倫理道德與資訊安全

- 資 訊 科 技 與 競 爭 優 勢 -

李政峰 (James Lee)
經濟部工業局-能源管理系統輔導顧問
E-mail : jameslee1858@gmail.com

- **ISO 27001 主導稽核員**
- **ISO 20000 主導稽核員**
- **BS 25999 主導稽核員**
- **BS 10012 主導稽核員**

目 錄

道　德　問　題

- 資　訊　科　技　與　競　爭　優　勢 -

道德

在不道德與不合法之間的界線是什麼呢？當使用電腦時，特別是上網際網路時，你可能會面臨這樣的問題：你最近是不是下載了音樂呢？

所謂的道德，多半都是教人辨別對與錯之間的差異，而且要人們選擇做正確的事、做對的事。

電腦使用者的電腦道德

要決定哪些是對的事情而且貫徹去做，經常不是件簡單的事。電腦常會引起新的道德兩難，並把人們推入一個無法預期的狀態中。**電腦道德學(computer ethics)** 就是使用基本的道德原則來幫助人們在每天的電腦使用中做出正確的決定。道德原則可以幫助你思考所能做的選擇。

圖 1A 電腦引發了新的道德兩難並把人們推向難以做出決定的狀態

電腦使用者的電腦道德

道德原則(ethical principle) 定義了在道德上是對或錯的法則，以便人們能夠在做出決定時有正確的參考。

在美國健康、教育以及福利部門報告中指出三項最常用的道德原則：

- 所謂的道德原則就是當每個人都以這樣的方式來做的話，社會的整體將會得到好處。
- 所謂的道德就是如果你對待人們是以對待人的方式來對待的話，而不是對待一種東西。
- 所謂的道德就是旁觀者會認為這對雙方或各方面都是公平的。

電腦使用者的電腦道德

當你使用一台電腦時，有件事情必須要知道的，那就是誰擁有了資料、程式以及網際網路存取的權利，如果你擁有你電腦系統的軟體，你當然可以簡單的做你自己想做事情，而且你也只需要為這件事單純的負責。

你的學校或工作場所常常會有電腦使用原則(code of conduct)之類的使用指導(acceptable use policy)，你可以透過所屬單位的網頁宣導而知道。

電腦使用者的電腦道德

遵循學校及單位的規定(續)

圖片來源：截取自學校網頁

電腦使用者的電腦道德

遵循學校及單位的規定 (續)

請仔細研讀這些政策並遵循以下規則。

- 自重
- 尊重他人
- 尊重單位內規

電腦使用者的電腦道德

電腦道德的世界

所謂的「電腦道德十誡」以供電腦使用者、程式設計師和系統設計人員來參考：

1. 不要使用電腦來傷害其他人。
2. 不要使用電腦來干擾其他人的電腦工作。
3. 不要使用電腦來窺視周遭人的電腦檔案。
4. 不要使用電腦來進行偷竊。
5. 不要使用電腦來做任何錯誤的窺探。
6. 不要使用電腦來複製或使用你沒付費的電腦軟體。

電腦使用者的電腦道德

電腦道德的世界 (續)

7. 不要在未經授權或適當付費的情形之下，使用他人電腦的電腦資源。

8. 不要使用電腦來侵犯他人的智慧結晶。

9. 不要使用電腦來製作你認為可能會對社會產生不良影響的程式或設計出相關的系統。

10. 除非你確定你所做的事是深思熟慮且尊重所有其他人，不然不要使用電腦。

電腦使用者的電腦道德

網路禮儀

前面所提到的「電腦道德十誡」經常只是宏觀的指導，但並沒有針對特定的情形，尤其是你在上網的時候提供確切的指導，無論這件事是發生在聊天室還是在進行網路遊戲。

圖 1C 網路禮儀提供了如何在聊天室或線上遊戲時所能依循的行為指導

電腦使用者的電腦道德

網路禮儀 (續)

根據Albion.com的網路禮儀首頁中網路禮儀的參考：

- 討論區
- 電子郵件
- 即時訊息 (IM) 與文字訊息
- 聊天室 (Chat Room)

網路禮儀在公共空間中是非常重要的，許多機構都提供了在公共空間中使用電腦的建議與指導，以便規範網路禮儀的標準。像是在開機時關閉電腦的音量，除了要尊重其他人在網際網路服務上的使用，玩電腦遊戲時也是會面臨道德上的兩難。

電腦使用者的電腦道德

電腦遊戲：太多暴力嗎？

電腦遊戲的道德規範並非每個人都會遵從的，超過二分之一的遊戲是動作類的，在這其中最受歡迎的多是強調暴力與血腥的遊戲，所以家長們以及政治家們會認為孩童們玩這些遊戲將會讓他們沾染到不當的行為，並對於現實生活產生不良的影響。

人們擔心暴力電腦遊戲會對人們的行為造成影響。

圖 1D 有些電腦遊戲不僅具有暴力還包含了離經叛道的行為

組織中的電腦道德

在每天報紙上都有許多關於人們在工作中，因為不當的使用電腦而造成各種問題。

要保護資料以避免遺失或誤存， 常常是屬於是否能正確備份中的一環。**備份程序(backup procedure)** 包含了把資料檔案做複製，以便保護資料免於遺失、誤存或損壞。不論這樣的損壞是來自天災還是其他人為的破壞，如果沒有備份程序這個單位將會讓客戶的資料遭受風險。

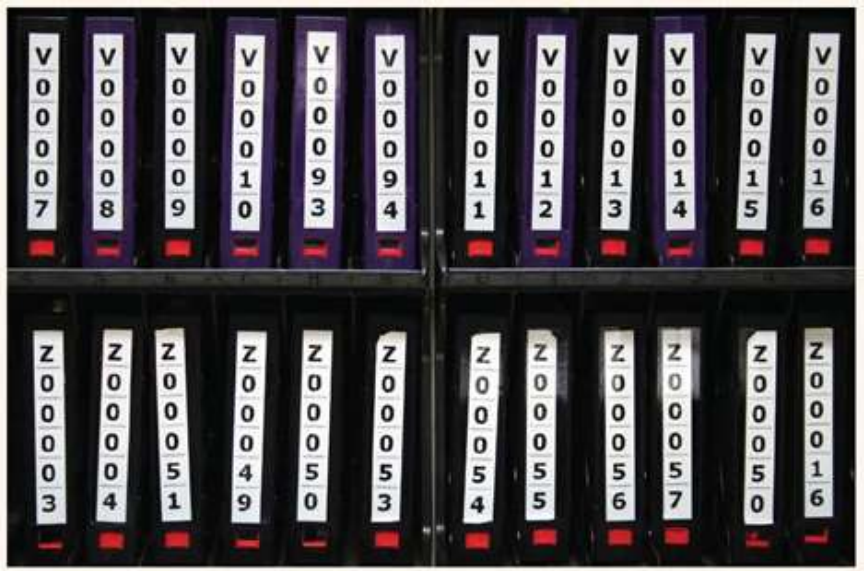


圖 1E 備份系統可以幫助企業資料、資產的維護，而電腦磁帶櫃或電腦磁帶庫就是儲存備份檔案常用的方式之一。

電腦專業人士的電腦道德

沒有一項專業在長期來看是不需要執行專業道德教條的，這就是為什麼我們在專業上要以不同的方式來探討道德的**執行規範(codes of conduct)**。

電腦專業人士的電腦道德

ACM執行規範

所有電腦組織的行為規範中，由ACM 所發展的是被認為最創新且最有遠見的內容。(計算機協會（Association of Computing Machinery，簡稱ACM）是一個世界性的計算機從業員專業組織，創立於1947年，是世界上第一個科學性及教育性計算機學會。)

根據ACM 的規範電腦專業人士的電腦道德是：

1. 對社會和人類福祉有貢獻的。
2. 避免傷害其他人。
3. 誠實且值得信賴的。
4. 對於種族、性別、宗教、年齡、殘障與否，或國籍、出生地等都不能有任何歧視而且要公平對待。

電腦專業人士的電腦道德

ACM執行規範 (續)

5. 對於著作權以及專利等所有權都要重視且引以為榮。

6. 當使用其他人的智慧財產時，必須要給予適當的尊重。

7. 尊重其他人的隱私權。

8. 對於機密和保密資料都要有所尊重。

電腦專業人士的電腦道德

電腦專業認證協會的道德規範

其他組織也提出了類似的道德規範，以便能約束所屬成員的行為。

- 追求更高標準的技能與知識。
- 捍衛所服務對象的機密關係。
- 公眾對專業標準與實務執行產生依賴。
- 一套值得遵循的道德標準。

電腦專業人士的電腦道德

安全第一

電腦專業人士所創造的產品會影響人們，甚至是有可能讓人們遭受傷害或死亡的危險。電腦和電腦程式常常影響系統的重要安全，包括交通監控以及醫院裡的病患監控系統。

圖 1F 病患監控可以讓醫院創造出更安全的環境

不只是不道德而且還不合法

電腦使用者還可能造成那些問題呢？讓我們來看看許多發生在各網路裡的問題，這會讓使用者引來嚴重的麻煩那就是：剽竊

。

不只是不道德而且還不合法

剽竊

使用其他人的智慧財產(其概念或寫下的文字) 被稱為剽竊 (plagiarism)，剽竊這種違法的行為早在電腦發明前即已存在，但電腦與網際網路讓這樣情形變得更容易而且更為嚴重。
剽竊是一項嚴重的冒犯行為！

不只是不道德而且還不合法

剽竊 (續)

當你越有名的時候，你所有犯過的過錯將越有可能被揭發出來，像是知名的歷史學家以及普立茲獎得主Doris Kearns Goodwin 就是一個例子。Goodwin 的剽竊在15 年後才被揭發，而且這不只是一個個案，你也可以在相關的知名網站中找出其他的案例(網址www.famousplagiarists.com)。

在資料的撰寫中你可以使用其他人的心血結晶在你自己的文章或報告裡，如果你使用這些句子或一些句子是從其他來源得到的話，只要列出你所用的來源即可，而且最好把這些來源的清單和基本的介紹給付上。

不只是不道德而且還不合法

誹謗

由於電腦強大的威力以及網際網路在通訊上的功能，這也讓誹謗變得更為嚴重，在美國所謂的誹謗(libel) 就是公開發表不當的言論，而且影響或傷害某人在工作上或名譽上的權益。

不只是不道德而且還不合法

盜版軟體

以下是常見的情況，你需要在文書撰寫、表格制訂時使用 Microsoft Office 2010，例如：你的一位朋友給了你他從他媽媽辦公室裡拿來的軟體，你就在你電腦裡安裝了這一份從他那裡拿來的軟體，那麼你這樣有錯嗎？

當然有，事實上你朋友也有錯，他違法的部分在於他從他媽媽辦公室裡複製來這套軟體。

不只是不道德而且還不合法

盜版軟體 (續)

圖 1H　軟體與資訊產業協會 (SIIA) 不斷告知大眾有關於軟體盜版的嚴重性

不只是不道德而且還不合法

盜版軟體 (續)

很多免費的程式是允許使用者複製和修改其內容的，這稱之為公眾導向軟體(public domain software)。但這並不意謂著公眾導向的軟體是可以完全免於著作權規範的，一般都可以透過其讀我(Read Me) 文字檔來瞭解其規範。

不同於公眾導向軟體， 你不能在沒有經過所有權人的允許之下就複製或修改共享程式(shareware)，一般都可以在其幫助(Help) 檔案中或讀我(Read Me) 檔案中找出其所有權人對於授權資訊的條件，一般這些讀我檔案都會放在程式安裝的同一個資料夾裡。

不只是不道德而且還不合法

盜版軟體 (續)

怎麼知道其他的軟體是否為盜版的軟體呢？以下所有的行為都是不合法的：

- 在沒有註冊費的前提下，持續使用已經過了試用期的共享軟體。
- 即使你已經付錢買了該程式，但卻違反其軟體授權的項目。舉例來說，你把同一份程式裝在桌上型電腦以及筆記型電腦，但軟體授權只允許你安裝在一台電腦，這就意謂著你違反了授權的項目。

不只是不道德而且還不合法

盜版軟體 (續)

- 把安裝在你工作中或學校裡所需要的網站授權程式(site-licensed program) 複製或安裝到你家裡的電腦(除非授權內容允許這樣的行為)。
- 把商用軟體複製或銷售給其他人。
- 把一部分或全部的GPL 一般公眾授權程式放到商用軟體中並進行銷售。

不只是不道德而且還不合法

盜版軟體 (續)

常見的授權證明是所謂的「產品註冊金鑰」(product Registration key)，一般都是由一連串且獨一無二的英文字與數字所組成，並且只適用於該軟體。這些金鑰常常是在安裝軟體時需要輸入，以便啟動或通過認可。而在日後升級、更新時，也會需要用到這些金鑰。

不只是不道德而且還不合法

檔案分享：音樂、電影以及其他

你或許聽過：下載一首具有著作權的MP3 檔案並且在24 小時之內可以合法的使用。但這是錯誤的。

政　府　法　規

- 資　訊　科　技　與　競　爭　優　勢 -

資通安全相關法令

- 國家機密保護法
- 電子簽章法
- 刑法(防駭條款)
- 個人資料保護法
- 檔案法
- 著作權法
- 行政院及所屬各機關資訊安全管理要點
- 機關公文電子交換作業辦法
- 智慧財產權法-商標權、專利權、著作權

網路使用可能涉及觸犯刑法的行為

- **第358條 無故入侵電腦罪**
  - 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。
  - 本條主要目的為遏止駭客入侵行為。
- **第359條 無故取得、刪除或變更他人電磁紀錄罪**
  - 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。
  - 本條主要目的為確保電腦內部電磁紀錄安全。
- **第360條 無故干擾電腦系統罪**
  - 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。
  - 本條主要目的為維護電腦及網路運作正常。

網路使用可能涉及觸犯刑法的行為

- **第361條 對公務機關犯罪之加重**
  - 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。
  - 本條主要目的為**確保國家安全**。
- **第362條 製作供犯罪程式罪**
  - 製作專供犯本章之罪之電腦程式，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。
  - 本條主要目的為**防止犯罪工具之利用與擴散**。
- **第363條 告訴乃論**
  - 第三百五十八條至第三百六十條之罪，須告訴乃論。
  - 本條主要目的為**集中司法資源對抗重大犯罪**。

電腦犯罪

- 未經授權的使用、存取、修改，以及破壞相關硬體、軟體、資料或網路資源。
- 主動傳播未經授權的資訊。
- 未經授權複製軟體。
- 拒絕使用者存取其所擁有的硬體、軟體、資料及網路資源。
- 經由計畫性地使用電腦或網路資源，以非法手段取得資訊或有形資產。

安全管理科技的採用比例

使用的安全科技		安全管理
防毒軟體	99%	• 在已開發國家，安全防護的預算約占 6% 至 8%。 • 74% 的公司已經或考慮在兩年內，設置安全長（chief security officer）或資訊安全長（chief information security officer）的職位。 • 40% 的公司已有隱私長（chief privacy officer），6% 的公司將在未來兩年內指派。 • 44% 的公司表示：在去年，它們的資訊系統或多或少都有資訊外洩的情況發生。 • 37% 的公司已投保網路險，5% 的公司也有意願投入。
虛擬私有網路	91%	
入侵偵測系統	88%	
資料備份	82%	
年度安全計畫測試	48%	
安全計畫遵守審核	27%	
生物識別	19%	

駭客入侵

- 非本份地使用電腦，或未經授權便存取並使用連網電腦
- 非法駭客經常攻擊網際網路等網路，以竊取或毀壞資料與程式
- 駭客社群可約略分為建立型與破壞型兩種。破壞者（cracker）〔亦可稱為黑帽（black hat）或邪派駭客（darkside hacker）〕是指不懷好意或企圖犯罪的駭客。這個詞彙鮮少被用在安全防護產業之外，現在的程式設計師也很少使用這個名詞。一般大眾都用駭客（hacker）來表示。在電腦的行話裡，駭客的含義比較廣泛，這個詞來自於白帽駭客（white hat hackers）的相對用法。

駭客攻擊企業網站常見的手法

常見的駭客手法

阻斷服務（Denial of Service）：常見的網路惡作劇型態。藉由對目標網站伺服器送出大量的訊息，有效地降低網站伺服器的服務品質，甚至造成當機癱瘓。這種讓電腦超載的技倆有時會被用來掩護其他的攻擊行動。

掃描（Scans）：廣泛地掃描探測網際網路來辨識電腦、服務與連線型態。心術不正的人則用來找尋電腦或軟體的漏洞以進行攻擊。

監聽（Sniffer）：能夠祕密監聽網際網路上的資料封包，藉此偷取密碼或完整的內容。

欺騙（Spoofing）：利用偽裝的電子郵件或網頁，來騙取使用者的密碼或信用卡卡號。

特洛伊木馬（Trojan Horse）：針對軟體漏洞所設計的惡意程式。

後門（Back Doors）：當原始進入的管道被發現，便另做一個隱藏且容易進入，但又難以發現的通道。

惡意小程式（Malicious Applets）：具有惡意的小程式經常夾帶在 Java 電腦語言中，可濫用你的電腦資源、竄改硬碟中的檔案、傳送不實郵件，並竊取密碼。

撥號戰術（War Dialing）：一種可以自動狂撥數千通電話號碼的程式，可偵測是否有數據機連線。

邏輯炸彈（Logic Bombs）：潛藏在電腦系統中的一段程式或指令，只要設定的條件吻合，就會觸發攻擊。

緩衝區溢位（Buffer Overflow）：傳送大量資料來灌爆電腦記憶體緩衝區的技術，藉此搞垮或取得電腦控制權。

解密程式（Password Crackers）：利用軟體工具猜測密碼的方法。

社交工程術（Social Engineering）：透過與沒有戒心的公司員工聊天，以騙取高價資訊（如：密碼）的手段。

垃圾搜尋（Dumpster Diving）：從公司內的垃圾搜尋出有價資訊，藉以侵入內部電腦系統。有時這些資訊會搭配社交工程術一起使用，增加可信度。

網路恐怖主義

- 網路恐怖主義使用組織或政府的電腦或資訊（特別是透過網際網路），來造成身體的、真實世界的傷害，或是建築物的毀損。
- 美國州議會聯合會下了一個較好的定義：
  - 恐怖組織或個人，使用科技來強化他們的攻擊。這包含使用資訊科技來組織並執行對網路、電腦系統和電信通訊基礎建設的攻擊，或是使用科技來交換資訊或製造威脅。
- 2007 年5 月，愛沙尼亞在塔林（Talinn）市中心拆除了俄羅斯第二次世界大戰紀念碑後，遭受到大規模的網路攻擊。採用的手法是分散式阻斷服務攻擊（distributed denial of service attack）。

職場裡的網路濫用

網路濫用	行為
一般電子郵件濫用	包括大量發送垃圾信件、騷擾訊息、連鎖信、懇求的訊息、惡作劇信件、傳播病毒／蠕蟲，以及毀謗性文章。
未經授權的使用及存取	未經允許而將密碼及存取權限分享給他人。
侵犯及剽竊版權	使用違法或盜版軟體的侵權行為，將導致公司付出數百萬美元的賠償，其中包含複製他人網站及其商標。
新聞群組發文	在各式各樣與工作無關的新聞群組中發表文章。
傳送機密資料	經由網際網路展示或傳播商業機密。
色情圖片	不僅在工作場合中瀏覽色情網站，並展示、傳播相關網站上的資訊。
駭客攻擊	從事駭客行為，範圍從阻斷式服務攻擊到非法存取公司資料庫都有。
下載／上傳與工作無關的檔案	利用程式分享軟體、電影、音樂、寫真圖片等，導致公司的網路頻寬被占用殆盡。
隨性瀏覽網站	經由公司網路從事個人活動，包含購物、寄送郵件、玩遊戲等。
使用外部網際網路服務供應商	利用外部網際網路服務供應商來連結網際網路，避免被公司發現。
兼差	利用公司的網路與電腦資源來從事個人的商業行為。

軟體侵權

- 未經授權而重製軟體〔或稱為軟體侵權（software piracy）〕也是軟體盜竊的主要手法。
- 很多公司都會簽署區域授權（site licenses）合約，允許在特定份數、特定地點範圍內進行重製，讓員工可以合法地使用軟體。其他方案還包括允許重製分享的共享軟體（shareware），以及沒有版權限制的免費軟體（public domain software）。
- 2007 年，世界上有38% 的軟體都是侵權的。報導顯示，軟體產業在2007 年因軟體侵權的損失將近480億美元。

智慧財產剽竊

- 音樂、電視節目、影像、文章、書籍，或與著作相關的作品也容易受到侵害，這就是智慧財產剽竊（intellectual property theft）。
- 點對點(P2P)檔案分享工具能讓MP3音樂檔在網路上的任兩台電腦中互傳。

電腦病毒與蠕蟲

- 在電腦犯罪中，破壞力最大的可能要屬電腦病毒（computer viruses）與蠕蟲（worms）。
  - 「病毒」一詞比較常見，但就技術層面而言，電腦病毒本身無法自行運作，必須依附在其他程式上
  - 「蠕蟲」則是獨立的程式，能自行運作
- 電腦病毒通常透過電子郵件與附加檔案，或經由網際網路與線上服務，以及非法重製軟體而進入電腦系統。
- 從網際網路下載的共享軟體也是一種常見的入侵方式。

廣告軟體與間諜軟體

- 廣告軟體是一種提供有用功能的軟體，讓網路廣告商不需經由使用者的同意便展示其橫幅廣告或彈跳視窗式廣告。在一些特殊的例子，廣告軟體甚至會蒐集客戶主機端的個人資訊，再透過網際網路傳送給該軟體所有人，而此類廣告軟體便稱為間諜軟體（spyware）

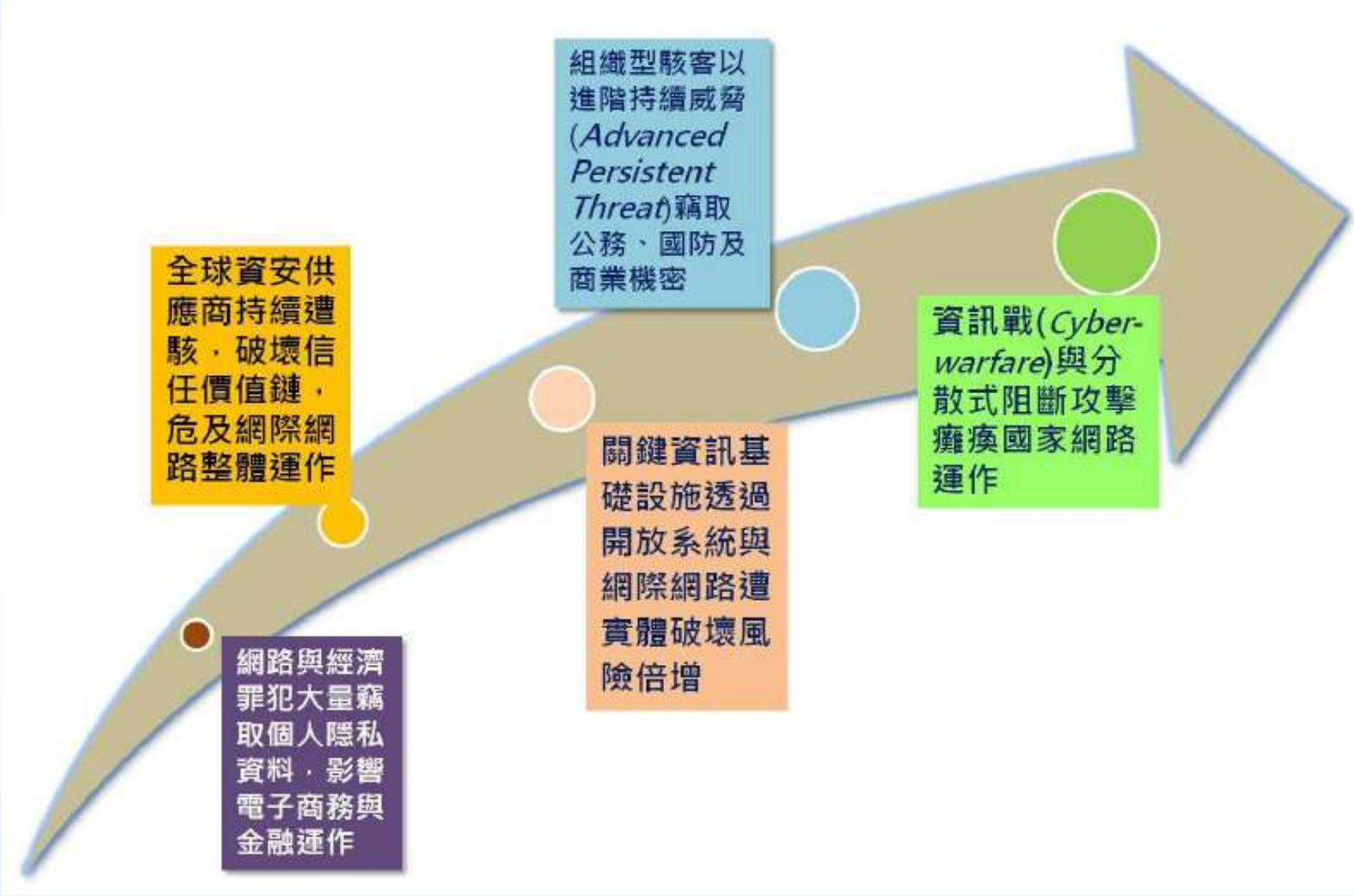
隱私權議題

- 存取私人的電子郵件交談與電腦紀錄，或蒐集並分享使用者瀏覽網站或新聞群組時所取得的個人資訊（違反隱私權）
- 行動與定位服務讓個人的行蹤更加無所遁形，完全掌握個人行蹤（電腦監視）
- 利用多種來源取得顧客資料，針對特定顧客群發展行銷計畫（電腦比對）
- 蒐集電話號碼、電子郵件信箱、信用卡卡號與其他個人資訊，來建立個別顧客輪廓（未經授權的個人檔案）
- 針對網際網路，選擇退出（opt-out）或事前同意（opt-in）是主要的爭論點。

資訊安全與道德的挑戰

- 資 訊 科 技 與 競 爭 優 勢 -

全球資安發展趨勢


網路與經濟罪犯大量竊取個人隱私資料，影響電子商務與金融運作
全球資安供應商持續遭駭，破壞信任價值鏈，危及網際網路整體運作
關鍵資訊基礎設施透過開放系統與網際網路遭實體破壞風險倍增
組織型駭客以進階持續威脅(Advanced Persistent Threat)竊取公務、國防及商業機密
資訊戰(Cyber-warfare)與分散式阻斷攻擊癱瘓國家網路運作

全球資安威脅情勢

- 組織化網路犯罪猖獗
- 個人隱私資料被竊與金融詐騙事件頻傳
- 關鍵資訊基礎設施資安風險增加
- 進階持續性威脅加劇
- 零時差攻擊造成資安防護困難

組織化網路犯罪猖獗

國際上資安威脅已從個別、單純的炫耀，演變成有組織、以經濟或政治等特定利益為目的的入侵行為。近來網路犯罪組織趨於高度專業分工，加以「網路戰」發起不受時間、空間條件限制，具有首戰即決戰之特性(一決勝負)，已使資通訊安全之概念及範圍產生實質變化。

個人隱私資料被竊與金融詐騙事件頻傳

駭客透過電子郵件社交工程或利用網站應用程式漏洞、網頁掛木馬等方式，在受害電腦植入惡意程式，以竊取個人隱私資料，並與犯罪集團合作，進行金融詐騙。例如2011 年4 月日本SonyPSN (Play Station Network)遭駭客入侵，導致近8,000 萬筆個資外洩。

關鍵資訊基礎設施資安風險增加

在數位經濟時代，重要資通訊設施一旦遭受破壞，勢將影響經濟、民生及整體政府運作；而各類關鍵基礎設施（Critical Infrastructure，CI）的監督控制與資料獲取系統（Supervisor Control And Data Acquisition，SCADA），通常較無堅實的資安防護設計，兩者均為網路駭客重要攻擊目標。

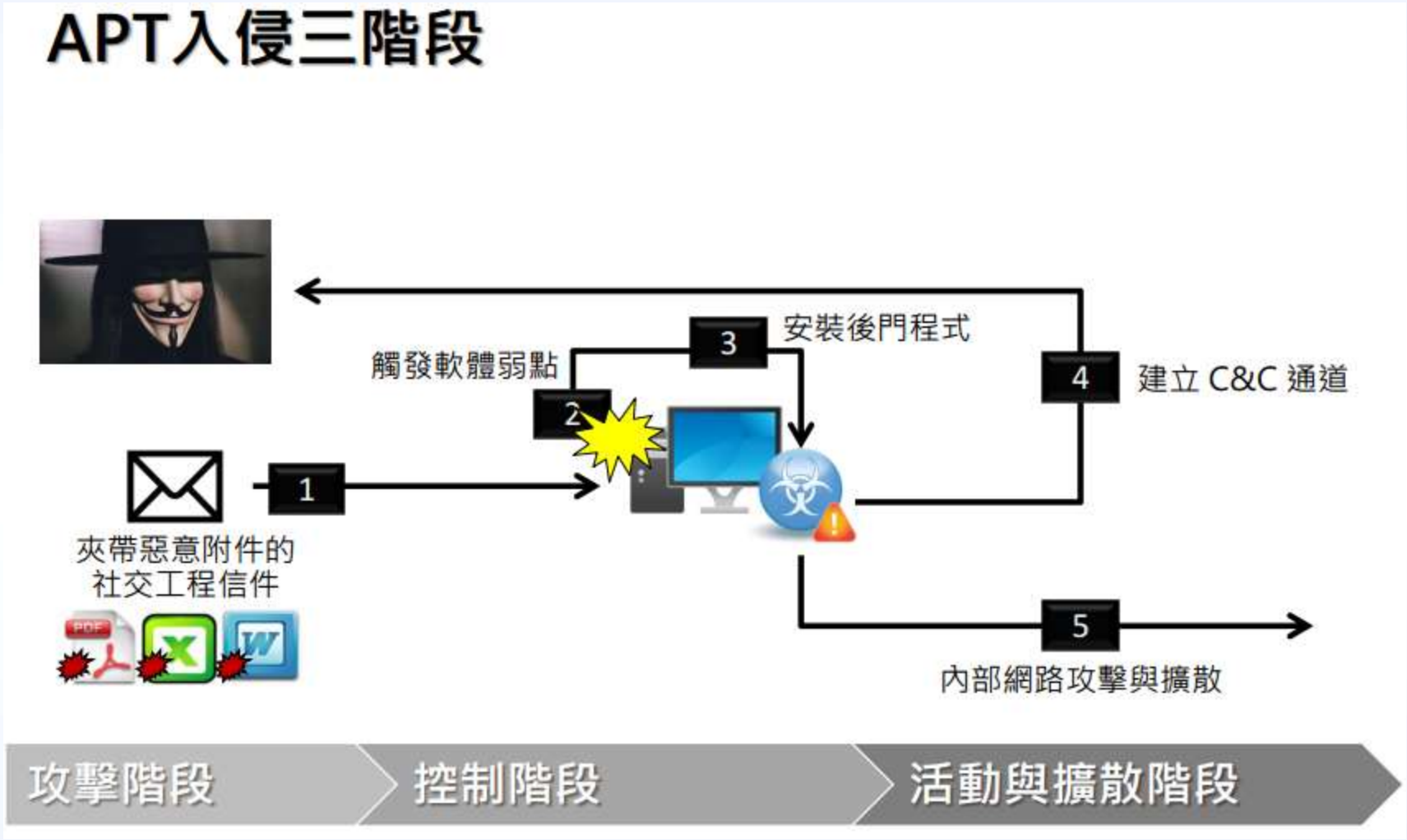
進階持續性威脅加劇

進階持續威脅(Advanced Persistent Threat，APT)攻擊之特徵為針對特定目標、低調、隱匿、手法多變、客製化等。近期美、英、法、德、紐及澳等國政府，均相繼傳出疑似遭APT 攻擊，企圖竊取該國政府重要及機敏資料。

進階持續性威脅加劇

- 進階持續威脅(APT)模式：(資料來源：技服中心)

進階持續性威脅加劇



資料來源：趨勢科技2013台灣APT白皮書

零時差攻擊造成資安防護困難

「零時差攻擊(Zero-day Attack)」係指在軟體弱點尚無修補方式之前，所出現之攻擊行為。駭客通常利用假冒寄件者身分、引人興趣之主旨與內文，並結合含零時差攻擊之附件檔，進行電子郵件社交工程攻擊。一旦收件者開啟電子郵件之附件檔，即被植入含零時差攻擊之惡意程式。

Top six security threats for 2014

1. BYO Trends in the Workplace
2. Data Privacy in the Cloud
3. Reputational Damage
4. Privacy and Regulation
5. Cybercrime
6. The Internet of Things

bsi.

Copyright © 2014 BSI. All rights reserved.

Source:
Information Security Forum (ISF) Dec. 2013

5

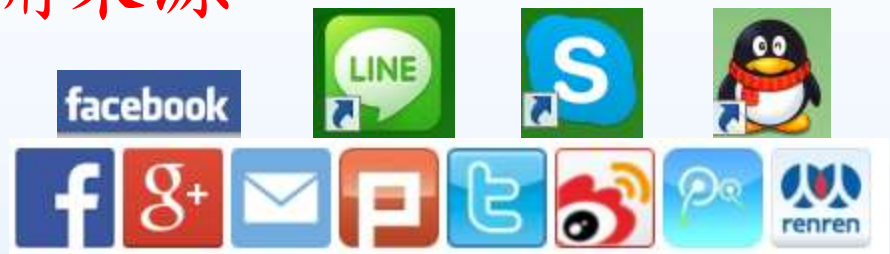
資料來源：BSI

資安法律事件案例分享

- 資 訊 科 技 與 競 爭 優 勢 -

資訊資料存在哪邊？

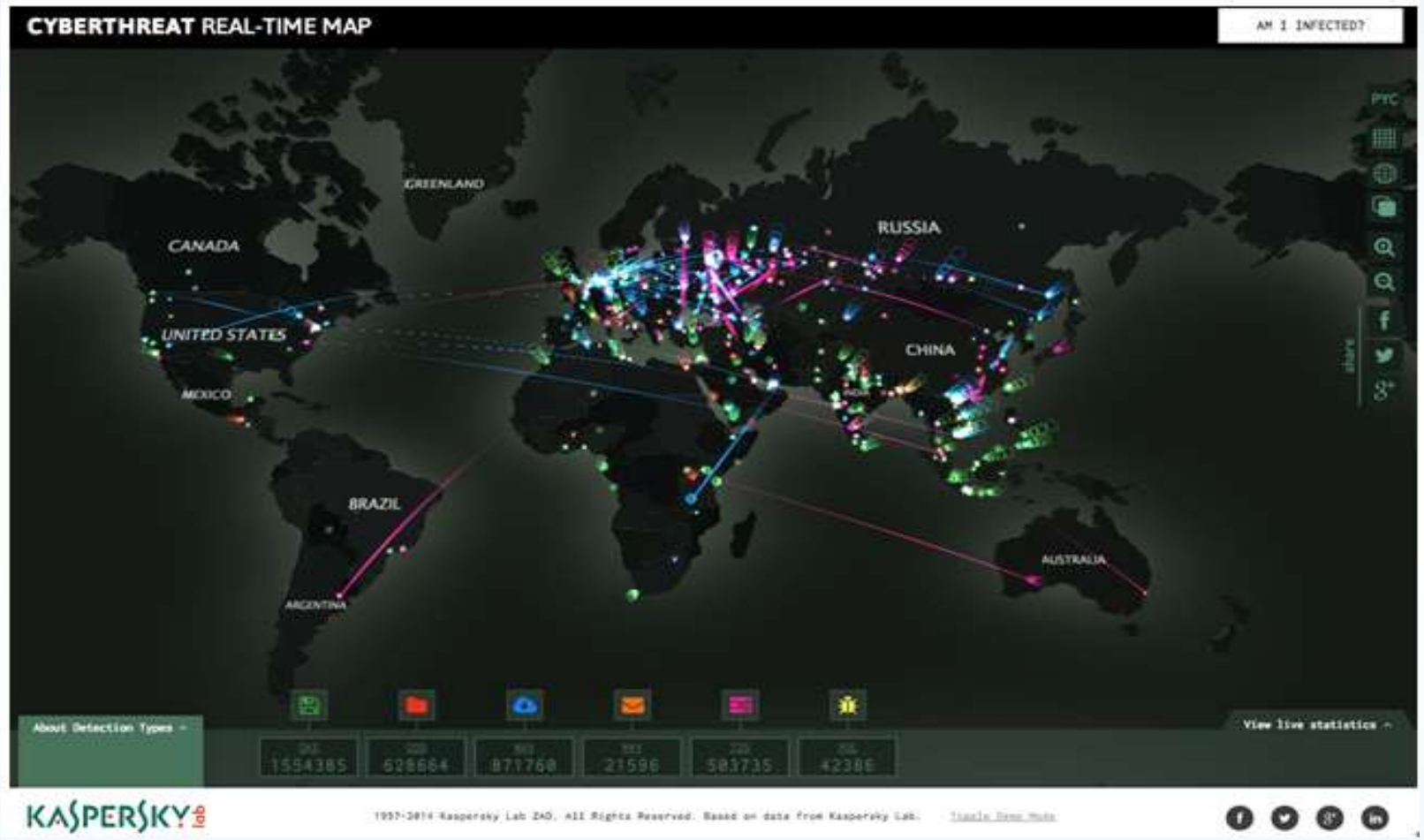
- 電腦相關資訊
- 正式文件
- 文件草稿
- 信手塗鴉
- 內部通訊
- 正式及非正式會議
- 媒體及公開來源
- 閒聊八卦
- 社群



資安法律事件分享

資料來源：卡巴斯基防毒公司

資安法律事件分享



2014 年 4 月 9 日來說，台灣名列全球最受網路攻擊國家的第28名。

資料來源：卡巴斯基防毒公司

資安法律事件分享

2013年企業概況

- 外洩資料總數：5.75億筆
  - 沒有意識到資料外洩企業比例：44%
  - 造成資料外洩原因：意外（27%）、**外部惡意程式**（57%）、內部人員外洩（13%）、駭客鎖定攻擊（2%）、國家級攻擊行動（1%）
  - 最常發生資料外洩的產業：健康醫療（28%）、政府（15%）、高科技製造業（11%）
  - 資料遭竊企業平均外洩資料：63萬筆
  - 資料遭竊最多產業：**高科技製造業占49%**，零售業占30%，政府部門占11%
  - 每筆外洩資料平均成本：188美元

bsi.

Copyright © 2014 BSI. All rights reserved.

Source:
SafeNet Data Protection Company, Apr. 2014

4

資料來源：BSI

資安法律事件分享

世界經濟論壇(WEF) Global Risks 2015 Report

資料來源：BSI

資安法律事件分享

架設色情網站或販賣、散佈、張貼猥褻圖文

刑法第235 條第1 項：

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。

兒童及青少年性交易防治條例第28 條第1項：

散布或販賣前條拍攝、製造之圖畫、錄影帶、影片、光碟、電子訊號或其他物品、或公然陳列，或以他法供人觀覽者，處三年以下有期徒刑，得併科新台幣五百萬元以下罰金。

資安法律事件分享

架設仲介色情網站

刑法第231 條：

意圖使男女與他人為性交或猥褻之行為，而引誘、容留或媒介以營利者，處五年以下有期徒刑，得併科十萬元以下罰金。

資安法律事件分享

轉寄色情圖文、影像

刑法第235 條第1 項：散佈猥褻物罪。

援助交際

社會秩序維護法第80 條第1 項規定，意圖得利與人姦、宿者處三日以下拘留或新台幣三萬元以下罰鍰。

兒童及少年性交易防制條例第29 條：

以廣告物、出版品、廣播、電視、電子訊號、電腦網路或其他媒體，散布、播送或刊登足以引誘、媒介、暗示或其他促使人為性交易之訊息者，處五年以下有期徒刑，得併科新台幣一百萬元以下罰金。

資安法律事件分享

木馬程式入駭

2004年5月27日，國內公民營機構上千台電腦遭中國駭客植入惡意木馬程式 Peep.exe 和 PeepBrowser.exe

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

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。

資安法律事件分享

竊聽及盜截機密資料

在2004年8月時，我駐韓代表部辦公室電腦遭竊聽及盜截機密資料。

就駭客攻擊或入侵電腦的行為而言，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。
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。」
國防機密，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。

資安法律事件分享

網頁被更改

- 2004年7月，財政部賦稅署網站遭中國駭客入侵，出現五星旗。
- 2015年8月1日，教育部網站疑似被「匿名者」亞洲分部（Anonymous Asia）的駭客組織攻擊。
- 2015年8月3日，「匿名者」三度攻擊 癱瘓國民黨、新黨、經濟部、國民黨台北市黨部網站。

資安法律事件分享

木馬程式入駭搶錢

近年來國內許多金融機構、科技公司等百大企業，遭到木馬程式入侵，竊取機密文件，且已有多家網路銀行於一年中就有近三千萬元以上損失。

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。

資安法律事件分享

盜刷集團

近年來盜刷集團盜取的被害人資料，冒名向發卡銀行申辦信用卡，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。

嫌犯以盜取的被害人資料，偽填信用卡申請書後向發卡銀行冒名申辦信用卡的行為，乃將構成偽造署押及偽造文書罪。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。

資安法律事件分享

入侵虛擬世界

多達數百萬會員的天堂網路遊戲服務多年前驚爆遊戲公司網站遭到駭客攻擊事件，許多玩家的帳號遭盜、寶物遭竊。

刑法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」

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者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

資安法律事件分享

竊取密碼

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。

刑法第359條之無故變更電磁紀錄罪

第339-3條之電腦詐欺罪。

資安法律事件分享

破解悠遊卡【資料來源：蘋果日報100/09/28】

悠遊卡設計四道加密防護機制，發行公司曾號稱「絕對不可能被破解」，嫌犯吳○○是○○科技公司資訊安全顧問，為了挑戰不可能，歷經四個月埋首研究、重寫程式，終於破解成功，可用自製讀卡機為悠遊卡竄改加值。吳○○以自製讀卡機加值300元，陸續持悠遊卡盜刷消費6 次、共608 元，扣除他卡片中原本的569 元，不法所得僅39 元。

違反《電子票證發行管理條例》、詐欺等罪嫌移送偵辦，最重恐面臨十年徒刑。

另外吳○○為提升駭客技術，和同伴常入侵大小公司系統，將會違反刑法第358 條以下的妨害電腦使用罪的相關罪名，併予說明。

資安法律事件分享

手機病毒

自2004年6月全球出現第一隻以行動電話為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為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。

製作病毒的行為，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。

資安法律事件分享

個人資料外洩

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。這個以劉嫌為首的集團，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

可能觸犯「個人資料保護法」第41條：「意圖為自己或第三人不法之利益或損害他人之利益，足生損害於他人，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。」

資安法律事件分享

處罰對象:
負責人與執行者

科大洩數百生個資 網路可輕易查到【資料來源：蘋果日報100/09/27】
有民眾反映兩科技大學，不慎將學生個資公布在網路上。對此，兩科大均坦承疏失，立即刪除相關資料，承諾加強教職員再教育。

依照新修正個人資料保護法(以下簡稱新版個資法)第5條1的規定，前述行為不得逾越特定目的之必要範圍，且應與蒐集之目的具有正當合理之關聯，否則將會違反新版個資法的規定。另依新版個人資料保護法27條的規定，非公務機關保有個人資料檔案者，應採行適當之安全措施，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。

資安法律事件分享

網路賭博

有些網站業者可能認為，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：「犯罪之行為或結果，有一在中華民國領域內者，為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為，司法機關一樣可以主張管轄權 。**(屬人主義，非屬地主義)**

資安法律事件分享

垃圾郵件

某男子為了替自己經營的網站行銷，竟利用網路發信軟體系統，侵入某軟體公司主機，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。

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

資安法律事件分享

報復行為

具有美國電腦碩士學位的張姓男子，遭美國知名網站購物公司開除後，為求報復，竟上網扮駭客，利用先前預留的後門，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。

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；

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。

資安法律事件分享

上網公佈不雅照片

某校研究生，上網公佈不雅照片。

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，為誹謗罪，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。」

資安法律事件分享

不當管理-警察筆錄P2P外洩

警察機關安裝P2P分享軟體Foxy，導致許多詳載個人資料的筆錄成為公共分享檔案。

資安法律事件分享

不當管理-誹謗罪

轉寄未經證實的八卦信
2000年10月，某網友因轉寄一則「XXX 醫師草菅人命」的網路信件而遭起訴的案件。

刑法第27 章「妨害名譽及信用罪」第310 條:
意圖散布於眾，而指摘或傳述足以毀損他人名譽之事者，為誹謗罪，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。
對於所誹謗之事，能證明其為真實者，不罰。但涉於私德而與公共利益無關者，不在此限。

資安法律事件分享

不當管理-誹謗罪

2015-07-10 03:00:51 聯合報 記者廖炳棋、劉時均／台北報導

LINE轉傳八仙謠言 男最高裁罰3萬

LINE等手機通訊軟體發達，但隨便在通訊軟體上散布不實言論可能觸法。依違反社會秩序維護法「散布謠言」罪嫌移請台中地院簡易庭裁處。

台北地檢署前檢察官徐士瑋指出，如果余姓男子只將這則訊息傳給一人，沒有給其他人觀看的意圖，就不涉及誹謗；但若傳送時如已預料對方會將訊息轉傳他人，就有散佈意圖，可能涉及誹謗；但誹謗罪是告訴乃論之罪，必須當事人提告才成案。

資安法律事件分享

不當管理-公然侮辱罪

在網站、BBS 或電子郵件中轉貼或撰寫謾罵他人的文章

刑法第27 章「妨害名譽及信用罪」第309 條：「公然侮辱人者，處拘役或三百元以下罰金」以及**第310 條**:
意圖散布於眾，而指摘或傳述足以毀損他人名譽之事者，為誹謗罪，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。對於所誹謗之事，能證明其為真實者，不罰。但涉於私德而與公共利益無關者，不在此限。

資安法律事件分享

不當管理-偷窺

偷窺他人的電子郵件或資料

刑法第315 條妨害祕密罪：
無故開拆或隱匿他人之封緘信函、文書或圖畫者，處拘役或三千元以下罰金。無故以開拆以外之方法，窺視其內容者，亦同。

資安法律事件分享

不當管理-任意公佈

未經同意將他人的私人資料放在網站上，例如個人電話號碼

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。

資安法律事件分享

不當管理-分享軟體

使用者不能利用「分享軟體」來販售圖利，以免侵害「著作權」。

著作權法第91 條規定：
擅自以重製之方法侵害他人之著作財產權者，處六月以上三年以下有期徒刑，得併科新台幣二十萬元以下罰金。

資安法律事件分享

不當下載

男子分享平台下載軍方資料被求刑

一名男子從FOXY網站分享平台發現陸軍作戰、防禦計畫等檔案，因為剛剛退伍，對軍事消息充滿興趣，所以下載了二十件檔案，包括陸軍砲指部資料、作戰防禦計畫等，而這些檔案當中，有部分資料尚未解密。高雄市調處在網路上意外發現該起事件，報請檢察官偵辦，對於這些資料如何流出，軍方還在瞭解。地檢署偵辦後依「外患罪」起訴該名男子，求處8個月徒刑，因為沒有造成損害，所以建議法院緩刑。

刑法第109條「中華民國國防應秘密之文書、圖畫、消息或物品」，因此該名男子在網路上蒐集及下載檔案資料的行為，屬於蒐集國防秘密，依照**刑法第111條**的規定，可能會面臨5年以下有期徒刑的刑事責任。

資安法律事件分享

第109條（洩漏交付國防秘密罪）

- 洩漏或交付關於中華民國國防應秘密之文書、圖畫、消息或物品者，處一年以上七年以下有期徒刑。
  洩漏或交付前項之文書、圖畫、消息或物品於外國或其他派遣之人者，處三年以上十年以下有期徒刑。
  前二項之未遂犯罰之。
  預備或陰謀犯第一項或第二項之罪者，處二年以下有期徒刑。

第111條（刺探搜集國防秘密罪）

- 刺探或收集第一百零九條第一項之文書、圖畫、消息或物品者，處五年以下有期徒刑。
  前項之未遂犯罰之。
  預備或陰謀犯第一項之罪者，處一年以下有期徒刑。

課　後　評　量

- 資　訊　科　技　與　競　爭　優　勢 -

李政峰 (James Lee)
經濟部工業局-能源管理系統輔導顧問
E-mail：jameslee1858@gmail.com

- ISO 27001 主導稽核員
- ISO 20000 主導稽核員
- BS 25999 主導稽核員
- BS 10012 主導稽核員