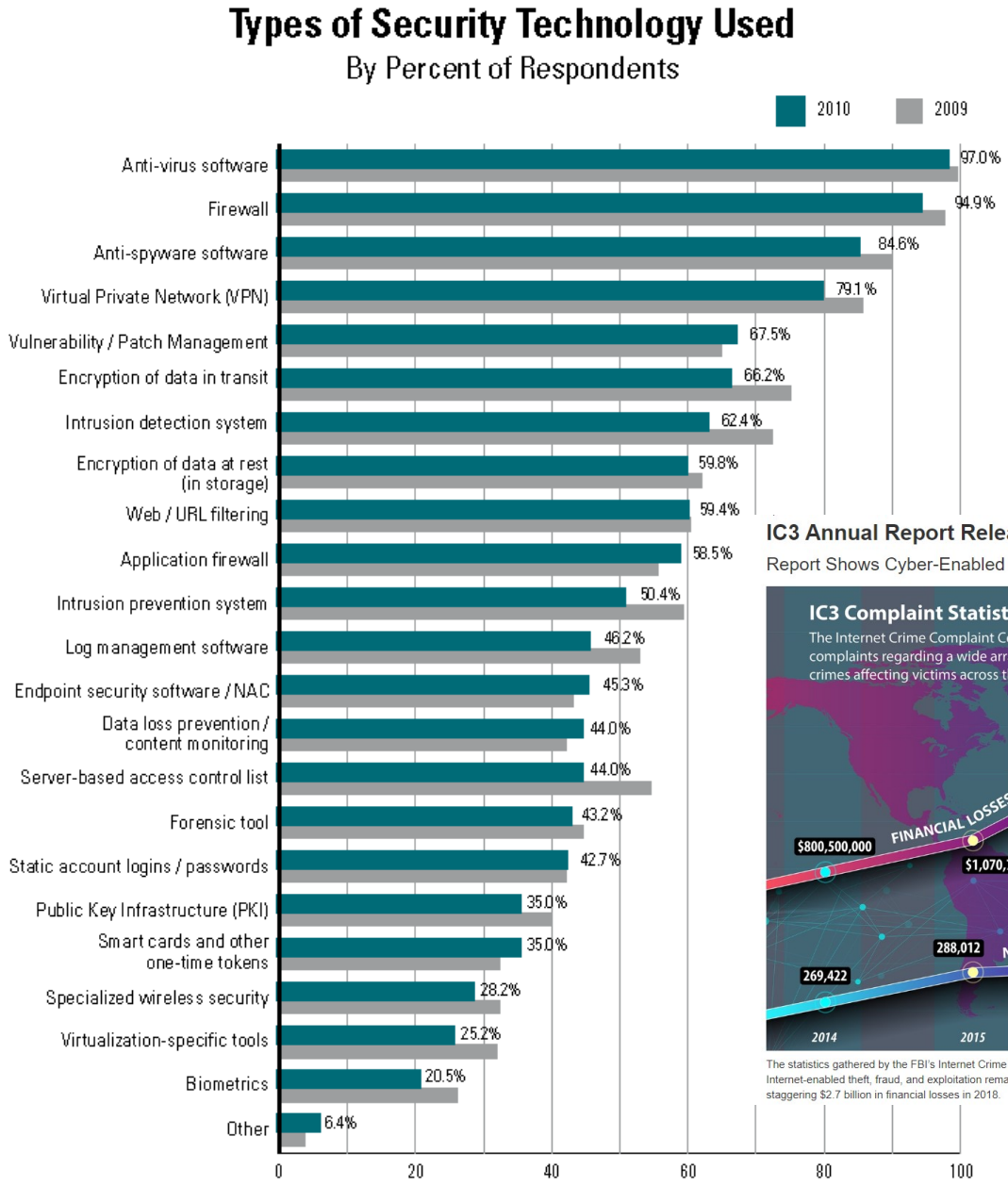
如何做好資訊安全？

南台科技大學

資訊管理系

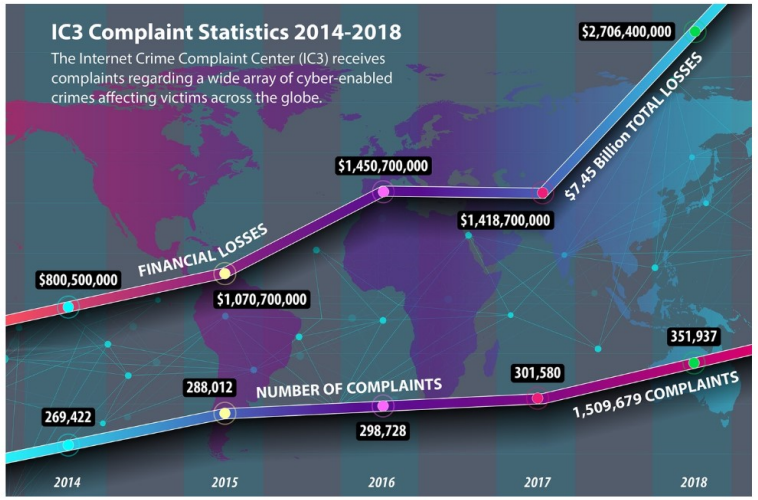
陳志達

CSI/FBI 電腦犯罪與安全調查



IC3 Annual Report Released

Report Shows Cyber-Enabled Crimes and Costs Rose in 2018

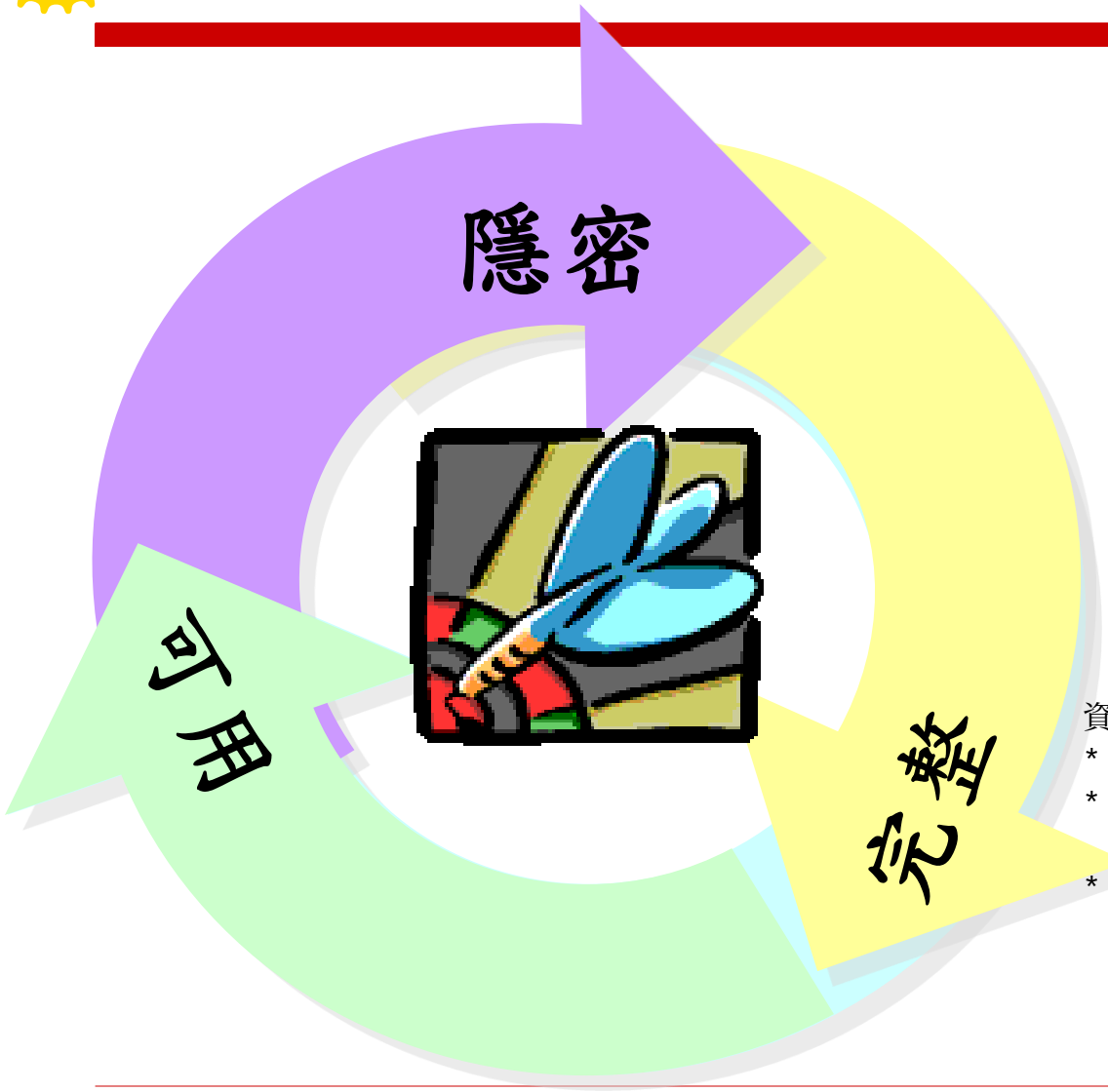


The statistics gathered by the FBI's Internet Crime Complaint Center (IC3) for 2018 show Internet-enabled theft, fraud, and exploitation remain pervasive and were responsible for a staggering $2.7 billion in financial losses in 2018.

資訊安全之威脅

- 電腦病毒
  - (病毒、蠕蟲、木馬等)
- 網際網路的安全性不足
  - (開放系統、通訊協定的把關)
- 安全措施不夠
  - 密碼設定問題、網路芳鄰
- **Hacker或Cracker**
  - 漏洞或破解密碼
- 系統或軟體本身的問題
  - 花旗銀行事件、作業系統的漏洞
- 管理不當(人禍)
  - 內賊、電腦與文件管理缺失
- 天災
  - 不可抗拒的災難

資訊安全的目標



C.I.A

- **Confidentiality(隱密性)**
  - 防止他人監看訊息內容(窺探)
- **Integration(完整性)**
  - 資料需要完整性(竄改、偽裝、否認)
- **Availibility(可用性)**
  - 保持供合法使用者可使用的狀態(阻斷服務)

資安3A

* Authorization(授權)：依需求給予實體適當的權限。
* Authentication(認證)：識別使用者身分，紀錄資訊被誰存取使用。
* Accounting(紀錄)：包含Measuring、Monitoring、Rrporting和Logging，用以提供Auding、Billing、Analysis、Management。主要精神在蒐集系統和user間的互動資料，並留下軌跡。

資訊安全的應用層面

- 資料安全
  - 傳統一般文件、檔案的安全管理
- 電腦系統安全
  - 個人電腦的資料管理
- 網路安全
  - 網路系統的資料管理
- 電腦病毒防治

資訊安全技術分類

- 資料安全
  - 企業資料安全
  - 個人資料安全
- 網路安全
  - 有線網路
  - 無線網路

電腦駭客與怪客（Hacker & Cracker）

- Hacker：
  - 熱衷研究、撰寫程式的專才，且必須具備樂於追根究底、窮究問題的特質
- Cracker：
  - 以非法手段侵入別人電腦，來竊取或修改電腦中重要資料的人，或利用系統本身漏洞，來攻擊散播駭客工具。
- 防止電腦駭客/怪客的入侵方式，最耳熟能詳的就是裝置「防火牆 」(Firewall) 。

什麼是病毒？

1. 病毒是一段電腦程式碼，它會將以自身附加(複製自身)到程式或檔案，在電腦之間傳佈，並在旅行途中感染電腦。病毒可能會損壞您的軟體、硬體和檔案。
2. 病毒的種類
   - **開機型病毒**
   - **檔案型病毒**
   - **巨集型病毒**

什麼是蠕蟲？

1. 蠕蟲（Worm）就像病毒，它的設計目的是在電腦之間複製它本身，但它會利用被掌控電腦做傳輸檔案的功能自動進行複製。
2. 蠕蟲極具危險的一點是，它會大量複製。『本尊』會複製出很多『分身』，就像西遊記中的孫悟空一樣，拔幾根毛就可以複製出幾個分身，然後像蠕蟲般在電腦網路中爬行，從一台電腦爬到另外一台電腦，最常用的方法是透過區域網路（LAN）、網際網路（Internet）或是 E-mail 來散佈自己。
3. 當新的蠕蟲散播時，它們會以極快的速度散佈開來，塞滿網路並可能讓您（及每個人）必須等待兩倍以上的時間才能檢視網際網路上的網頁。
4. 最近流行的有： Sasser 和 Blaster、VBS_LOVELETTER 蠕蟲。

什麼是特洛伊(Trojan)木馬程式？

- 特洛伊木馬程式就像神話中所述的一樣，看起來像是一件禮物，但結果卻是一些突擊特洛伊城的希臘士兵，它會潛伏在被駭的電腦中收集各式各樣的資料，然後傳送給駭客。
- 攻擊方式：
  - 轉向入侵(Redirect Intrusion)
  - 遠端遙控
  - 偷取封包
  - 獲取各類密碼
  - 刪除或複製各類檔案
  - 在電腦上開一後門
  - 更改或刪除登陸資料(Registry)

間諜程式(Spyware)

- 間諜程式並非病毒或惡意的程式碼， 而是危及您隱私的應用程式，允許駭客在您毫無知覺的情況下取得您電腦的控制權。
- 經常隨著您下載想要的應用程式的同時，不知不覺地下載到您的電腦上。
- 包括間諜程式、廣告軟體、惡意撥號程式、惡作劇程式、駭客工具、遠端存取工具、密碼破解應用程式，以及其他未分類的軟體。

我如何判斷是否已感染蠕蟲或其他病毒？

- 電腦
  - 速度可能會變慢
  - 停止回應
  - 當機
  - 每隔幾分鐘重新啟動
- 病毒有時會攻擊啟動電腦時所需使用的檔案。在這種情況下，您可能會按下電源按鈕，並發現整個螢幕都是空白的。

Email會受到那些方式的攻擊與入侵？

- 癱瘓信箱收件(郵件炸彈)
- 截取信件
- 信件夾帶
  - 病毒或破壞程式
  - 木馬程式
- 騙取各類密碼(含網路釣魚;Phishing)
- 惡作劇或罵人信件

Phishing(網路釣魚)

- 網路拍賣買空賣空騙錢術
- 綁架網路銀行 駭客偷卡號
- 真病毒假網頁 要釣你的錢
- 我中獎了…？是被騙了！
- ……

瀏覽器會受到那些方式的攻擊與入侵？

- 網頁中夾帶惡意程式碼、病毒或木馬
- 下載檔案
- 網頁釣魚法(Phishing)
  - 更新瀏灠器的安全修正程式，取消瀏覽器中密碼自動記憶功能，並調高IE安全性設定
- 利用部落格(Blog)
- 漏洞入侵(各種瀏覽器都存在有漏洞)

主機會受到那些方式的攻擊與入侵？

- 一般電腦入侵
  - 透過網路芳鄰PORT 139入侵(Port是網路送收雙方進行訊息交換服務所使用的管道)
  - 打開Telnet服務
  - Email植入木馬、病毒或破壞程式
- 漏洞入侵
  - Windows、IIS、Apache、SQL Server漏洞
- 拒絕服務攻擊(Denial of Service)
  - 封包攻擊、漏洞攻擊、DDoS分散式攻擊

達成資訊安全的方法

- 安裝防火牆(Firewall)
- 企業通訊採用VPN(Virtual Private Net)
- 更新您的電腦
- 使用現有的防毒 軟體
- 備份管理與異地備份

Firewall

- 對內及對外的**雙向安全管理機制**(軟硬體方式皆有)
- 只允許一些特定的資料通過，且必須經過一些事先設定的安全規則和策略才能放行。
- 能有效紀錄網路傳輸的資料量與種類
- 不能防護沒經過它的資料傳送
- 不能防止新的威脅也不能完全防止病毒

企業通訊採用VPN(Virtual Private Net)

- 利用公眾網路（ Public Internet ）的骨幹，如ADSL，做私人的資料傳輸。
- 為了不使私人的資料在公眾網路上遭到攔截，加密及解密的技術 在企業虛擬網路中可說極為重要。

更新您的電腦

- 安裝 Windows 及 Windows 元件的安全性更新
  - **Windows Update**
    http://windowsupdate.microsoft.com
- 安裝 Microsoft Office 產品的安全性更新
  - http://office.microsoft.com/officeupdate

防毒軟體廠商的清單

- Kaspersky Lab(http://www.kaspersky.com/)
- F-Secure Corp. (http://www.f-secure.com/)
- McAfee, Inc. (http://www.mcafee.com/tw/)
- Symantec(http://www.symantec.com.tw/)
- 趨勢科技 (http://www.trendmicro.com/tw/home/enterprise.htm)
- Panda 軟體(http://www.pandasoftware.es/home)
- 金山毒霸(http://db.kingsoft.com/default.shtml)

排行網址

AV-Comparatives

AV-TEST

備份管理與異地備份

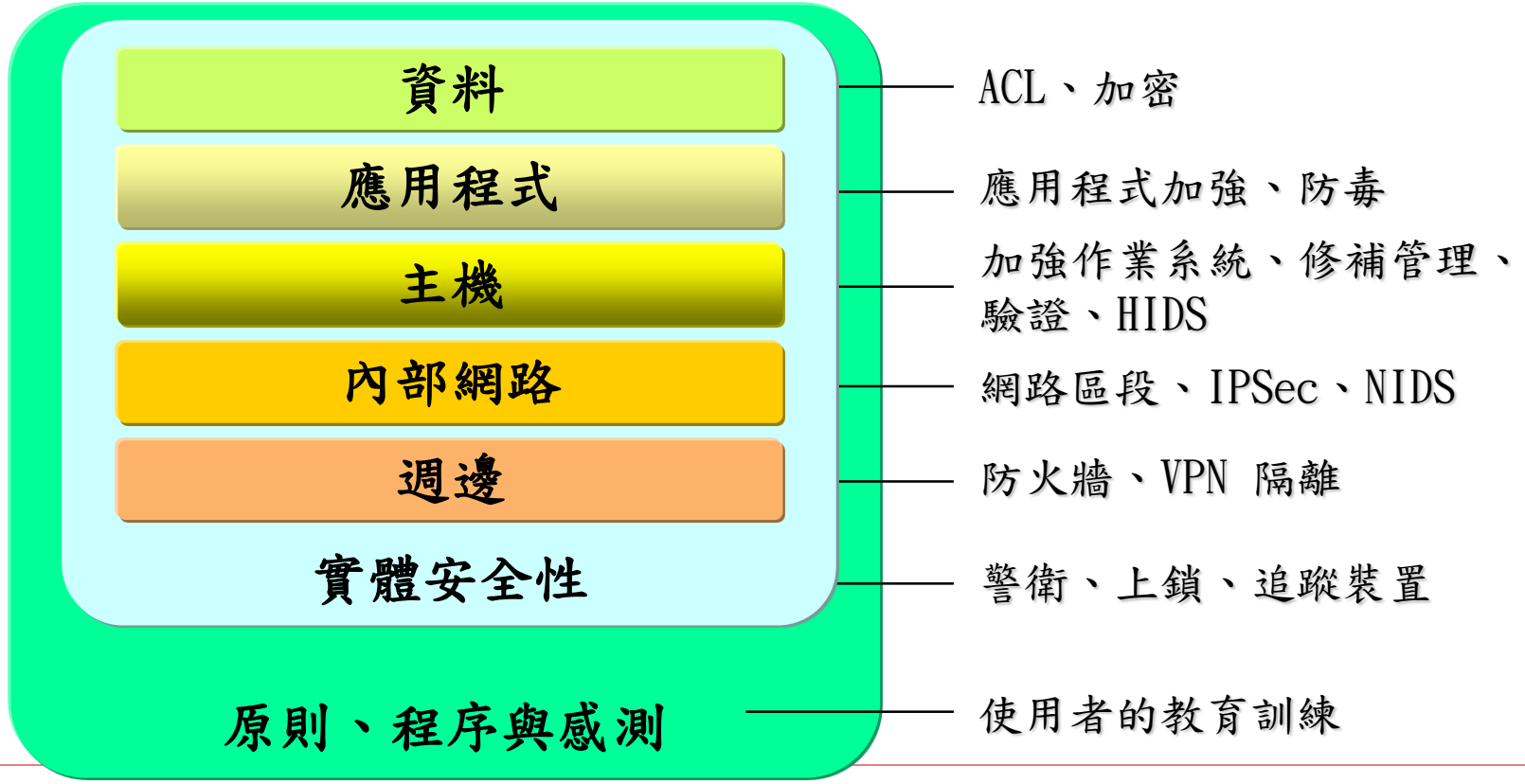
- 個人電腦備份
  - 使用Ghost等備份軟體
  - 使用Recover等還原軟體
- 伺服器的備份
  - 定期備份伺服器資料(每天、每星期…)
- 異地備份
  - ISO 文管所規範

系統被入侵後的修復工作：

- 立即拔除網路線：
- 分析登錄檔(Registry)資訊，搜尋可能的入侵途徑(使用Antispyware或WindowsDefender)：
- 重要資料備份：
- 重新安裝全新作業系統：
- 安裝可信任的防毒軟體或防火牆
- 套件的漏洞修補：
- 關閉或移除不需要的服務：
- 連上 Internet：

組織安全性的架構

- 採用分層方式：
  - 加強偵測攻擊者的風險 、減少攻擊者成功入侵的機會



10 條安全性法則

1	如果攻擊者能夠在您的電腦上執行他的程式，那麼這部電腦就不再是您的電腦。
2	如果攻擊者能夠修改您電腦中的作業系統設定，那麼這部電腦就不再是您的電腦。
3	如果攻擊者能夠自由地在您的電腦上操作，那麼這部電腦就不再是您的電腦。
4	如果您允許攻擊者將程式上傳到您的網站，那麼這部電腦就不再是您的電腦。
5	簡單的密碼會使周全的安全保護措施形同虛設。
6	只有值得信任的系統管理員，才有安全的系統。
7	加密資料的安全性取決於解密金鑰是否受到安全的保護。
8	過時的病毒掃描器只比完全沒有病毒掃描器的情況好一點。
9	在真實生活中或網路上，很難做到完全匿名。
10	科技不是萬靈丹。

結論

- 降低自己被入侵的機會～網路安全基本概念
- 實作安全性保護措施所費不貲，但比起修補安全性入侵事件的費用，可就小巫見大巫
- “便利”與”安全”是 trade-off
- 沒有絕對的安全