資訊安全之社交工程防治及個資保護

王駿瑋

講師簡介

https://www.cloudapps.org.tw/

王 駿 瑋

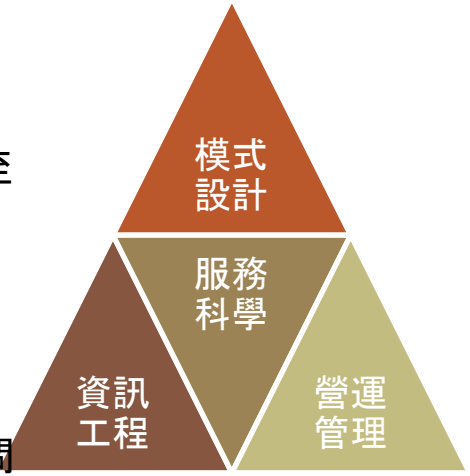
David Wang

0981603226

- 信念：創造價值
- 專業：跨領域(如右圖)
- 經歷：1997投身IT產業之3D/VR領域，之後擴張至

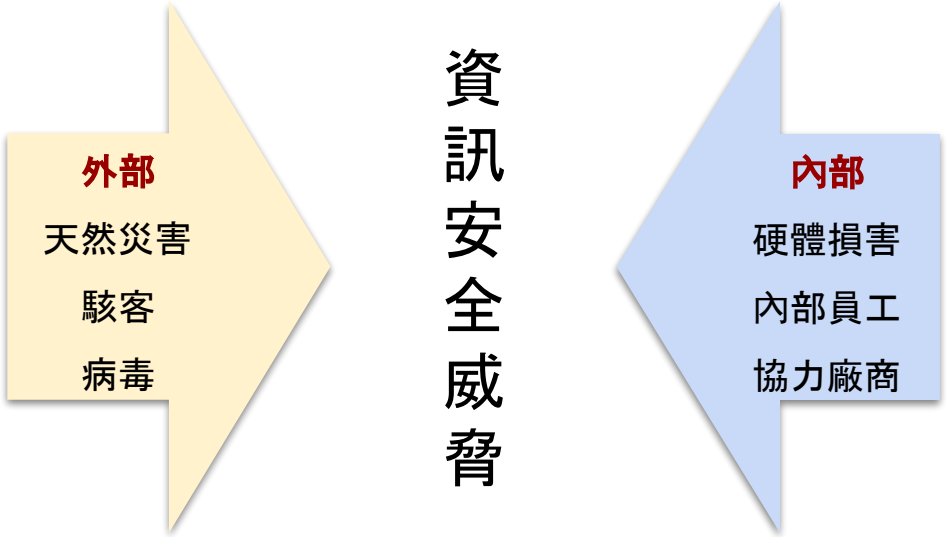
  (1)商模設計(2)電子商務(3)軟體工程

  (4)雲端運算(5)企業架構(6)人力資本
- 現職：
  - MCAP OFFICE 移動雲端應用計畫辦公室顧問
  - 娜路彎酒店集團 顧問 2014至今

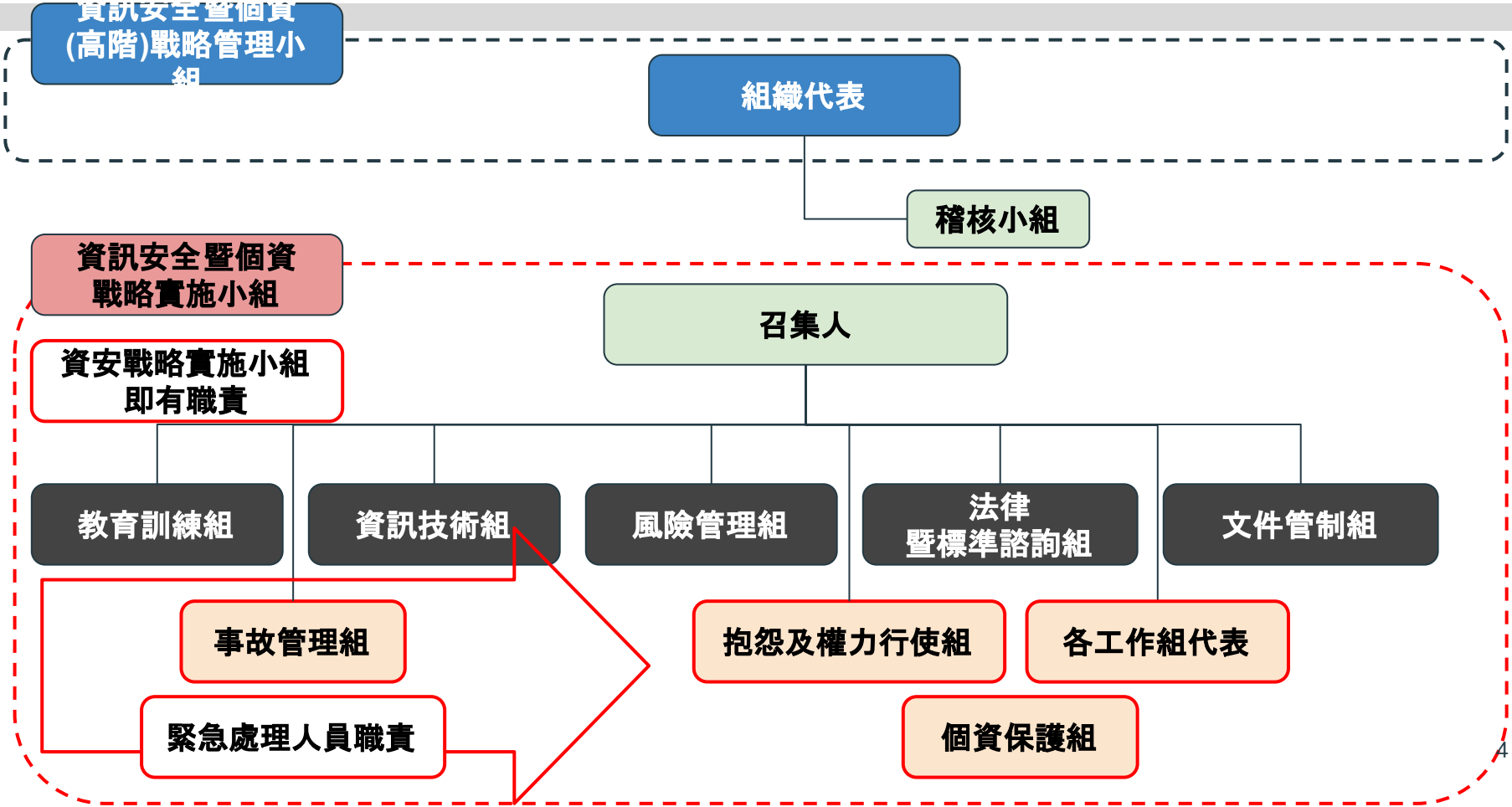


學習主題

1. 資訊安全
2. 社交工程防護
3. 個資保護



資安暨個資管理架構


資訊安全暨個資
(高階)戰略管理小組
組織代表
稽核小組
資訊安全暨個資
戰略實施小組
召集人
資安戰略實施小組
即有職責
教育訓練組
資訊技術組
風險管理組
法律
暨標準諮詢組
文件管制組
事故管理組
抱怨及權力行使組
各工作組代表
緊急處理人員職責
個資保護組

資安即國安

2018年遭受網絡攻擊的五大行業是

計算機/電子、醫療保健、商業服務、網際網路/軟體

和製造業。

《2019年網路安全報告》

台灣受攻擊次數是全球平均2倍

台灣部分不但所有惡意軟體攻擊次數與比例都是全球平均值的2倍，而且也是全球殭屍網路攻擊最多的地方，但資安投資卻沒有等比例成長，一般企業反而認為資安是支出成本

據研判，台灣常被當作網路攻擊的中繼站，經由台灣當跳板，再去攻擊別的國家，另外，很多來自共產國家的攻擊，目標都是鎖定台灣政府或企業，所以台灣遭受攻擊次數才會明顯的高。

2018年度全球有五大威脅態勢，依序為

1. 挖礦:如Coinhive(網頁挖礦程式)、Cryptoloot、Jsecoin
2. 行動
3. 殭屍網路(Botnet)-台灣被攻擊全世界排名第一，如Virut，台灣高於全球平均
4. 金融木馬攻擊:如Ramnit
5. 勒索軟體

CoinHive網頁挖礦程式

駭客廣為利用它來網頁挖礦，讓使用者在造訪網頁時，被偷偷利用用戶電腦資源以挖掘門羅幣加密貨幣。

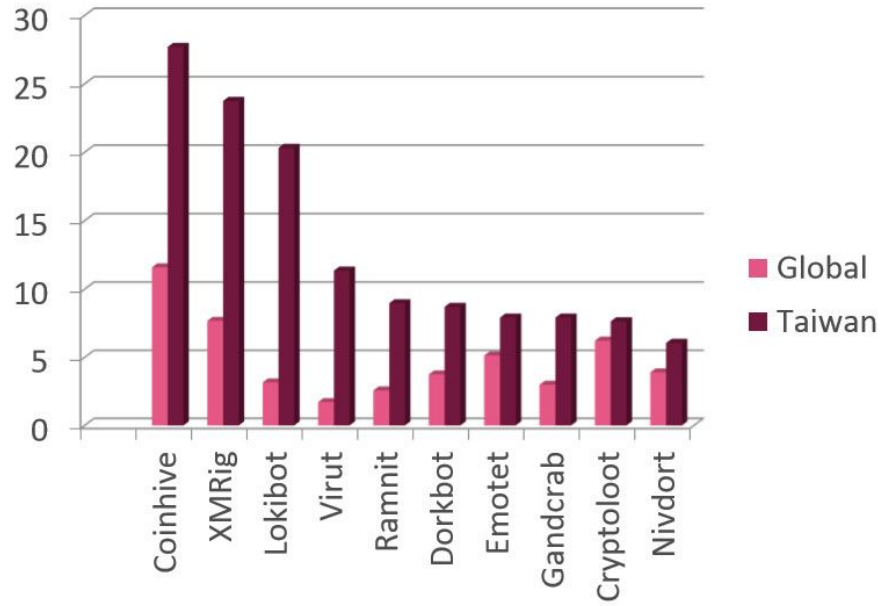
CoinHive在全球的影響程度是**24.7%**，在臺灣的影響程度則是高達**49.59%**。

2019年3月台灣前五大惡意軟體：

惡意軟體 家族名稱	描述	全球影響力	台灣影響力
Coinhive	當用戶訪問網頁時，該加密貨幣挖礦軟體可在用戶不知情或未經用戶批准的情況下，執行門羅幣加密貨幣的在線挖掘。植入的 JavaScript 會利用終端使用者機器上的資源進行挖礦，這可能造成系統崩潰。	11.59%	27.7%
XMRig	XMRig是一個開源的CPU挖礦軟體，專門挖掘Monero加密貨幣。XMRig於2017年5月首次被發現。	7.68%	23.75%
Lokibot	Lokibot惡意軟體主要由釣魚郵件發送，用於竊取不同資料，如電子郵件身分認證資料、加密貨幣錢包與FTP伺服器的密碼。	3.16%	20.32%
Virut	Virut 是網路上最主要的殭屍網路與惡意軟體散佈程式之一，用於DDos攻擊、發佈垃圾郵件、資料竊取及詐欺。此惡意軟體會透過已受感染裝置中的執行檔進行傳散。	1.71%	11.35%
Ramnit	Ramnit是一種蠕蟲病毒，透過感染抽取式磁碟機（例如 USB 快閃磁碟機或外接式儲存裝置）及上傳到公共FTP服務的文件散播。此惡意軟體能夠自我複製並感染外接式與內接式的儲存裝置；Ramnit同時可作為後門病毒。	2.57%	8.97%

% of Organizations Impacted by Malware Type in Taiwan 2019 JAN

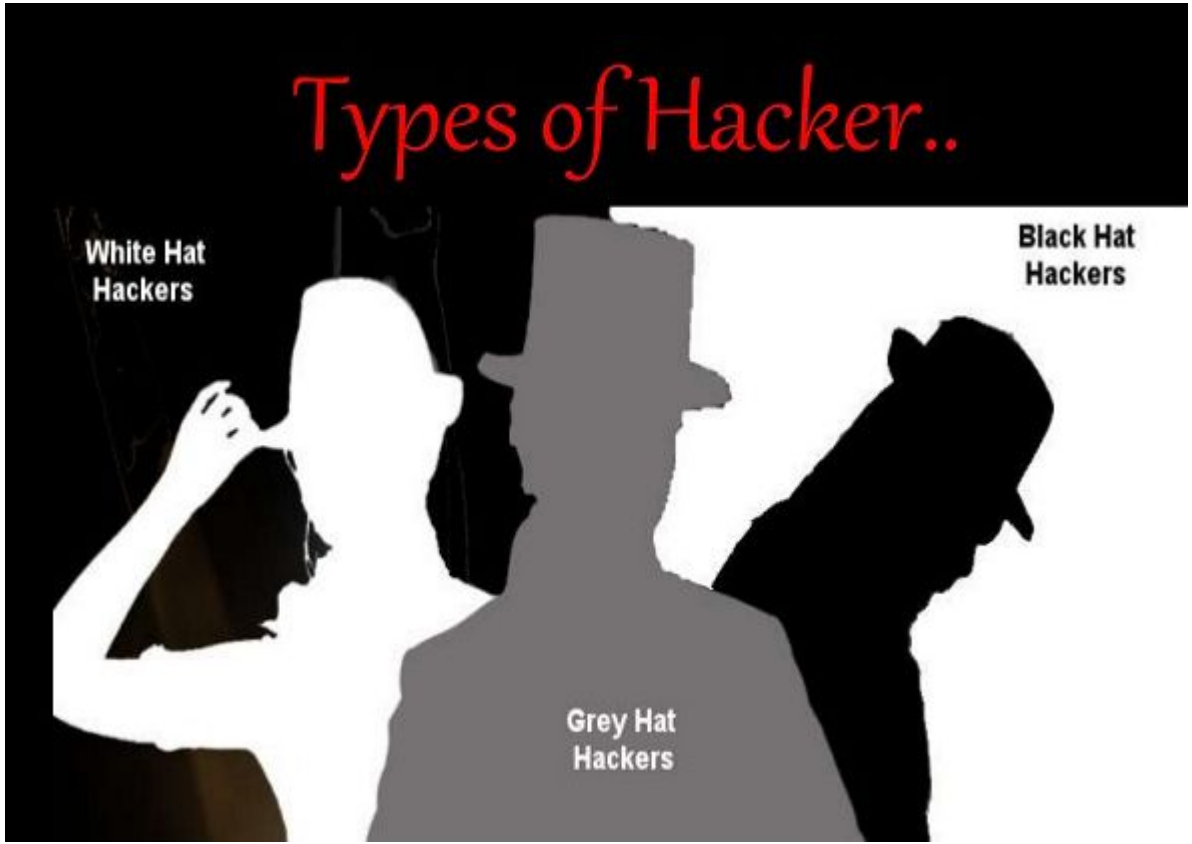
Malware Family Name	Global	Taiwan
Coinhive	11.59%	27.70%
XMRig	7.68%	23.75%
Lokibot	3.16%	20.32%
Virut	1.71%	11.35%
Ramnit	2.57%	8.97%
Dorkbot	3.75%	8.71%
Emotet	5.14%	7.92%
Gandcrab	2.99%	7.92%
Cryptoloot	6.23%	7.65%
Nivdort	3.90%	6.07%



在2019年初的最新惡意程式攻擊趨勢中，除了Coinhive仍是全球與台灣的第一，臺灣遭受XMRig、Lokibot、Virut、Ramnit的攻擊的比例，更是遠高於全球平均，幾乎都達到3倍以上。

「雲端安全」網路攻擊事件

過去一年，全球18%的組織遭遇了「雲端安全」網路攻擊事件，而最常見的事件類型包括資料外洩、帳戶盜用和惡意軟體感染。


Types of Hacker..
White Hat Hackers
Black Hat Hackers
Grey Hat Hackers

白帽(White Hat)

組織會僱用白帽駭客，有時也稱為道德駭客，去試探和入侵他們的電腦系統以確認這些系統的安全性，並提出建議以提高安全程度。他們通常會充分披露他們的研究成果，以便讓整個資安社群都能從他們所收集的資料中獲益。白帽黑客的行為是合法的，因為他們有取得客戶的許可。

黑帽(Black Hat)

黑帽駭客則是犯罪分子，他們的出發點是惡意的。在未經邀請下，他們就侵入受害者的電腦系統只為了獲取自己的利益。

灰帽(Grey Hat)

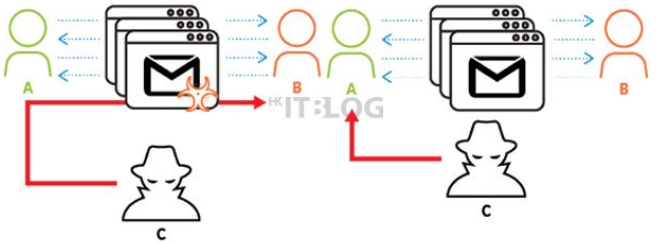
在一定程度上，激進駭客模糊了白帽和黑帽駭客間的界線。他們經常和非法行動有關，但是就如同Anonymous一樣，他們的某些行動也是好的。所以我會將激進駭客放在另外一個分類，稱為*灰帽(Grey Hat)*。

2019 年網路安全領域的

9個預測

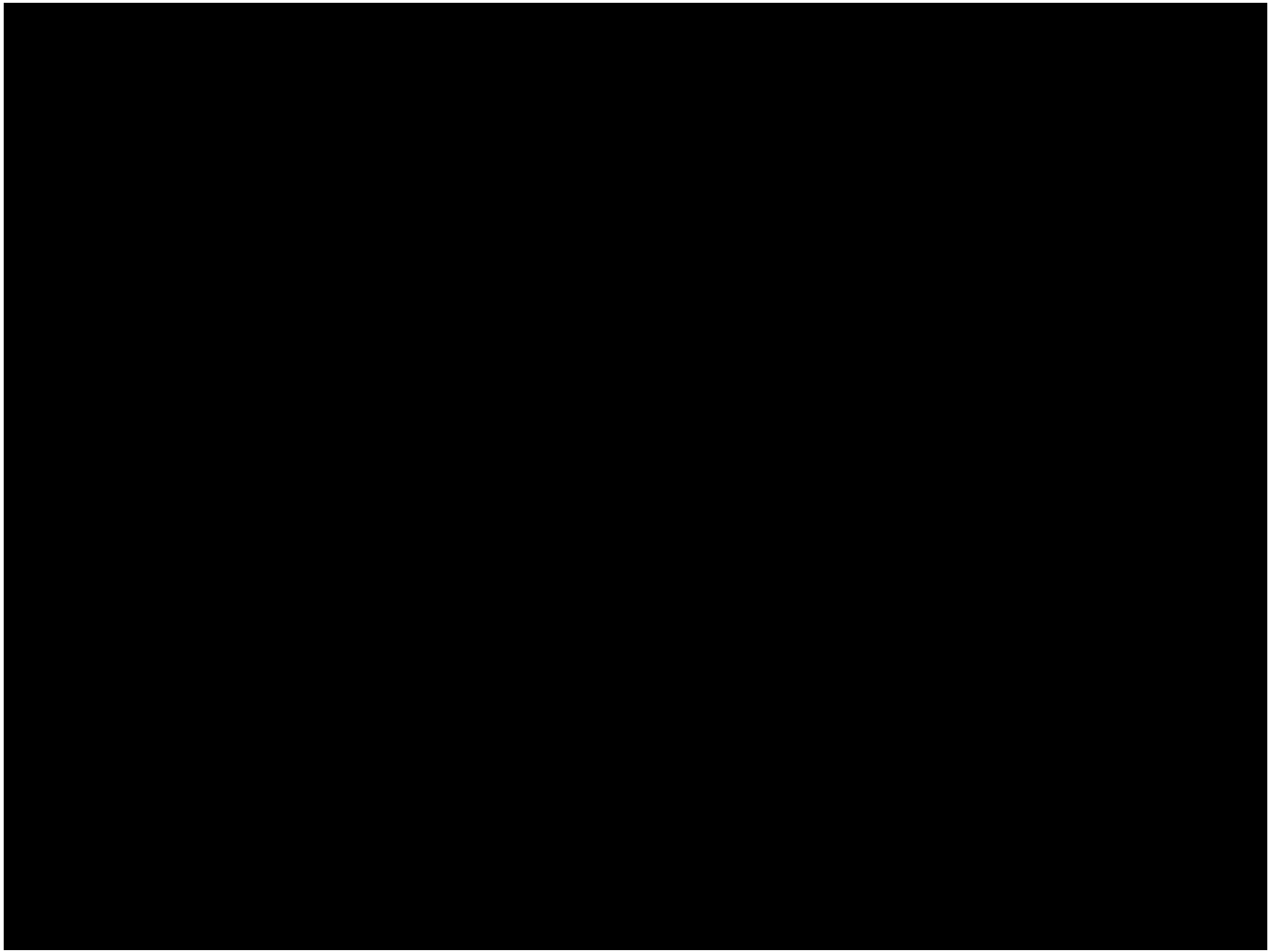
2019 年網路安全領域的10 個預測

1. 魚叉式網路釣魚更具針對性



網路釣魚（Phishing）

網路釣魚（Phishing）的起源可回溯至 1970 年代的*飛客 (phreaking)* 入侵手法，這種手法利用簡單的兒童玩具**哨子**就能非法使用電話系統，至今依然惡名昭彰。網路釣魚延續了*電話飛客*手法的傳統，同樣都是爲獲取實質利益而將專業技術用於不正當的用途。



2019 年網路安全領域的10 個預測

2. 商業詐騙無處不在

BEC金融詐騙(Business E-mail Compromise)-

企業郵件受駭/變臉詐騙

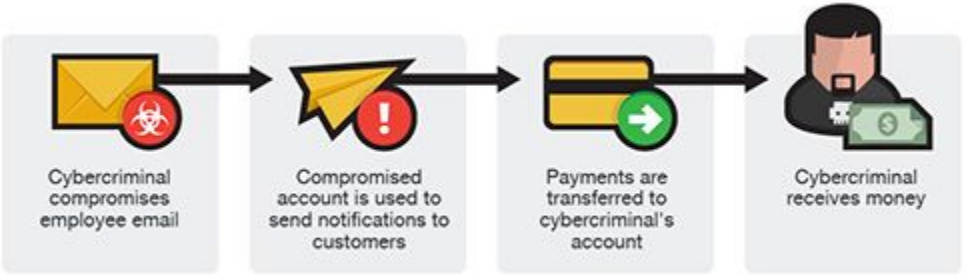
例:北市某貿易公司業務經理的電郵帳號遭仿冒，宣稱上游供應商要求變更匯款帳戶，逕行匯款，損失折合台幣近百萬元。

BEC金融詐騙(Business E-mail Compromise)

- **商業電子郵件詐騙(Business E-mail Compromise, BEC), 也簡稱BEC詐騙。**
- **受害對象 與國外供應商或業務有所往來的企業, 尤其是製造、食品、零售、運輸等傳統類型產業, 資安警覺性較低, 受害可能性高。**

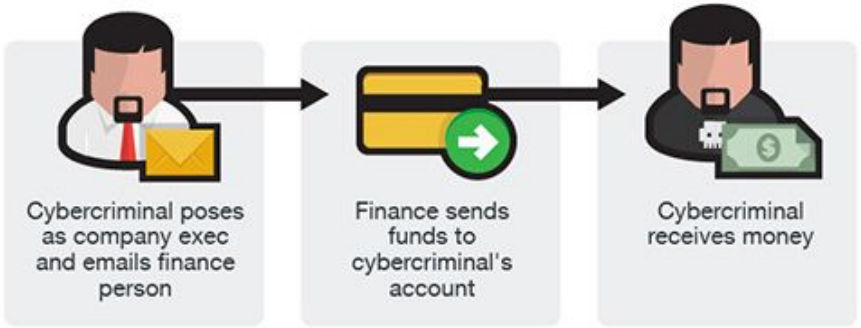
五種常見BEC詐騙方式

- **場景一　駭客假冒海外供應商以要求企業付款。**
  - 網路犯罪分子假冒國外客戶E-mail，要求變更匯款帳號，導致公司匯款至詐騙用帳戶。或者是假冒臺灣公司名義發送E-mail給國外客戶，導致國外客戶匯款至詐騙用帳戶。



五種常見BEC詐騙方式

- **場景二　駭入企業高階主管的電子郵件帳號，並假冒其名義要求企業內部的財務經理人匯款。**
- **網路犯罪分子假冒老闆E-mail，像是CEO、CIO、CFO，向公司會計要求需緊急處理某筆電匯。**



五種常見BEC詐騙方式

- **場景三　與客戶聯繫的企業窗口電子郵件帳號被駭，並假冒其名義要求供應商付款。**
  - 網路犯罪分子竊取公司企業窗口甚至負責人電子郵件，直接寄送偽造內容的信件，致使對方匯款至詐騙用帳

五種常見BEC詐騙方式

- 場景四　駭客假冒律師或事務所的代表，宣稱要處理緊急事件而要求匯款，可能選在工作日的最後一天發信給受害者。
- 場景五　同樣是駭入高層主管郵件帳號，假冒其名義發信給內部的人事或審計主管，要求彙整提供所有員工資料。

BEC詐騙流程的四個階段

階段1　確認目標

駭客從網路上或展場中，蒐集到各企業大老闆或企業窗口的聯繫資訊，以及各式相關資訊。

BEC詐騙流程的四個階段

階段2　潛伏觀察

駭客透過入侵或釣魚手法成功取得企業郵件登入帳號密碼，或透過惡意軟體側錄使得雙方通信內容一覽無遺，掌握公司財務對象、大老闆行程與交易資訊，等待時機攻擊。

BEC詐騙流程的四個階段

階段3　正式發動攻擊

在國內企業與國外廠商交易快完成前，中斷廠商之間的通訊，向是Reply-to的寄件者至竄改的假冒E-mail，並假冒出口商要求變更匯款帳號，或是假冒大老闆名義向公司會計要求匯款。

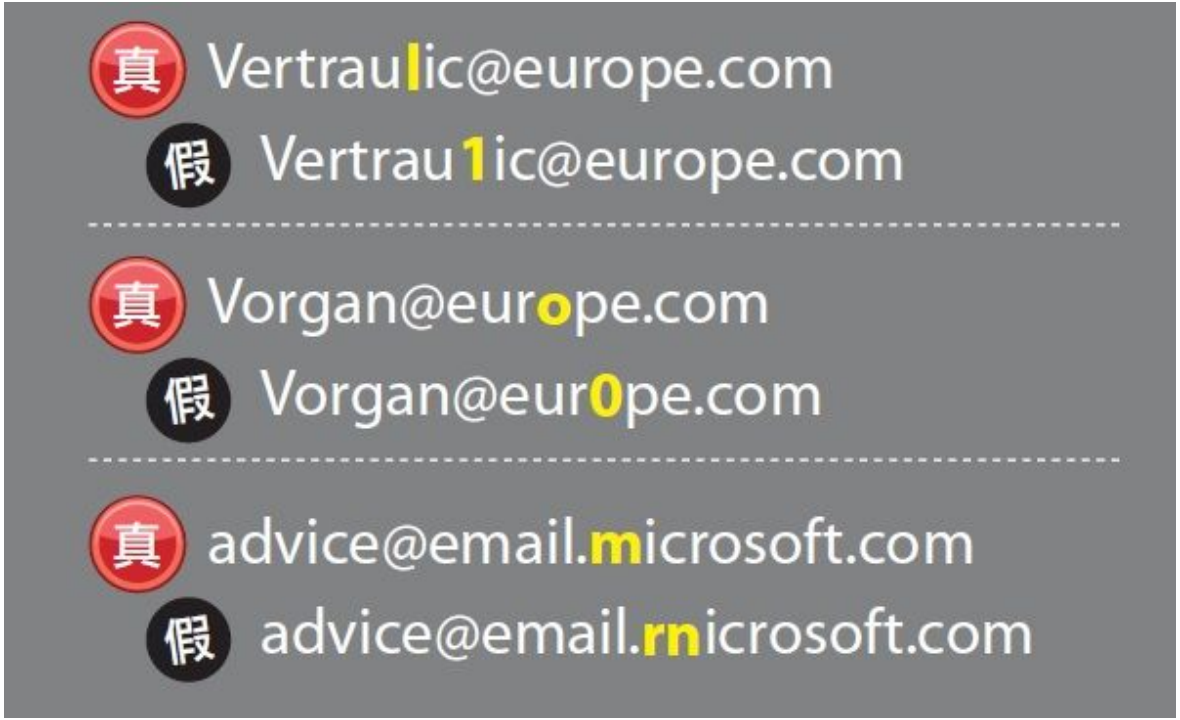
BEC詐騙流程的四個階段

階段4　取走匯款

待企業上當匯款之後，將款項提領一空，或是再匯至第三個國家地區銀行或第四個國家地區銀行。

注意竄改Email帳號的偽裝手法

竄改Email手法｜字形混淆變化



注意竄改Email帳號的偽裝手法

竄改Email手法｜字元加減變化

注意竄改Email帳號的偽裝手法

竄改Email手法｜位置調換與直接假冒

面對BEC詐騙，企業該採取的5大行動

行動1　收到匯款變更通知，務必第二管道確認：

對於經常往來國外廠商突然變更收款帳戶，或是變更出貨地等情況時，應提高警覺，確認是否為正確郵件，最好要以電話等方式聯繫，做為雙重認證機制。

面對BEC詐騙，企業該採取的5大行動

行動2　增強內部稽核流程：

合作廠商若要變更匯款資訊，企業內部是否也要制訂相關SOP，像是需要經由公司另一位人員複核。對於公司主管來信，各單位也應確認是否為正確郵件，如有金錢與重要資料交付有關，其他通訊管道聯繫確認。

面對BEC詐騙，企業該採取的5大行動

行動3　提升員工資安意識：

被害廠商疏於交易匯款確認，為深化員工的資安意識，可加強人員對釣魚郵件與BEC詐騙的認識，或是增加社交工程詐騙演練，到養成一些簡單的預防動作，例如確認電子郵件寄件來源。

面對BEC詐騙，企業該採取的5大行動

行動4　強化企業資安防護：

被害廠商疏於公司資安保護，應強化公司電腦資安維護，減少駭客入侵、木馬程式植入之機會。

行動5　檢舉報案：

一旦察覺任何詐騙事件，立即報警或向165反詐騙檢舉。

2019 年網路安全領域的10 個預測

3. 勒索軟體仍會橫行肆虐，如WannaCry

WannaCry

WannaCry（直譯「想哭」、「想解密」，俗名「魔窟」，或稱**WannaCrypt**、**WanaCrypt0r 2.0**、**Wanna Decryptor**）是一種利用NSA的「永恆之藍」（EternalBlue）漏洞利用程式透過網際網路對全球執行Microsoft Windows作業系統的電腦進行攻擊的加密型勒索軟體兼蠕蟲病毒（Encrypting Ransomware Worm）。該病毒利用AES-128和RSA演算法惡意加密用戶檔案以勒索比特幣，使用Tor進行通訊，為WanaCrypt0r 1.0的變種[12]。

WannaCry 2018重創台灣台積電

損失80億左右新台幣

預防勒索病毒,如何避免成為WannaCry/Wcry勒索蠕蟲的受災戶?

1. 立即使用隨身碟、外接硬碟或者雲端空間，備份您的重要資料。
2. 關閉Windows系統的445通訊埠，關閉網路共用資料夾。
3. 不要點擊來路不明的網站和檔案等。
4. 修補相關漏洞。
5. 開啟電腦作業系統的Windows Update，隨時升級系統與修補漏洞。

預防勒索病毒,如何避免成為WannaCry/Wcry勒索蠕蟲的受災戶?

另外請務必注意:如果您的電腦遭攻擊，建議千萬不要乖乖繳納贖金，因為這會助長犯罪,且不保證檔案可以取得回來。

2017 年 05 月 12 日

台灣、中東、日本和數個亞太地區(APAC)國家也都顯示出大量的感染。WannaCry 勒索病毒感染影響了各個產業，包括了醫療保健、製造業、能源(石油和天然氣)、科技、食品和飲料、教育、媒體和通訊以及政府。

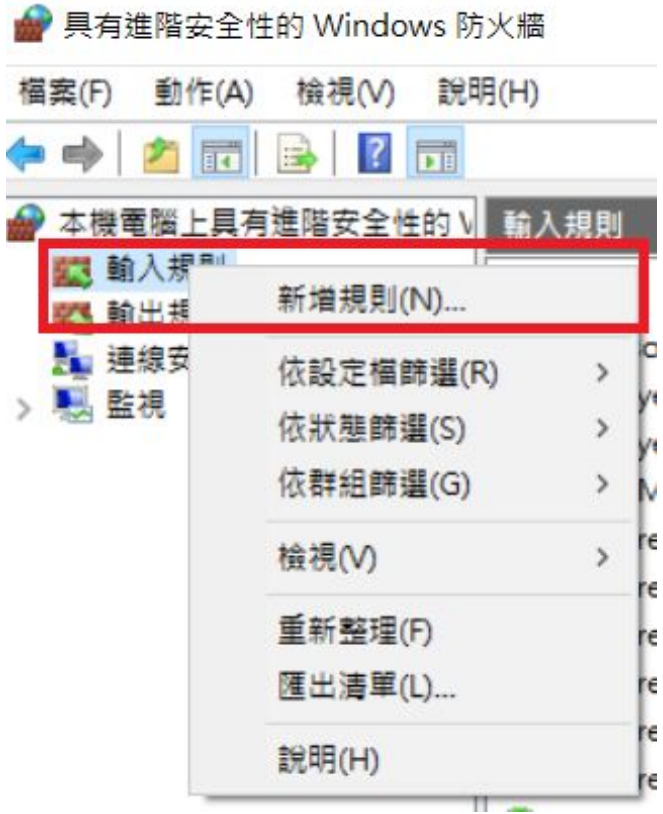
勒贖通知要求用比特幣支付300美元

關閉445通訊埠之參考步驟：

1、從控制台中選擇「Windows 防火牆」，並點選左方「進階設定」：

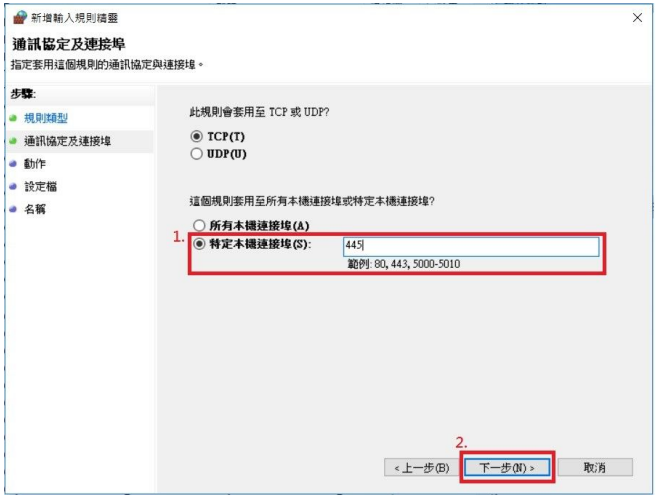
關閉445通訊埠之參考步驟:

2.於「輸入規則」點選右鍵選擇「新增規則(N)...」



關閉445通訊埠之參考步驟：

3、選擇建立「連接埠(O)」的規則，並輸入要關閉的445。Ps, 務必使用半型輸入。

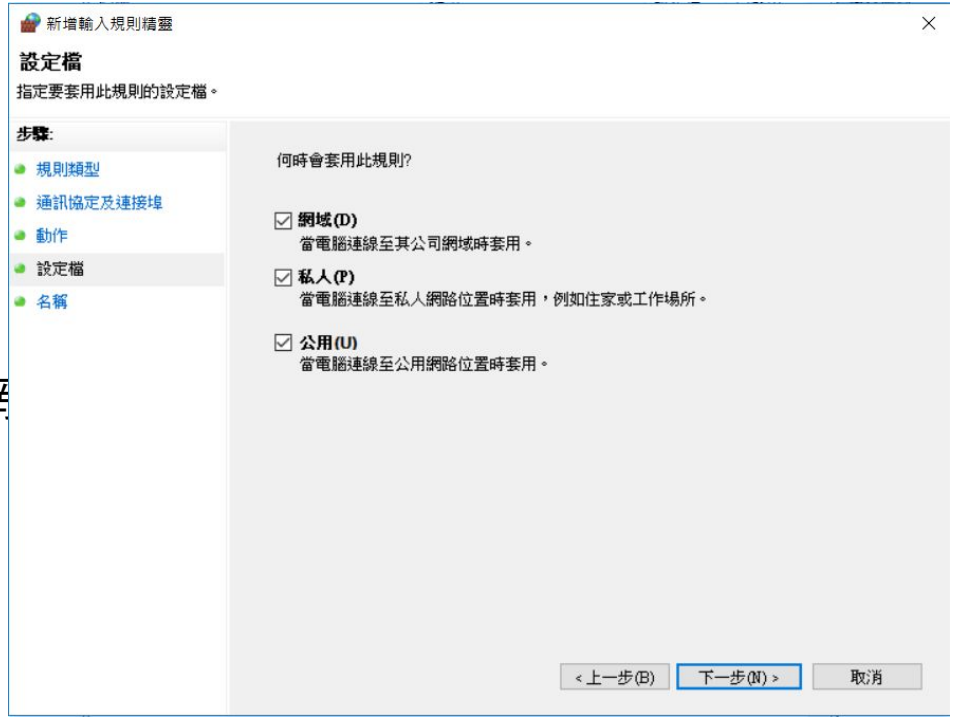


關閉445通訊埠之參考步驟：

4、選擇「封鎖連線」，並建議於所有網路環境套用規則。

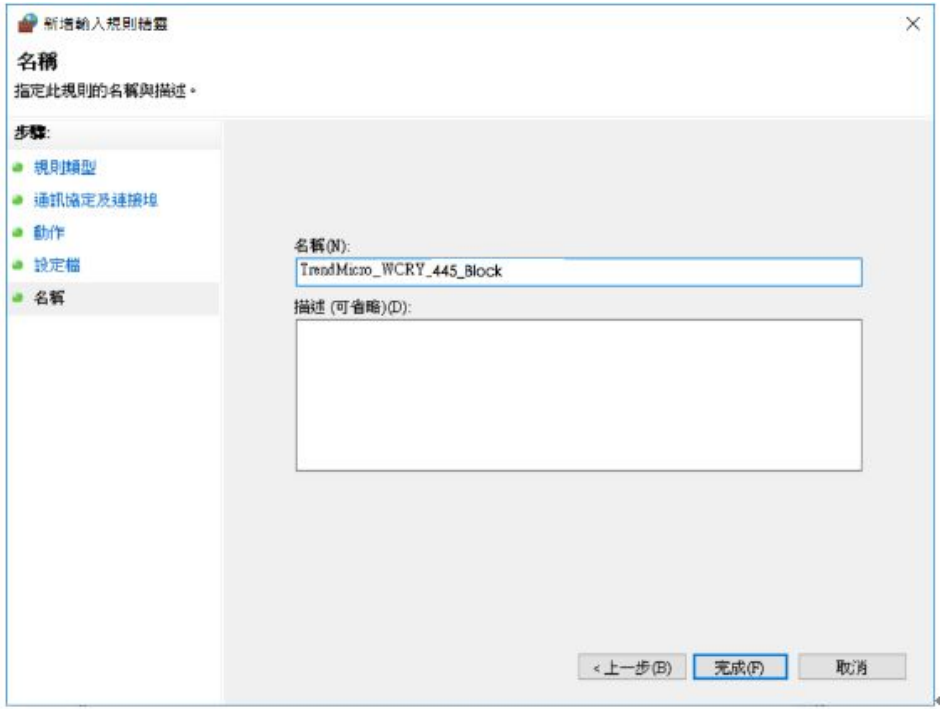
關閉445通訊埠之參考步驟：

4、選擇「封鎖連線」，並建議於所有網路環境套用規則。



關閉445通訊埠之參考步驟：

5、針對規則命名，建議名稱可與事件或規則內容有關，避免忘記其用途。範例：TrendMicro_WCRY_445_Block



2019 年網路安全領域的10 個預測

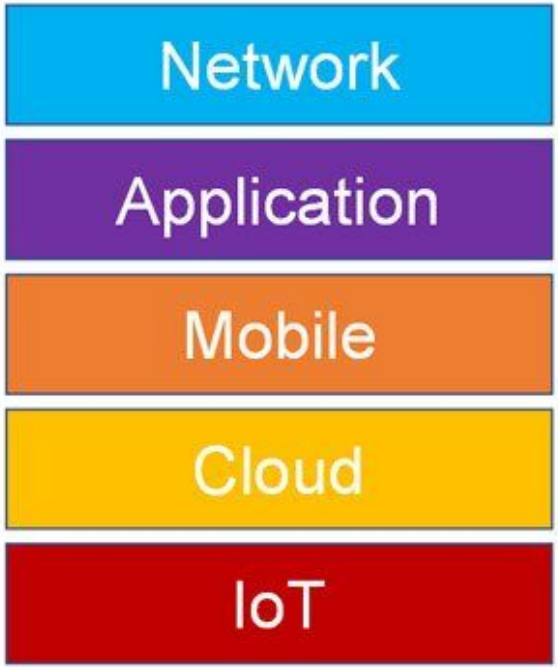
4. 伴隨物聯網

(IoT,Internet of Thing)**的魔咒**

2019 年物聯網發展

延續 2018 年熱潮，從與 AI、5G、雲端的結合，到數位孿生、數據經濟應用，乃至道德、資安、民主化的規範面等，更加成熟聚焦於衍生應用和資安基礎的建立。若以政策法規、市場需求與技術發展為觀察指標，物聯網在 2019 年持續多元發展，應用更實務落地，為廠商帶來實質效益，也為城市帶來防護能耐。

The Current IoT Security Problem



- services, encryption, firewall, input…
- authN, authZ, input validation, etc.
- insecure APIs, lack of encryption, etc.
- AuthSessionAccess
- **Net + App + Mobile + Cloud = IoT**

圖片來源: RSA Conference 2015

Mirai事件的爆發

Mirai是一款惡意軟體，針對執行Linux的系統，使之成為被遠端操控的「殭屍」，透過殭屍網路進行大規模網路攻擊。一群網路攻擊者利用Mirai所發動的DDoS攻擊，創下每秒Tb級的攻擊流量，另外，他們也成功癱瘓Dyn網路服務商的DNS服務。

Mirai事件的爆發

同時，此次DDoS攻擊有效地擊中要害，並且造成北美各大網站受到影響，使用者無法瀏覽，而這些攻擊，則是來自高達10幾萬臺被Mirai所感染的IoT裝置（IP Camera），作為殭屍網路(Botnet)利用。

殭屍網路

殭屍網路（Botnet，亦譯為**喪屍網路**、**機器人網路**）是指駭客利用自己編寫的分散式阻斷服務攻擊程式將數萬個淪陷的機器，即駭客常說的傀儡機或「肉雞」（肉機），組織成一個個命令與控制節點，用來傳送偽造包或者是垃圾封包，使預定攻擊目標癱瘓並「阻斷服務」。通常蠕蟲病毒也可以被利用組成殭屍網路。

殭屍網路常見的功能

- 各種C&C模式：集中式或分散式
- 攻擊類型：垃圾郵件、DDoS、資料竊取
- 使用更多通訊協定：IRC、HTTPS
- 使用有效的躲避技術：SSL、VoIP通道
- 多樣化的召集機制：寫死的IP地址、分散式DNS服務

殭屍網路常見的功能

殭屍網路也被用來攻擊銷售端點(PoS)和其他支付系統。

以下是惡名昭彰的殭屍網路:

- ZBOT/ZeuS – 銀行資料竊取病毒
- KOOBFACE – 最成功的Web 2.0殭屍網路
- WALEDAC – 惡名昭彰的垃圾郵件殭屍網路病毒

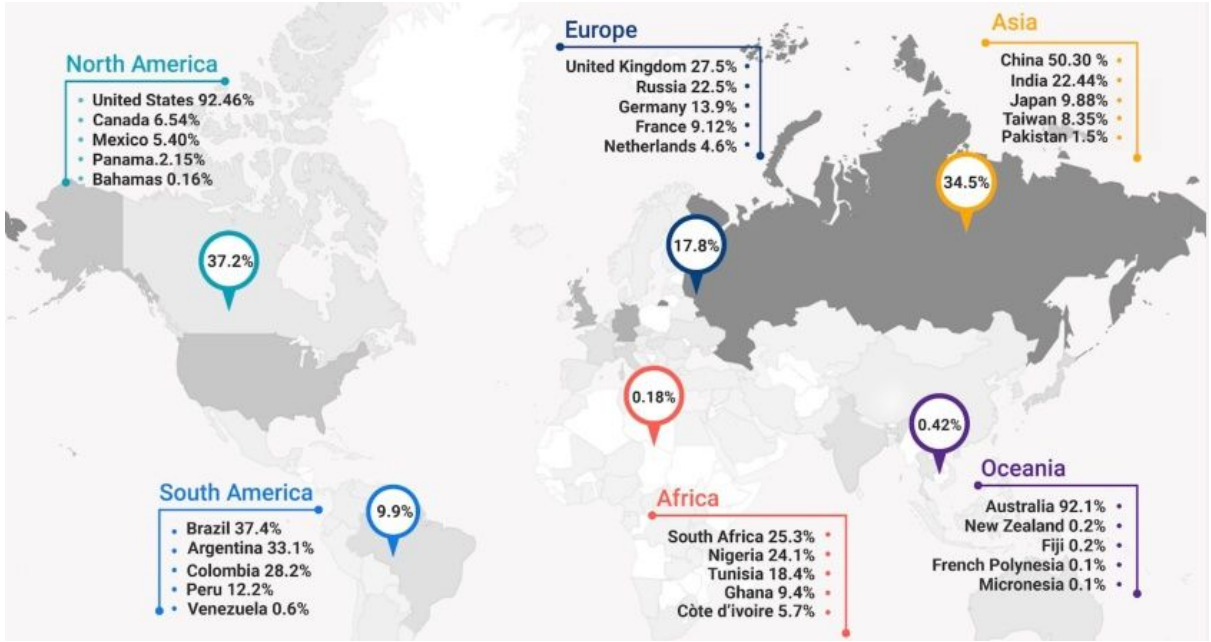
有害軟體	傳播性	可控性	竊密性	危害級別
殭屍網路	具備	高度可控	有	全部控制:高
木馬	不具備	可控	有	全部控制:高
間諜軟體	一般沒有	一般沒有	有	資訊泄露:中
蠕蟲	主動傳播	一般沒有	一般沒有	網路流量:高
病毒	用戶干預	一般沒有	一般沒有	感染檔案:中

2019 年網路安全領域的10 個預測

5. 數據洩漏 – 網路之隱痛

By BusinessFocus on 20 Dec 2018

2018年确认数据泄漏12,449起，比上年增加424%

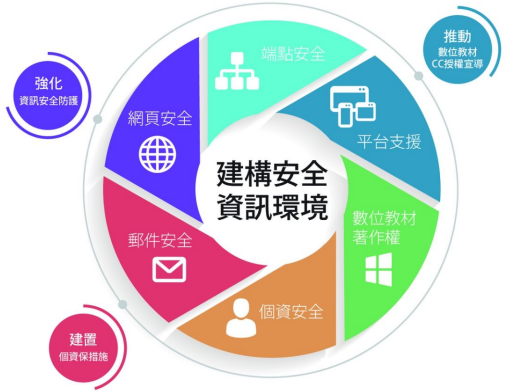


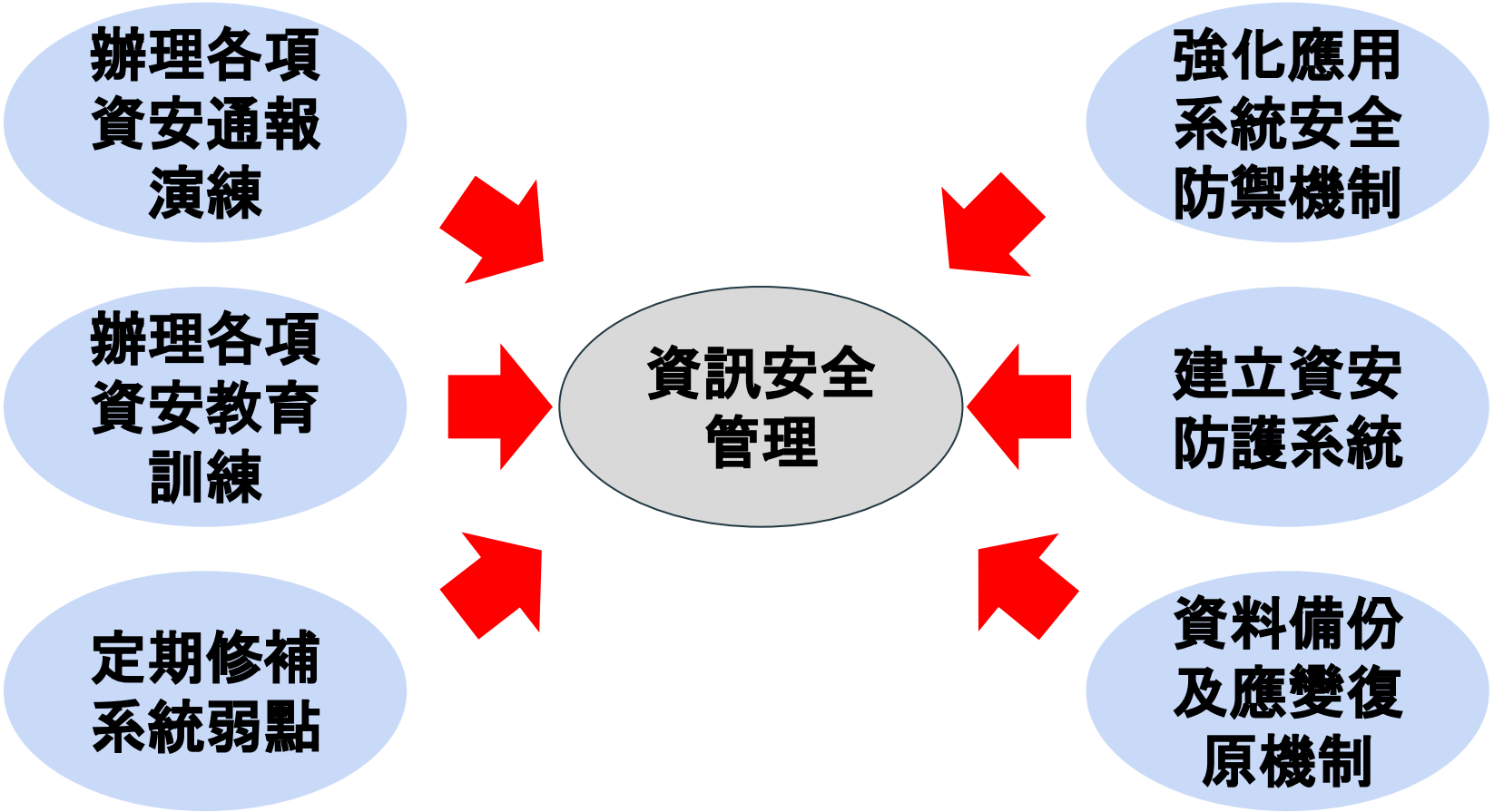
2019 年網路安全領域的10 個預測

6. 關於漏洞的老話題

2019 年網路安全領域的10 個預測

7. 資安教育訓練正逢其時




辦理各項資安通報演練
辦理各項資安教育訓練
定期修補系統弱點
資訊安全管理
強化應用系統安全防禦機制
建立資安防護系統
資料備份及應變復原機制

資訊安全風險管理參考架構

2019 年網路安全領域的10 個預測

8. 安全回應會更為智慧化

2019 年網路安全領域的10 個預測

9. 區塊鏈(Blockchain)安全

剪不斷理還亂

繼蒸汽機、電力及電腦後
之第四次革命

第四次革命

施瓦布(Klaus Schwab)於去年世界經濟論壇前出版《第四次工業革命》一書，將近年出現的最新科技及技術，包括人工智慧(AI)、機器人、物聯網(IoT)、自動駕駛汽車、3D列印、生物技術及區塊鏈(blockchain)稱為第四次工業革命，或稱「工業四．○」。

區塊鏈是什麼?

從字義來看，區塊鏈(Blockchain)是由區塊(Block)、鏈條(Chain)兩個英文所組成。它是一種開放的技術規格，類似網際網路的技術標準；區塊鏈必須應用到生活或商業模式，才能產生價值，也必須要搭配相關工具及服務。

區塊鏈的原理是什麼?

想像看看，家裡連上網路的每一台電腦硬碟就是系統中的一個區塊，當透過金鑰加密更動資料後，區塊鏈上的每一台電腦硬碟都會跟著同步更動，就如同一本全球性的網路帳簿，紀錄系統內的每一筆交易。

區塊鏈與現在有何不同?

現在交易模式都要有第三方控管，且要建置大型資料庫，區塊鏈是去「中心化」，將資料存放在不同電腦裡，並相互監控數據，紀錄一變動是不可逆的、且具可塑性，也就是說可保護個人隱私，但交易過程透明。

區塊鏈未來如何應用?

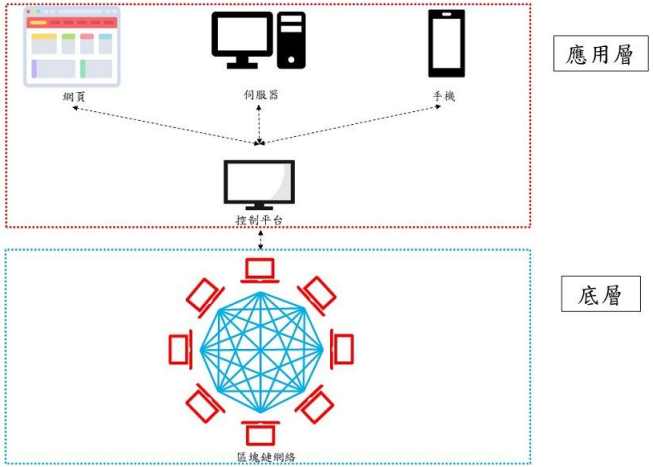
區塊鏈技術的應用，目前以比特幣交易最知名，等同在一本全球比特幣網路帳本上記錄所有交易；區塊鏈應用非常廣泛，目前以金融業最積極，因可保護個人隱私，可大幅度降低銀行的後台成本出錯可能。

區塊鏈有哪些類型?

主要有實名、匿名制兩種類型，匿名制以比特幣為代表，像紙票一樣不記名，但也因匿名會有洗錢的疑慮，目前大多區塊鏈發展的商業模式都採實名制。

區塊鏈的資訊安全防護最主要需考量兩個重點

- 區塊鏈系統本身的安全防護機制
- 架構於區塊鏈系統上的應用服務安全防護機制



區塊鏈的資訊安全防護層

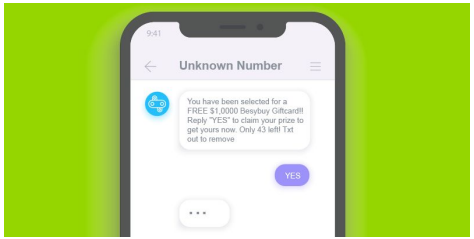
社交工程防護

常見的社交工程心理

1. 恐懼。
2. 服從。
3. 貪婪。
4. 樂於助人。

社交工程攻擊類型

Phishing 網絡釣魚	Spear Phishing 魚叉式網路釣魚	Vishing 語音釣魚
Smishing 釣魚短信	Mining Social Media 挖掘社交媒體	



社交工程常應用之題材

1. 政治：例如選舉候選人的新聞。
2. 色情：例如某個知名影星外洩的清涼照。
3. 贈品、抽獎：例如通知中獎訊息。
4. 影音媒體：例如最新熱門影片或單曲下載。
5. 系統管理：例如更新作業系統的修補程式，或通知某帳號之密碼已即將過期需變更密碼。

手法---利用人性弱點，如貪心、好奇心...

- 電子郵件
  - 假冒寄件者
  - 有惡意程式(木馬)的附件或超連結
  - 令人感興趣的郵件主旨或內容引發點擊附件
- 偽裝作業系統修補程式或軟體更新程式

預防社交工程引發資安事件

- 正確的電子郵件使用習慣
  - 檢查寄件者身分的真偽
  - 確認信件內容的真實度
  - 不要輕易開啟來路不明的郵件(附件,超連結和圖片)
  - 關閉郵件預覽功能
  - 未經確認的郵件不可轉寄

個資保護

個人資料包括:

姓名　出生年月日　身分證號碼　護照號碼　特徵

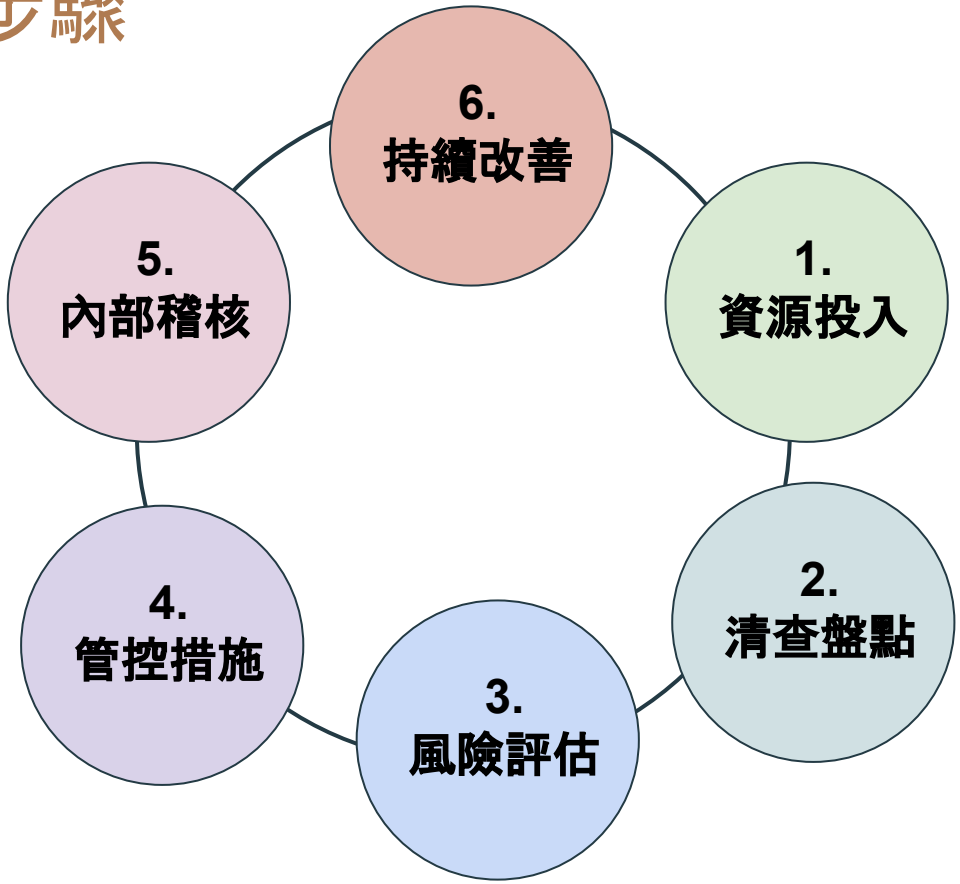
指紋　婚姻　家庭　教育　職業　病歷

醫療　基因　性生活　健康檢查　犯罪前科

特種個人資料

聯絡方式　財務狀況　社會活動　其他可直接或間接識別該個人的資料

個資保護六步驟



個資保護六步驟之1.資源投入

投入軟硬體資源，成立個資保護推行小組

任何部門只要其作業與個資法所規定的個資蒐集、處理、利用和國際傳輸有關，就必須在個資因應小組有代表人。

成立個資保護推行小組的目的

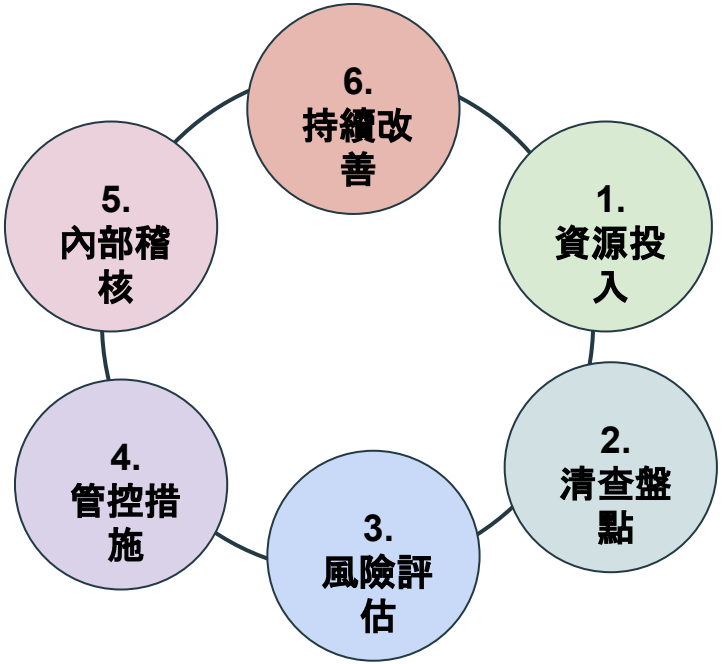
成立個資保護推行小組

法律面	制度面	標準面
符合法規 要求	持續落實 PDCA循環	國際標準的 共通作法

持續落實個人資料保護

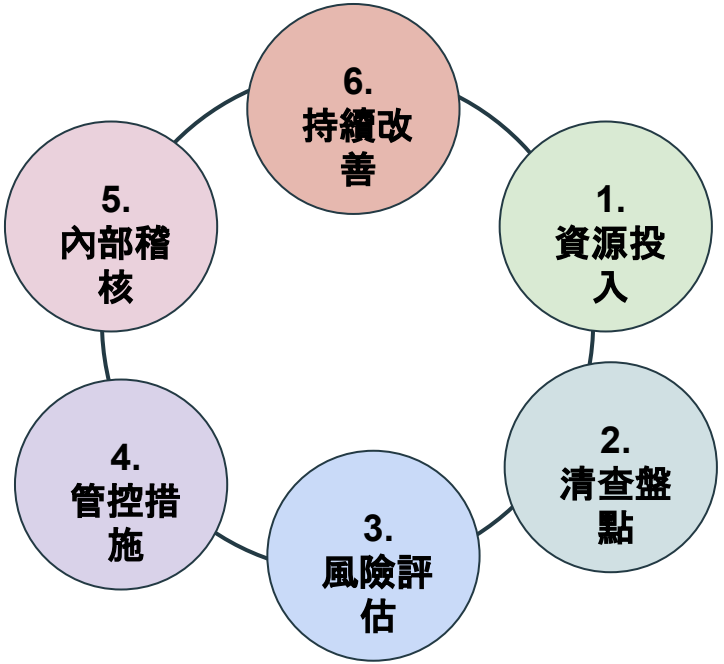
個資保護六步驟之2.清查盤點

確認個資檔案及蒐集、處理、利用個人資料之流程、劃定個資保護範圍並建立個資檔案清冊及流程說明。



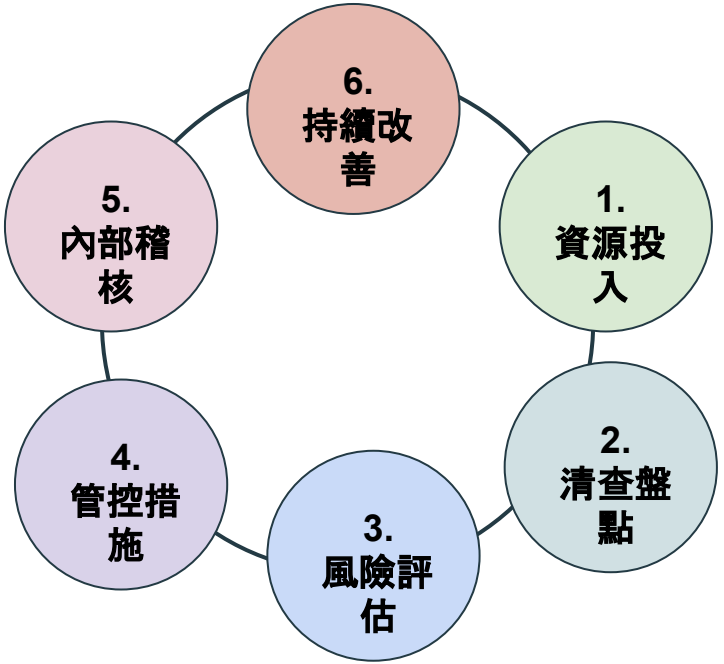
個資保護六步驟之3.風險評估

請納入管理範圍之個人資料，評估可能面臨的風險



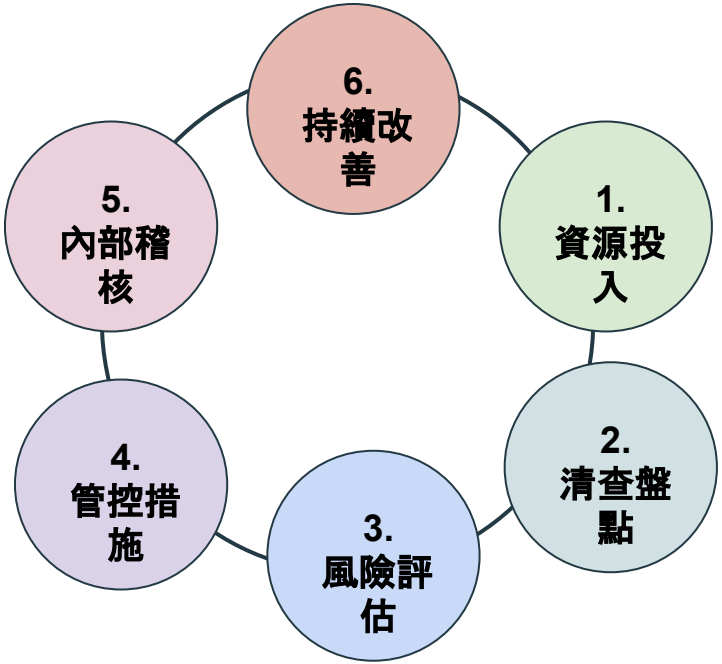
個資保護六步驟之4.管控措施

依據風險評估訂定並執行必要且適當的安全管控措施。



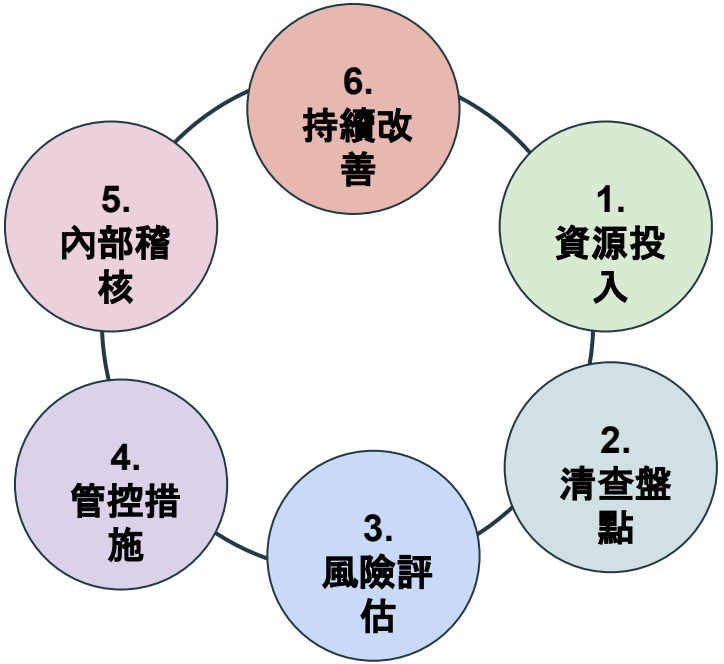
個資保護六步驟之5.內部稽核

定期以內部查核工作確保個資保護與管理是否合法規要求。

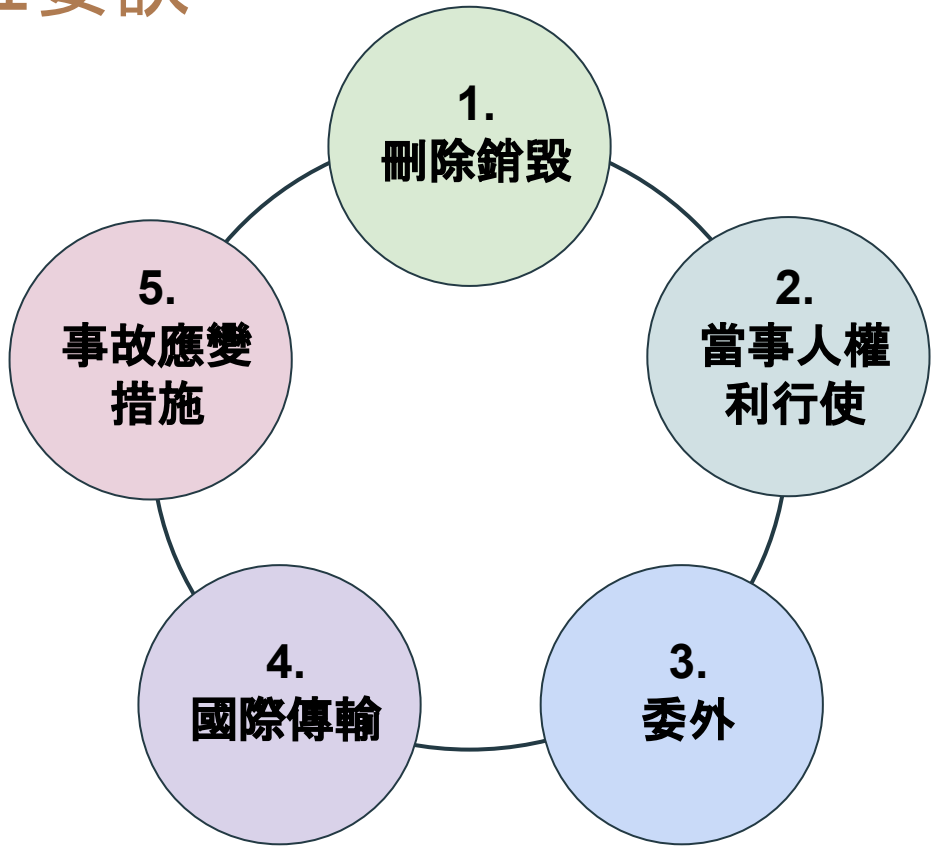


個資保護六步驟之6.持續改善

改善不符合事項，並調整及修正管控措施。

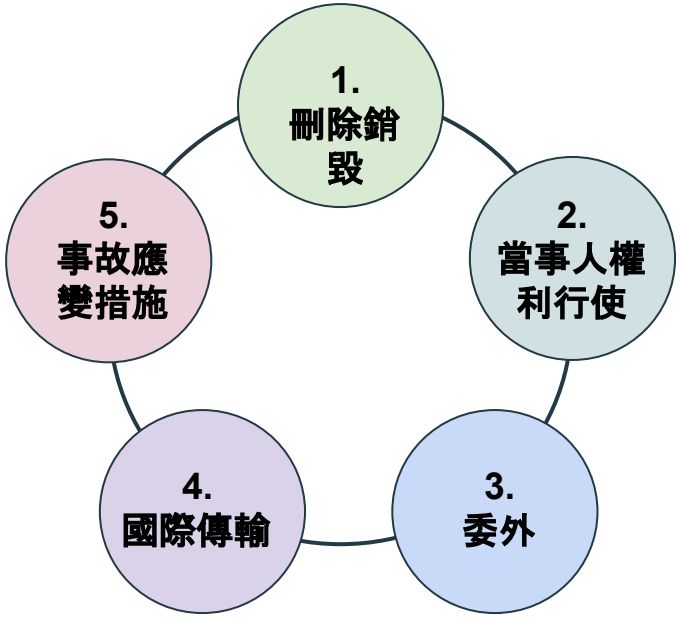


個資管理五要訣



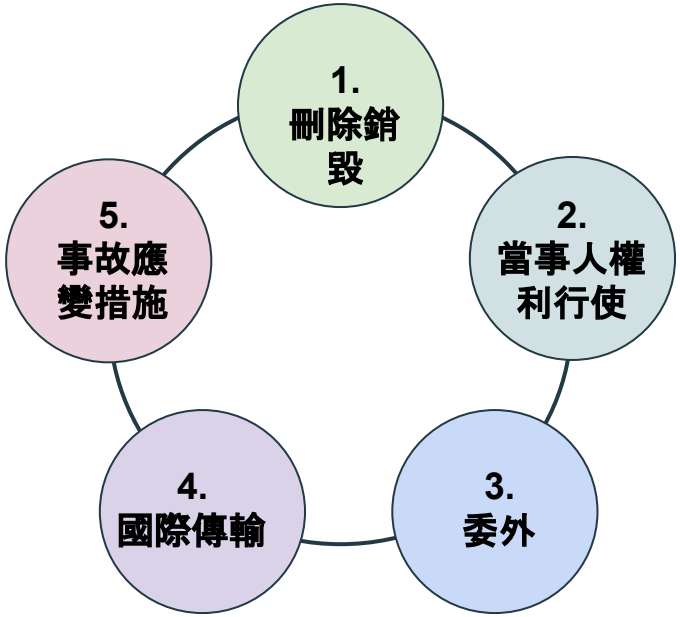
個資管理五要訣之1-刪除銷毀

組織應主動或依據當事人請求，刪除/銷毀已屆保存期限或無保留之個資。



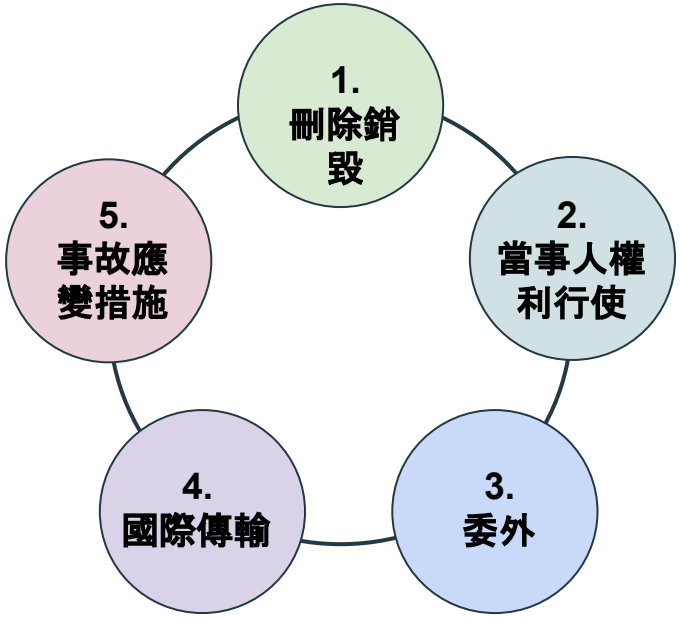
個資管理五要訣之2-當事人權利行使

個資法賦予個資當事人查詢、閱覽、請求製給複製本，並得要求停止蒐集、處理或利用，已及刪除個資之權利。



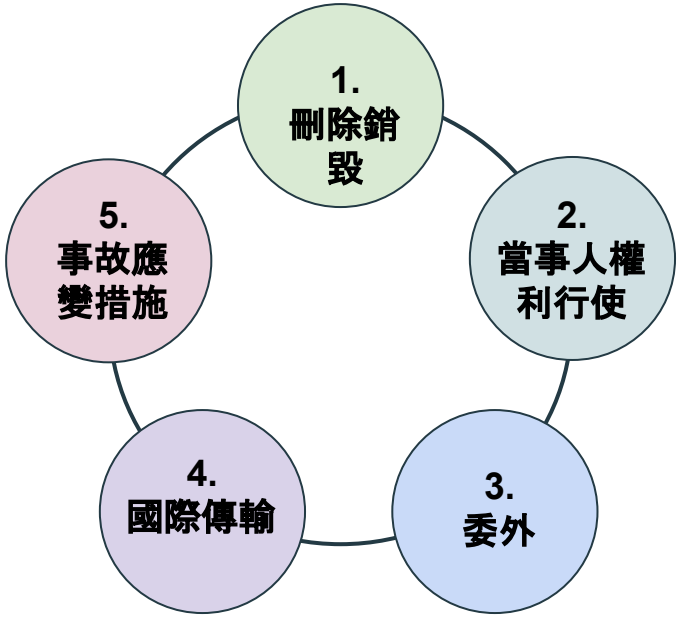
個資管理五要訣之3-委外

組織將涉及個資檔案之業務委託外部廠商時，應善盡監督義務。



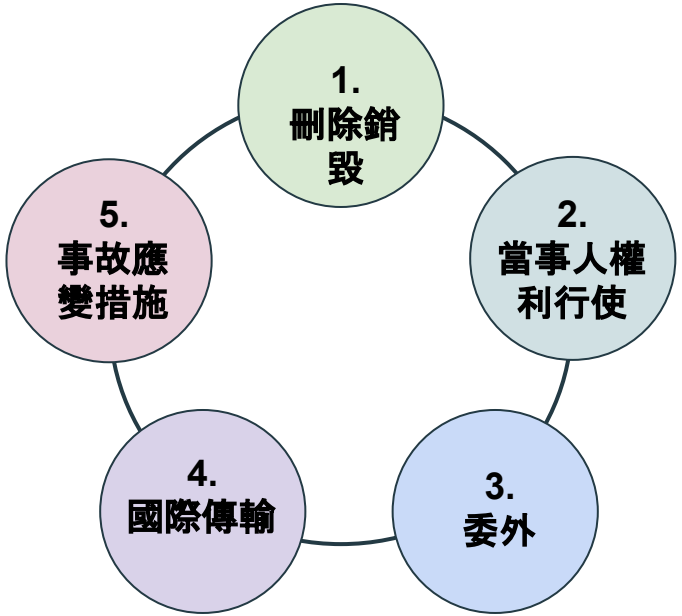
個資管理五要訣之4-國際傳輸

組織於進行個資檔案國及傳輸時應注意是否有違反個資法規範，以及國際個資傳輸規範。



個資管理五要訣之5-事故應變措施

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。



Thank you