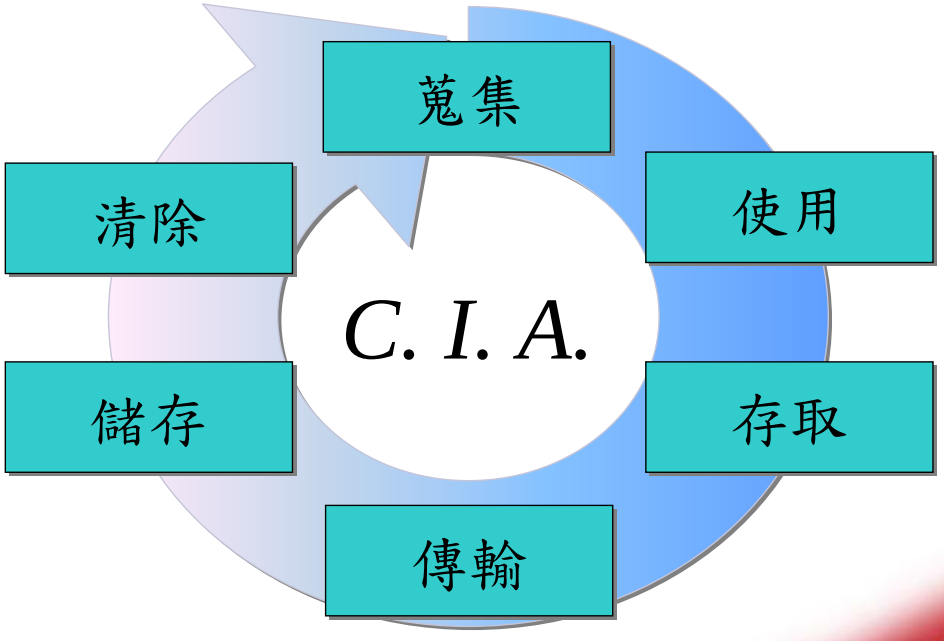
12

個人資料保護法
—提高賠償責任與罰則

- ☑ 提高賠償責任與罰則
- ☑ 於公務機關在非天災等不可抗力因素外，導致個資外洩而侵害當事人權益時，得依每人每一事件新台幣500元~20000元以下；若造成多數人權益受損時，則由2000萬調高至2億。（第4章第28條）
- ☑ 加重違反罰則
  - 違反時仍為處以二年以下有期徒刑、拘役並由原有的4萬元以下罰金增加為20萬（第5章第41條）；
  - 增加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5年以下有期徒刑、拘役或科或併科新臺幣100萬元以下罰金（第5章第42條）。

13

個人資料生命週期管理
（Personal Data Life Management）



個人資料管理重點 (I)

- ☑ 蒐集
  - 蒐集個人資料之理由、方法與告知義務
  - 確認個人資料之正確性及內容是否為法律定義之「得以直接或間接方式識別該個人之資料」
- ☑ 使用
  - 符合法律之使用規範
  - 符合組織政策之內部使用規範(例如：交叉行銷)
- ☑ 存取
  - 存取個人資料之權限管理
  - 委外或外包廠商之資訊安全管理

個人資料管理重點 (II)

- ☑ 傳輸
  - 個人資料傳輸過程中之安全（加密或安全網路）
- ☑ 儲存
  - 個人資料新增及修改之作業程序
  - 存放個人資料場所及設備之安全管理
  - 備份或歸檔後之資料安全
- ☑ 清除
  - 個人資料刪除或報廢之安全處理程序
- ☑ 其它
  - 客訴、法律糾紛、懲處程序

新版個資法重點彙整（1）

- ☑ 限制特種資料的蒐集
  - – 醫療、基因、性生活、健康檢查及犯罪前科等五類個人資料，原則上不得蒐集、處理或利用
  - – 除外條款
    - 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
    - 當事人自行公開或其他已合法公開之個人資料
    - 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，為統計或學術研究而有必要，且經一定程序

新版個資法重點彙整（2）

- ☑ 向當事人蒐集個人資料時應明確告知（有除外條款）
  - – 公務機關或非公務機關名稱
  - – 蒐集之目的
  - – 個人資料之類別
  - – 個人資料利用之期間、地區、對象及方式
  - – 當事人依第三條規定得行使之權利及方式
  - – 當事人得自由選擇提供個人資料時，不提供將對其權益之影響
- ☑ 公務機關或非公務機關蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知來源及前條所列事項
  - – 除外條款
    - 當事人自行公開或其他已合法公開之個人資料（例如：人肉搜索）
    - 不能向當事人或其法定代理人為告知
    - 基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限
    - 大眾傳播業者基於新聞報導之公益目的而蒐集個人資料

新版個資法重點彙整（3）

- ☑ 公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人
- ☑ 公務機關應公告或提供查閱
  - 個人資料檔案名稱
  - 保有機關名稱及聯絡方式
  - 個人資料檔案保有之依據及特定目的
  - 個人資料之類別
- ☑ 當事人之權利（不得預先拋棄或特約限制）
  - 查詢或請求閱覽
  - 請求製給複製本
  - 請求補充或更正
  - 請求停止蒐集、處理或利用
  - 請求刪除

新版個資法重點彙整（4）

- ☑ 個人資料之蒐集與處理
  - 需當事人書面同意
  - 非公務機關：與當事人有合約、與公共利益有關、取自於一般可得之來源（但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限）等
- ☑ 個人資料之利用應依據蒐集之目的與範圍（有除外條款）
  - 包括學術研究之必須、避免危及當事人生命財產等
- ☑ 非公務機關限制任意行銷
  - 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
  - 非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用

新版個資法重點彙整（5）

- ☑ 中央目的事業主管機關、直轄市或地方政府得強制檢查、處分或處罰
  - 認有必要或有違反本法規定之虞時，得派員檢查並要求相關人員說明、配合或提供資料
  - 檢查時可扣留或複製相關證據
  - 得率同資訊、電信或法律等專業人員共同進行
  - 非公務機關及其相關人員不得規避、妨礙或拒絕
  - 參與檢查之人員負保密義務
  - 除罰鍰外並得為下列處分：
    - 禁止蒐集、處理或利用個人資料
    - 命令刪除經處理之個人資料檔案
    - 沒入或要求銷燬違法蒐集之個人資料
    - 公布非公務機關之違法情形，及其姓名或名稱與負責人
- ☑ 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。前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之（可能研擬範本）

新版個資法重點彙整（6）

- ☑ 團體訴訟機制
  - 財團法人或公益社團法人
    - 財團法人之登記財產總額達新臺幣一千萬元或社團法人之社員人數達一百人
    - 章程範圍涵蓋保護個人資料事項
    - 許可設立三年以上
  - 由二十人以上受有損害之當事人授與訴訟實施權
- ☑ 責任及處罰
  - 違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任
  - 除外：公務機關因天災、事變或其他不可抗力所致者；**非公務機關能證明其無故意或過失者（舉證責任反置）**
  - 被害人不易或不能證明其實際損害額時，以每人每一事件新臺幣五百元以上二萬元以下計算
  - 同一原因事實造成多數當事人權利受侵害，合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限（需舉證）

新版個資法重點彙整（7）

- 違反本法足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。意圖營利者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金
- 因圖利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
- 公務員加重其刑 至二分之一
- 原則上為告訴乃論，但意圖營利及非法變更、刪除資料者為公訴罪
- 非公務機關之代表人或管理人，因該非公務機關違法受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰

☑ 過渡條款

- 立法前取得之個人資料，應於處理或利用前向當事人告知，自法律修正施行之日起一年內需完成

☑ 日出條款

- 本法施行日期，由行政院定之
- 據側面了解，可能實施日期為 100 年 6 月
  - 政府需研訂施行細則
  - 政府可能會研訂個人資料檔案安全維護計畫之範本

爭議條文修正與討論

中廣新聞 2010-04-28

☑ 立法院三讀通過個人資料保護法，其中最受矚目的就是網友人肉搜索受到限制；但在修正後，人肉搜索也變成合法，讓警方未來透過人肉搜索，有了法源依據。這也意味「全民警察」的時代即將來臨，數以百萬計的網友幫忙找人，效率十分驚人，警方也戲稱「這下子線民也愈來愈難混了」

☑ 事實上，最近網友人肉搜索屢建奇功，包括董氏基金會公佈三歲幼童抽煙喝酒影片、無腦妹破壞公物，以及惡阿嬤掌摑孫子事件，都透過網路人肉搜索，在短時間內找到人，效率之快和資料之詳盡，連警方的戶口課都自嘆不如

聯合報／陳長文　2010.04.29

☑ …至於何謂「公共利益」這個不確定法律概念，授權法務部訂定施行細則，將「公共利益」做更明確的劃分。筆者認為一方面，應將「公共利益」做最廣泛的定義，讓媒體的不安感降到最低。另一方面，個人資料的使用與公益的維護，應該要有手段與目的的連結性。當然，無論如何制定，法律仍不可能百分之百的明確，這時，還是要留待**法官依據個案裁量**，透過判決與判例累積，形成穩定的法律規範體系與判準

四、個資洩漏案例

洩漏管道：駭客攻擊

中國時報　2007/09/22

- 曾入侵總統府網站、被警方喻為電腦天才而主動吸收協助辦案的網路駭客蘇柏榕，又重蹈迷途復出犯案！這次他被黑幫吸收，夥同林姓少年各自以專精的電腦技巧，利用學術網站作為掩護，侵入中華電信公司等知名網站，非法取得多達上千萬筆的會員資料販售圖利。
- 林姓高二生以及暱稱「cb」的蘇柏榕兩人，係以學術網路為骨幹，將跳板主機隱藏於台灣學術網路內，並利用木馬程式、網站漏洞侵入各大知名網站非法取得資料後，存放在國外網站主機，用以規避追查

卡優新聞網　2009/04/22

- 「資安人」雜誌總召集人侍家驊表示，民眾要定期注意惡意網站訊息的公佈，國內像「資安之眼」、「大炮開講」，或國外的「Zone-h」都有提供這些服務
- 侍家驊感慨，遭受駭客攻擊的很多企業網站，民眾瀏覽這些網站，很容易因此個資外洩，包括曾記麻糬、屈臣氏、2009宜蘭綠色博覽會、金門旅遊網、墾丁旅遊網等，每日流量都很高，但業者卻缺乏要付起資安的責任感
- 近年來非常流行的部落格，現在同樣是個資外洩一個重要管道，警政署資訊室主任李相臣表示，國、高中生在網站上不但放置個人私密資料與照片，還為了衝高人氣，想盡各種辦法，其實這些都是在讓個人隱私更透明

洩漏管道：內賊

自由時報 2009-3-21

- ☑ 校長為錢，竟然出賣學生！彰化地檢署去年底接獲檢舉，指稱員林鎮大佳補習班涉嫌與多所學校校長、甚至前教育局長勾結，以現金行賄取得學生個資，包括彰化縣及台中縣市有**二十多所學校、高達十萬筆學生個資被「賣」**
- ☑ 彰檢襄閱主任檢察官張慧瓊指出，檢方針對涉案重大的校長與業者展開監聽調查，今年二月初展開搜索約談，在主嫌吳芝庭（卅六歲）經營的大佳補習班搜到大批學生名冊與帳冊，吳芝庭坦承行賄校長，但因牽涉的學校過多，為免吳芝庭串證或湮滅證據，將她收押至今
- ☑ 據調查，吳錫勳、楊清順、顏士程等**三名校長從九十六年至九十八年間，涉嫌收取大佳補習班卅五萬元到七十六萬元不等，將學生資料提供給補習班**，資料包括學生年籍、照片、通訊地址、電話、家長名字及職業等，甚至地檢署檢察官的資料也在外洩名單中

洩漏管道：電腦失竊或儲存設備

筆記型電腦失竊 9.8萬人的資料外洩
（CNET新聞專區 2005/03/30）

- ☑ 柏克萊加州大學警告，該校研究所入學許可辦公室的**一台筆記型電腦遭竊，可能導致超過9萬8千人的個人資料外洩**
- ☑ 校方28日晚間發布消息說，該校研究所部的辦公室失竊一台電腦，內含的資料中，有三分之一的檔案儲存98,369名研究生或申請就讀研究所人士的姓名、出生日期、住址和社會安全號碼。有的檔案的建檔歷史長達三十年
- ☑ 校方表示，已採取額外措施防止類似的資料失竊事件再度發生。例如，該校已在儲存社會安全號碼的電腦上加裝加密軟體

隨身碟

記憶卡


MP3/MP4


手機

數位相機


PDA

2.5” 行動硬碟

遺失電腦與光碟造成個資外洩

ITHome 2009-4-14

- ☑ Sony生命保險週五（4/10）表示，公司內部遺失一部PC，硬碟中保存約14萬名顧客的個人資訊
- ☑ 該公司在4/3～4/4進行辦公室樓層搬遷作業後，4/7清點財產時發現少了一部PC，持續尋找至4/9均尚未尋獲，因此向警局報案
- ☑ 已確認遺失的個人資訊是2008年3月至2009年2月間，採用親至便利商店或金融機構繳款的顧客資訊，共14萬151人的保單編號、出生年月日、保單簽約日等資訊都在該遺失PC的硬碟中，不過並未包含姓名地址、電話、存簿帳號等更深入的個人資訊

中時電子報 2007/11/22

- ☑ 英國政府二十日坦承，遺失兩張包含二千五百萬民眾個人機密資料的光碟。這個數目近乎英國總人口六千萬的一半。
- ☑ 這兩張光碟記載了所有英國兒童福利補貼申請者個人資料，包括了二千五百萬人的姓名、地址、出生日期、國家保險號碼、以及銀行資料，包括個人帳號、密碼等。
- ☑ 這兩張未受鎖碼保護的光碟，自十月上旬裝入到印有英國皇家稅務及海關總署的信封袋後，從未遞達到倫敦國家審計局

洩漏管道：網站註冊

NOWNews 2010/02/01

- ☑ 駭客盜取資料的目標不是只有針對企業、不是只為了金錢？網路安全專家發現，目前網路犯罪已出現為了特定目的而搜集個人資訊與聯絡人的案例，包括電子郵件、IRC、即時通訊、P2P等在內的社交工程是主要手段，在2009 年第四季，亞太地區排行最高的感染管道為網際網路下載或其它惡意軟體所安裝的程式
- ☑ 其中，電影《暮光之城》(Twilight) 的新續集《新月》(New Moon) 也成了社交工程利用的對象之一，成為某個檔案分享入口網站的廣告工具，目的是希望藉由會員註冊來非法搜集個人資料
- ☑ 報告提醒，有越來越多的社交工程攻擊開始運用一些熱門時事，而且形態也出現各種變化

洩漏管道：部落格 & 網路相簿

NOW News 2009/12/15

- ☑ 服役於聯勤單位的22歲中士陳學葳自拍照曝光，引發社會不少譴責與關注。陳學葳已經坦承自拍，只是不知道放進無名小站「加密」，卻還是外流
- ☑ 先不論軍紀，從個人隱私的觀點來說，將照片放進加入密碼的網路相簿其實並不安全。所謂「道高一尺　魔高一丈」，其實把隱私照或是性愛照放入加密的部落格相簿，說穿了僅是跟全世界分享，甚至是請其他人幫你存檔
- ☑ 網路世界是非線性的載體，自拍照流出已經成了一種另類的永恆。因為台灣警方對於IP位址設在國外的網站，基本上是束手無策的，就算被害人要求刪除地球上所有的自拍照最後還是徒勞無功

NOW News 2009/11/10

- ☑ 散播自拍影片小心觸犯妨害風化罪！先前一名22歲從事服務業的潘姓女子從去年12月開始，在網路相簿中張貼色情圖片。而且還利用「台灣學生3P牛奶妹」等著名外流事件作為噱頭。後來屏東地方法院判決潘女處拘役25天，易科罰金2萬5千元
- ☑ 根據《刑法》235條明文規定，「散布、播送或販賣猥褻之文字、圖畫、聲音、影像或其他物品，或公然陳列，或以他法供人觀覽、聽聞者，處二年以下有期徒刑、拘役或科或併科三萬元以下罰金。」許多網友散播色情貼圖，其實也觸犯了這條法律

洩漏管道：Google Hacking（人肉搜索）

香港文匯報 2008-07-16

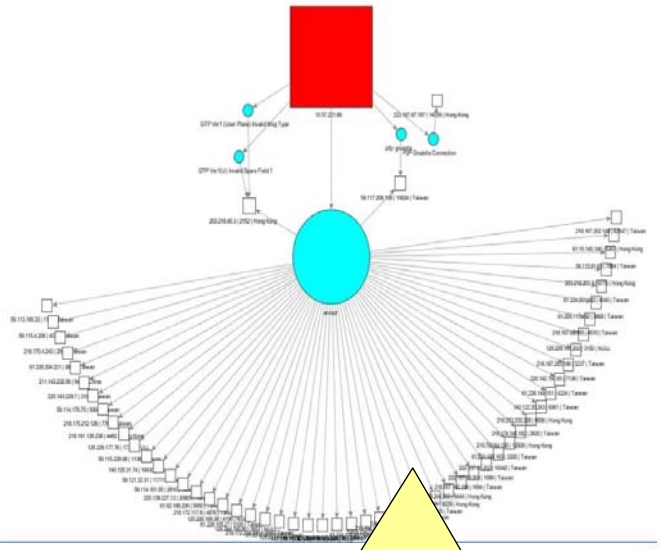
- ☑ 據搜狐網報道：成都九眼橋一酒吧老闆趙女士哭稱自己「即將崩潰」，因網民誤把她當成「二奶」，她受到大肆攻擊
- ☑ 6月16日，網上出現一篇名為《我就喜歡做二奶，我覺得我現在的生活就很好啊！》，發帖者叫「菊花香香兒1986」，炫耀自己當「二奶」的種種好處，激起了網友的憤怒並啟動「人肉引擎」
- ☑ 6月27日，一名叫「wangyouisliliang」的網友稱找到「菊花香香兒1986」的兩張照片。網友visav不久稱他搜索到「菊花香香兒1986」的博客和QQ號，相冊裡照片與「wangy-ouisliliang」公佈的正是同一人，即趙女士
- ☑ 趙女士說，6月28日，她打開自己博客，發現竟有上萬個留言，全是罵「爛貨」、「不要臉」、「無恥」等惡毒的話
- ☑ 針對趙女士的「人肉引擎」仍在變本加厲，昨天下午，她4歲兒子的照片也在一人肉搜索QQ群中流傳開來

洩漏管道：惡意程式與P2P軟體

網路資訊雜誌 219 期

☑ 社交平臺的威脅

- 主動型威脅：說白一點，就
電話詐騙的手法，詐騙內容
然是離不開角色扮演，不然
麼會博取你的「貪心、擔心
同情心、色心」，以達到詐
的行為
- 被動型威脅：此種威脅大多
使用者的不當行為所造成的
例如：上傳個人大頭照、私
照或包含不當背景的照片，
上傳過多的個人資訊，例如
生日、電話號碼、學經歷…。
- 混合式威脅：例如電子郵件社交工程的攻擊手法，進行網路釣魚：1. 使用誘人、感興趣的主旨與內文 2. 含有惡意程式的附件 3. 利用零時差攻擊



- Foxy、iMesh、 eDonkey、uTorrent等
- P2P 軟體同時與多部電腦的 P2P 軟體連線
- 分享設定錯誤或不良，造成重要資料外洩

竊個資門檻低 惡意程式年倍增

中廣新聞 2010-04-30

☑ 電腦左堵右防，就怕惡意程式上門，不過資安業者公布的年度全球資安報告顯示，由於入侵電腦，竊取個資的技術門檻越來越低，惡意攻擊持續攀升，去年惡意程式的數量比前一年成長一倍，尤其企業受害深，超過七成曾遭攻擊

☑ 儘管去年金融海嘯來襲，不過惡意程式攻擊卻有增無減，賽門鐵克資深技術顧問莊添發指出，像是去年惡意程式的數量就比前一年成長100%，尤其企業受害深，約七成五曾遭攻擊，進一步分析，與攻擊工具的技術門檻越來越低有關

☑ 賽門鐵克資深技術顧問莊添發說：「這些相關的攻擊工具可以用幾百美元，或甚至是免費下載的方式取得，使得入侵電腦、竊取個人資料的門檻越來越低。這也是為什麼說，網路犯罪的行為跟惡意活動持續不斷的增加。」

☑ 這份年度全球資安報告指出，台北去年躍升為全球殭屍電腦感染最多城市，占全球5%，另外報告提到，資安惡意攻擊的版圖，持續擴張到巴西、印度、俄羅斯等新興國家

機密個資路邊買得到

工商時報　2010/01/24

- ☑ 在俄羅斯，前科紀錄、個人地址、護照號碼、通聯紀錄、銀行帳戶資料、稅務資料或出入境紀錄都能一網打盡
- ☑ 莫斯科附近的Gorbushka市場，可媲美日本東京秋葉原的電器街，手機、電漿電視或最新DVD應有盡有，但真正內行的都知道，此處是個資黑市交易的大本營，只要你主動詢問，賣軟體的店家就會向你展示被政府列為機密的「資料庫」清單，據估計交易規模達數千萬美元
- ☑ 店家販賣的光碟名目繁多，諸如「內政部—聯邦道路安全局」、「稅務局」和「聯邦反毒局」等，每片光碟要價100美元。燒錄在光碟內的為俄羅斯執法單位或政府機構掌握的機密個資，舉凡前科紀錄、個人地址、護照號碼、通聯紀錄、銀行帳戶資料、稅務資料或出入境紀錄一網打盡
- ☑ 機密資料對罪犯、間諜和新聞記者來說，是夢寐以求的金礦，對那些將機密個資賣給電腦駭客牟利的警察和公務員來說尤其是。與俄羅斯不肖官員勾結的駭客，在取得這些個人資料後大量製作光碟，然後透過電子商場的店家或網路公開販售
- ☑ 個資黑市交易的規模估計高達數千萬美元

線上購書遭詐騙

中央社／台北縣 2009.12.15

- ☑ 台北縣議員林國春今天依民眾投訴指出，有人向誠品書局網購書籍，但取書後沒多久就接到詐騙集團電話並被騙失金，已要求北縣警方深入了解誠品內部是否有員工涉及個資外洩
- ☑ 林國春表示，家住板橋市的賴姓高二女學生，11月29日在誠品網站訂購書籍並到超商取貨，12月12日就接到疑似誠品客服來電告知，指賴女到超商取貨時, 誤簽12期分期付款單，要求在當晚12時前到自動提款機（ATM）操作，以取消分期手續
- ☑ 由於冒充誠品客服人員清楚說明她購書的所有資料，賴女不疑有他，就依來電指示轉帳新台幣2萬9800元，對方食髓知味，後來又再次來電，要求賴女須再拿另外一張提款卡到ATM(自動提款機)操作，且要求帳戶存款金額必須超過3萬元，才能完成退款動作
- ☑ 正當賴女急忙返家拿另1張提款卡時，家屬懷疑是詐騙集團並加以制止，除向警方報案外，也向誠品反映但未獲回應，因此，賴女家屬才向林國春投訴

利菁變性隱私遭洩

NOW News 2010/01/2

- ☑ 從購物天后轉戰演藝圈的利菁「變性」隱私，曾幫她操刀的醫師張啟中日前卻在醫師公會期刊上，揭露利菁「由男變女」的始末，經週刊報導後，醫師公會在網站上移除內文。衛生署指出，「張啟中洩露病人隱私，將要開罰。」
- ☑ 在台中醫師公會第59期期刊，他所寫的一篇文章第三段，字字句句本來是和同業分享，幫助病人由男轉女的案例，但文章最後一句，患者主動出書《歷經過去，利菁未來》，指名道姓病例當事人就是利菁，等於揭發病人隱私
- ☑ 衛生署醫事處副處長王宗曦表示，張啟中的作為，違法醫療法第72條「醫療機構及其人員因業務而知悉或持有病人病情或健康資訊，不得無故洩露」，也違反醫師法第23條「醫師除依前條規定外，對於因業務知悉或持有他人病情或健康資訊，不得無故洩露」
- ☑ 王宗曦表示，依醫療法的相關罰則，主管機關可處罰張啟中新台幣5萬元以上、25萬元以下的罰鍰；依照醫師法的罰則，則可罰2到10萬元，並可連帶懲處醫療機構負責人；如果按刑法第316條洩漏業務上知悉秘密罪，可處1年以下徒刑、拘役或5萬元以下罰金

警員洩漏個資被起訴

聯合報 2010.02.04

- ☑ 高雄市警楠梓分局陳姓警員為方便妻子與鄰居打官司，使用警方的刑事資料系統，查探對方親戚底細，高雄地檢署昨天依公務員洩漏國防以外秘密罪，將他提起公訴
- ☑ 陳員因妻子疑遭陳姓婦人女婿李姓男子恐嚇，便根據李姓男子的機車車牌，先查出李姓男子的身分證字號，再查出他犯有毒品前科
- ☑ 去年7月2日，陳妻到高雄地檢署開庭時，把李姓男子有毒品前科的事說了出來。李姓男子檢舉後，檢察官問陳姓男子的妻子怎麼知道李姓男子有前科，她說是在公園聽人講的
- ☑ 檢察官查出陳姓警員確實使用過刑事資料系統，搜尋李姓男子的刑事紀錄，且他本人也承認此事。檢察官因他坦承，且並非惡性重大，請法官對他從輕量刑

戶政人員涉洩漏個資

中央社 2009年07月21日

- ☑ 板橋地檢署今天指揮調查局北縣幹員，搜索台北市萬華警分局東園派出所及萬華第一戶政事務所等處
- ☑ 板橋地檢署偵辦台北看守所管理員貪瀆弊案時，意外查出案外案，發現有警察與戶政事務所人員，以每筆新台幣1000元至3000元的價格，涉嫌洩漏個人資料提供給非法職業賭場與土地開發業者，賭場並以此作為暴力討債的線索
- ☑ 檢察官王正皓約談1名警員與1名戶所課員，初步調查瞭解，東園派出所曹姓警員涉嫌以每筆新台幣3000元出售個人資料，戶所黃姓員工涉嫌以每筆1000元代價，提供個人資料
- ☑ 因兩人都涉嫌瀆職，檢調正深入調查，多少筆的資料被賣出

直銷邀填問卷小心個資外流

聯合報 2010.01.19

- ☑ 高雄火車站附近假日人潮洶湧，最近有直銷業者派出穿著套裝、身材高俊男美女，請陌生人寫問卷，不少人填寫後被拉去參與直銷活動，擔心個資外洩，上網發文警告民眾小心
- ☑ 記者實地觀察，發現平常日白天，也有不少戴著識別證、手拿問卷、筆的女子，在火車站前走廊找陌生人搭訕，假日則出現成群結隊、穿著套裝的俊男美女，打扮都很時尚
- ☑ 王先生分享被直銷搭訕經驗，填寫問卷後會被找去參加座談會，在遊說下購買不少保健食品，他強調，這些勸人加入直銷的說詞、伎倆都很老套，但隨意填寫問卷恐有個資外洩的疑慮，提醒民眾小心

Facebook再爆隱私漏洞

工商時報 2010-05-07

- ☑ 社交網站Facebook周三因系統錯誤造成部分用戶的線上聊天內容曝光
- ☑ Facebook在周三經歷「數小時」的系統故障，導致部分用戶不經意看到Facebook好友的私人聊天內容及尚未取得同意的交友邀請
- ☑ Facebook表示故障當時「用戶必須登入隱私設定頁面，並使用個人檔案預覽功能，還要輸入特定好友名稱才會看到上述私人資訊」，暗示這次故障影響範圍應該不大，但由於Facebook自年初以來不只一次發生類似情形，外界的批評聲浪依舊不減
- ☑ 華爾街日報報導，Facebook在年初就曾因系統故障導致私人訊息誤傳。這次的故障則是因為隱私設定功能的程式發生錯誤
- ☑ 消費者調查機構Consumer Reports資料顯示，社交網站成年用戶當中過半數都在網站發表「危險個人資訊」，卻有23%的用戶「不知道或不想使用隱私設定功能」

ITHome 2010-05-27

- ☑ Facebook執行長Mark Zuckerberg周三（5/26）宣布新的隱私設定功能，採用更簡化的設定與更清楚的規範，並允許使用者擁有全面的資料存取權限控制功能。Facebook此次更新的主軸之一就是內容單一控制介面，其他還包括針對使用者基本資料提供更強大的控制功能，以及讓使用者輕易就能關閉所有應用程式

隱私權相關法律（1）

刑法 306 條	☑無故侵入他人住宅、建築物或附連圍繞之土地或船艦者	處一年以下有期徒刑、拘役或三百元以下罰金
刑法 133 條	☑在郵務或電報機關執行職務之公務員，開拆或隱匿投寄之郵件或電報者	處三年以下有期徒刑、拘役或五百元以下罰金
刑法 315 條	☑無故開拆或隱匿他人之封緘信函、文書或圖畫者 ☑無故以開拆以外之方法，窺視其內容者	處拘役或三千元以下罰金
刑法 315-1 條	☑有下列行為之一者： –無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者 –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	處三年以下有期徒刑、拘役或三萬元以下罰金

用戶剪卡 保全員重黏盜領

自由時報／台北報導 98.12.23

- ☑ 台北市八德路的第一銀行，常有信用卡客戶剪卡或停卡寄回，大樓保全郭仲豪即趁機偷拆信，再記下卡號等資料或將剪斷的卡片用膠帶黏貼重組，犯案58次，持卡盜領2次，獲利4萬，遭台北地院依業務侵占等罪判拘役120日，可易科罰金12萬，緩刑5年；仍可上訴
- ☑ 郭某所屬的保全公司已賠償第一銀行損失，並向郭某追償，因郭某犯後態度良好，法官因此予緩刑5年，緩刑期間應服60小時的社區勞動，並接受保護管束以導正法律觀念

遙控視訊偷拍身體隱私

地方中心／屏東報導(2008/12/01 16:59)

- ☑ 日前屏東一名女子赫然發現自己的個人部落格上，竟然被人PO上她洗完澡的全裸影片，嚇得她趕快報警，以為房間內被裝設針孔攝影機。警方調查後發現，女子的電腦遭駭客入侵做怪，駭客把木馬程式用一段影片或圖檔包裝，放在公共的論壇讓人下載，使得下載民眾把木馬程式植入自己的電腦，駭客再利用木馬程式遙控對方電腦
- ☑ 被害女子的筆記型電腦裡就被植入一種叫做彩虹橋的木馬程式，因為她把電腦放在床上，剛好視訊就對準浴室，才會被拍到全裸出浴的畫面

隱私權相關法律（2）

民法第 195 條	不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操，或不法侵害其他人格法益而情節重大者，被害人雖非財產上之損害，亦得請求賠償相當之金額。其名譽被侵害者，並得請求回復名譽之適當處分。
兒童福利法第 19 條	依本法保護、安置、訪視、調查、輔導兒童或其家庭，應建立個案資料。因職務知悉之秘密或隱私及所製作或持有之文書，應予保密，非有正當理由，不得洩漏或公開。
醫療法第 70 條	醫療機構之病歷，應指定適當場所及人員保管，並至少保存七年。但未成年者之病歷，至少應保存至其成年後七年；人體試驗之病歷，應永久保存。醫療機構因故未能繼續開業，其病歷應交由承接者依規定保存；無承接者至少應繼續保存六個月以上，始得銷燬。醫療機構對於逾保存期限得銷燬之病歷，其銷燬方式應確保病歷內容無洩漏之虞
醫療法第 72 條	醫療機構及其人員因業務而知悉或持有病人病情或健康資訊，不得無故洩漏

病歷當廢紙案例

台視新聞 2006.3.5

- ☑ 新竹馬偕醫院驚傳病患大批的病歷資料，出現在對面的廢棄空屋內上，包括初診病患的資料資料，掛號單等隱私全部一覽無遺
- ☑ 手術室的紀錄表、住院保證書全都出現在新竹馬偕醫院對面廢棄屋的瓦堆裡
- ☑ 院方解釋，可能是前天三月三號晚上，清潔人員將回收的廢紙集中在三號電梯前時，其中有一箱廢紙就不見了

隱私權相關法律（3）

醫療法第 74 條	醫院、診所診治病人時，得依需要，並經病人或其法定代理人、配偶、親屬或關係人之同意，商洽病人原診治之醫院、診所，提供病歷複製本或病歷摘要及各種檢查報告資料。原診治之醫院、診所不得拒絕；其所需費用，由病人負擔
醫師法第 23 條	醫師除依前條規定外，對於因業務知悉或持有他人病情或健康資訊，不得無故洩露
護理人員法第 28 條	除依前條規定外，護理人員或護理機構及其人員對於因業務而知悉或持有他人秘密，不得無故洩漏
藥師法第 14 條	藥師對於因業務而知悉他人之秘密，不得無故洩漏
人體器官移植條例第 10-1 條	衛生機關、醫療機構、醫事人員、受委託之機構、團體及其相關人員，對於因業務知悉願意捐贈器官及等待移植者之姓名及病歷資料，不得無故洩漏
傳染病防治法第 10 條	各級主管機關、醫療 (事) 機構、醫事人員及因業務知悉傳染病病人或疑似感染傳染病之病人之姓名、病歷及病史等有關資料者，對於該資料，不得洩漏

修法讓病例分級

蘋果日報 2009年11月19日

- ☑ 國民黨立委吳育昇驚爆與美女鋼琴老師孫仲瑜去薇閣汽車旅館偷情後，孫仲瑜也遭爆料，到在台北市汀州路開業的減肥名醫林政誠診所求診，至少減肥十公斤。林政誠昨證實，他確實為孫仲瑜減肥，「她本來快三十（吋）腰，現在是二十五（吋）腰，減了確有十公斤。」

自由時報 99.1.3

- 國民黨籍立委郭素春提案修改「醫療法」，建議增加「醫院對於病歷，應依其性質或敏感性分級」，如果未來法案順利通過，像是減肥名醫林政誠出來爆料，立委吳育昇外遇對象孫仲瑜曾在其門診減肥10公斤有成的舉動，將遭到更嚴厲的處分
- 而修改醫療法第67條條文，也被外界戲稱「孫仲瑜條款」，對此立委郭素春表示，民眾就醫紀錄必須有更高等級的保密措施
- 郭素春也說，台灣自2002年開始推動電子式可攜病歷，2005年公告「醫療機構電子病歷製作及管理辦法」，但沒有將電子病歷依敏感性分級。甚至還發生過媒體報導明星罹病消息，而消息來源居然是主管機關員工

李登輝罹開放性肺結核案例

聯合報 2006/04/26

- ☑ 台北榮民總醫院昨天證實，前總統李登輝罹患輕度肺結核，經給予妥善藥物治療，其痰液結核菌抹片檢查，由陽性轉為陰性反應，已於前天下午三時卅分出院
- ☑ 李登輝因發燒、咳嗽和腹瀉，在三月十九日下午住進榮總治療，當時院方面對外界詢問，都稱李是因感冒才住院
- ☑ 某媒體報導前總統李登輝染肺結核住院，衛生署疾病管制局昨天要求台北市衛生局，須依傳染病防治法進行適當處置
- ☑ 疾管局說，肺結核是第三類法定傳染病，依照傳染病防治法，在未獲得病人本人同意之前，不得透露病人隱私，疾管局也從未對外發布單一結核病人的病情，對媒體報導個人罹病隱私，相信地方主管機關會依法做適當處置
- ☑ 傳染病防治法規定，因業務而知悉傳染病病人病情並洩漏，得處罰九萬元至四十五萬元。疾管局副局長施文儀說，若媒體是從他人處得知此事，應可認定是因業務而知悉
- ☑ 不過，台北市疾病管制處處長顏慕庸則認為，某媒體是否符合因業務知悉而洩漏傳染病人病情，還有討論空間，但將先進行規勸

acer

五、資安防護措施

（CERT Best Practices）

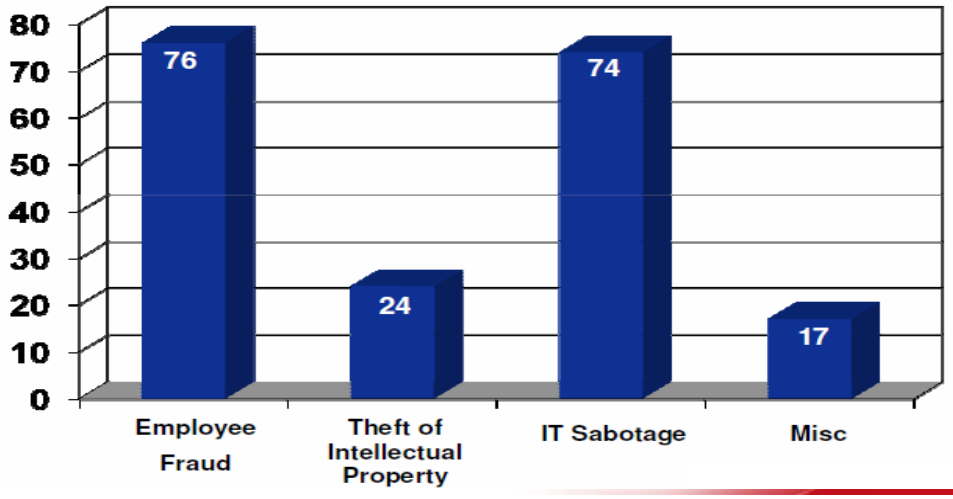
acer

CERT 研究與最佳實務（1）

☑ 研究過去數百個案例

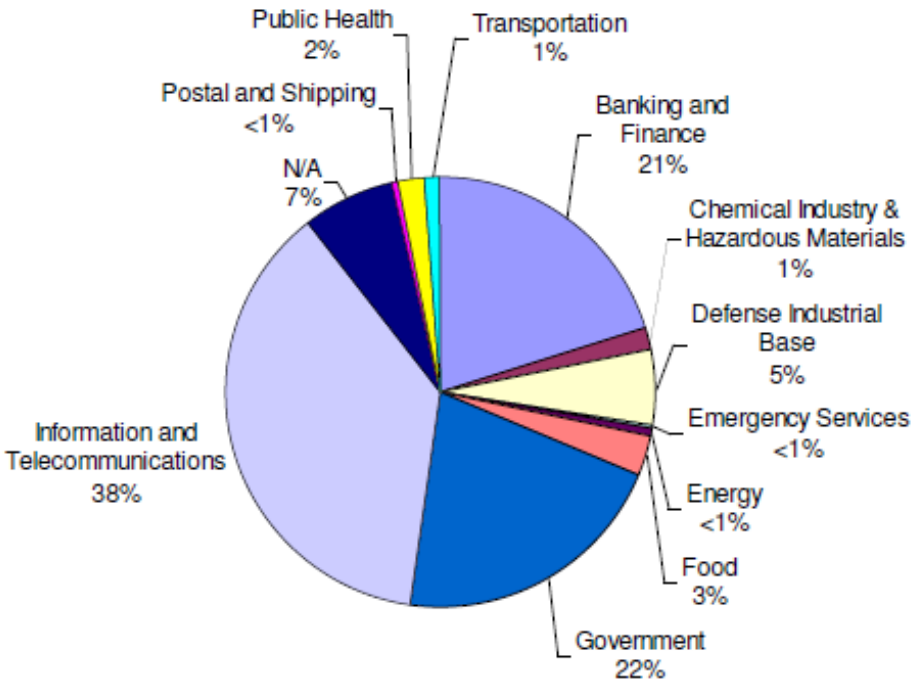
- 美國案例，1996 至 2009
- 重要基礎建設領域
- 包括技術與行為資訊

☑ 案例依屬性統計



CERT 研究與最佳實務（2）

☑ 案例依領域統計



CERT 研究與最佳實務（3）

- ☑ **Best Practice #1:** 在企業風險評鑑中考慮內賊與業務伙伴的威脅
  - 電話公司、信用卡公司、銀行等企業與某A單位簽約，但A單位雇用另一B單位的人，且B單位的系統管理者竊取前述企業數以百萬計的客戶個人資料
- ☑ **Best Practice #2:** 清楚寫下並一致性的強制實施政策與控制措施
  - 前任的合約包商遠端連線到組織的伺服器，拷貝業務計畫與軟體，並寄 E-mail 告知該組織禁止使用那些軟體，因為他擁有它們
- ☑ **Best Practice #3:** 實施週期性的資安意識教育訓練
  - 一位簽約的程式設計師在離職到競爭企業的前一天晚上，進入組織並在一位同事的辦公室偷走重要的程式原始碼，準備帶給新公司

CERT 研究與最佳實務（4）

- ☑ **Best Practice #4:** 針對可疑或破壞行為進行監視及回應
  - 一名不滿的系統管理員恐嚇同事並利用備份磁帶將重要程式集中，試圖擴大一個邏輯炸彈的衝擊
- ☑ **Best Practice #5:** 預見及管理負面的辦公室爭議
  - 一名資料庫管理員因長期與主管、同僚不合，為報復而刪除重要資料，造成 115 位員工耗費 1800 小時的工時重新回復及輸入資料
- ☑ **Best Practice #6:** 追蹤及強化實體環境
  - 一個能源管理單位的下包商打破緊急電力按鈕的防護玻璃，並關閉控制電網之間交換電力的電腦。該員工先前因與同事口角而被雇主取消進入廠區的權限，但仍設法潛入

CERT 研究與最佳實務（5）

- ☑ **Best Practice #7: 實施嚴格的密碼與帳號管理實務**
  - 一名系統管理員因績效差而被炒魷魚，之後利用離職前建立的帳號，花了數週佈建遠端攻擊的方法
- ☑ **Best Practice #8: 強制實施職責分離（Separation of Duty）和最小權限（Least Privilege）**
  - 一名不滿的系統管理員，即便其考績欠佳被降級且權限受限，仍有能力設計邏輯炸彈並竄改稽核記錄以陷害其主管
- ☑ **Best Practice #9: 在軟體開發生命週期中考慮內賊威脅**
  - 某電信公司的服務突然中斷，調查顯示一名不滿的程式設計師在一年前於網路通訊協定中插入惡意程式，且於半年前離職

CERT 研究與最佳實務（6）

- ☑ **Best Practice #10: 特別小心系統管理員及技術、特權使用者**
  - 某系統管理員突然辭職，公司拒絕支付其最後兩天的薪資，因此他將所有系統管理帳號的密碼變更，並要求以薪資來交換密碼
- ☑ **Best Practice #11: 實作系統異動管制**
  - 某程式設計師修改程式將異動警示功能關閉，該警訊是當一個罕用的操作畫面被用來修改重要資料時會警告安全人員。該程式設計師因此用該操作畫面犯罪長達一年半而未被發現
- ☑ **Best Practice #12: 紀錄、監控、稽核員工之線上行為**
  - 一名化工研發人員在前往競爭公司就任新職之前，於原公司下載 38000 個檔案，包括商業機密在內

CERT 研究與最佳實務（7）

- ☑ **Best Practice #13: 針對遠端攻擊採用分層防禦（Layered Defense）**
  - 某技術長在被降薪後辭職，遠端存取其前任雇主的系統，並將色情網站發出的色情郵件轉址給其雇主，造成郵件主機淹沒。此外並傳送威脅郵件給 CEO
- ☑ **Best Practice #14: 人員離職後終止其電腦存取權限**
  - 一名系統管理員因績效差而被炒魷魚，利用在離職前建立的遠端連線帳號，於離職當晚關閉公司的生產程序
- ☑ **Best Practice #15: 實作安全備份與回復程序**
  - 因內賊損毀系統並從異地偷走備份媒體，導致119 救災單位必須於民眾報案後以人工方式查閱案發地址
- ☑ **Best Practice #16: 發展內賊事件應變計畫**
  - 一位管理者因為疑似涉入詐欺活動而被暫停職務，卻以社交工程手法操控其員工在無意中銷毀其犯罪證據

CERT 研究與最佳實務（8）

- ☑ 內賊問題可能因下列因素而更複雜
  - 與外部人員共謀：內賊係外部人員雇用或為外部人員工作，包括組織犯罪、國外的政府或組織
  - 業務合作伙伴：對「信賴的」業務伙伴，很難對資訊和系統的存取進行控制/監視
  - 併購：被併購的公司可能有內賊，造成續存公司的風險升高
  - 文化差異：對美國公司內的非美籍員工，難以辨識內賊所呈現的行為指標
  - 忠誠度：美國的跨國公司在境外的分公司，大多數的員工並非美國公民

機關網站與系統
—宏碁經驗

- ☑ 制訂網站與系統安全規範
  - 檢核網站與系統之開發團隊資安能力
  - 要求設計開發落實資安規範，檢核 check-list
  - 對網站定期進行安檢（弱點掃瞄、滲透測試）
- ☑ 對重要系統（註冊、成績、...）限制存取
  - 僅能由校內網路存取使用
  - 校外需透過 VPN 或加密認證
  - 考慮納入 SOC 監控，定期檢核系統使用記錄（登錄頻率、密碼錯誤頻率、資料下載頻率、...）
  - 落實密碼管制：密碼定期更換、不多人共用密碼、使用動態密碼、...

Q&A