全球資通安全威脅趨勢分析與案例分享

輔導顧問師 蘇志哲 (Arthur Su)

ISO27001/BS10012/ISO27701主導稽核員

風險管理決策與危機證書/資訊安全防護證書

Mobile: 0905-051517

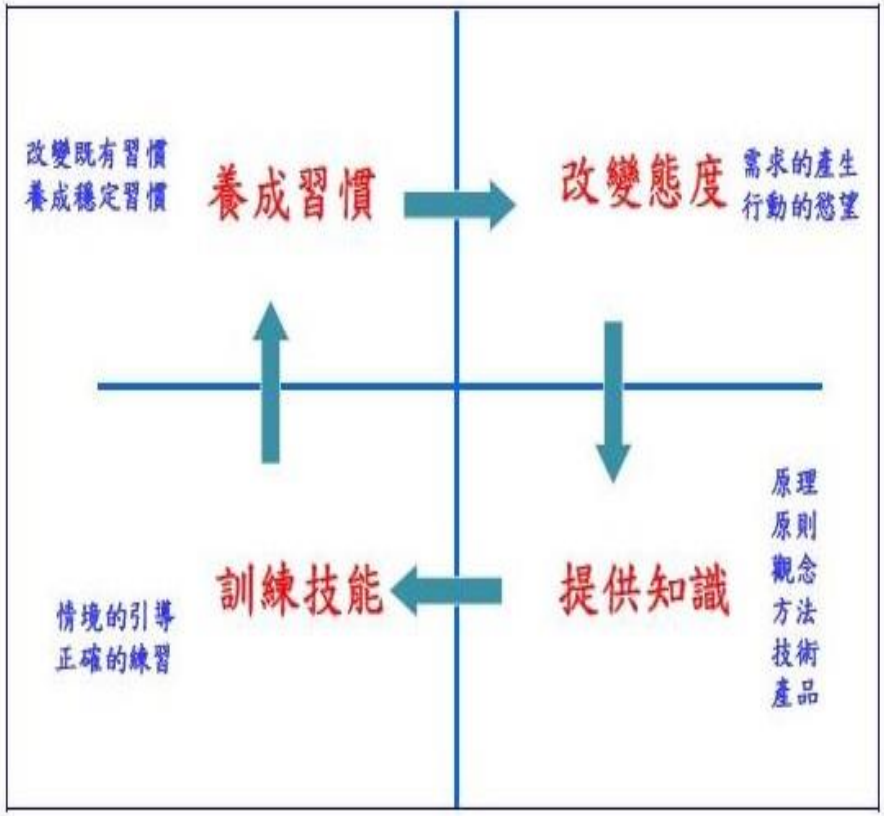
E-mail: suchihche@gmail.com.tw

SafeLink 博創資訊科技股份有限公司

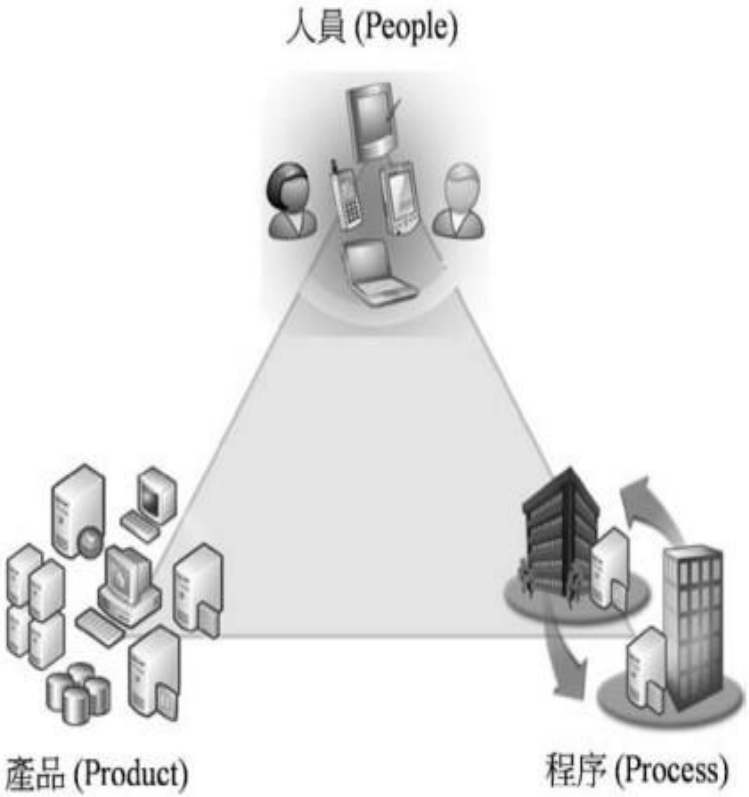
課程大綱(Agenda)

- 前言
- 全球資通安全威脅趨勢
- 案例探討及分享
- 造成資料外洩的原因
- 政府資安威脅趨勢
- 政府資安威脅案例分享

前言

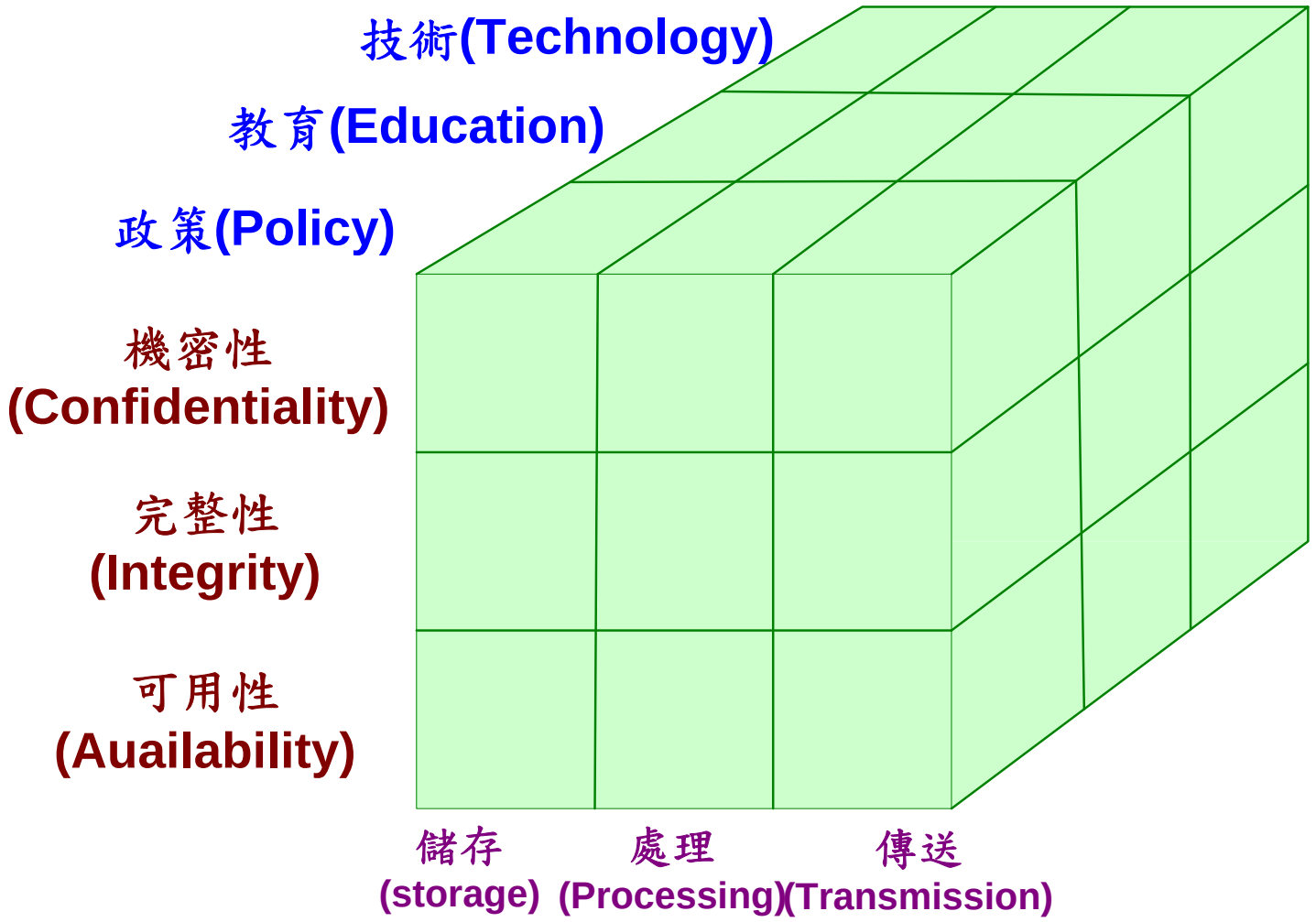


認知訓練方法論架構圖



資訊安全的三個 P

前言


技術(Technology)
教育(Education)
政策(Policy)
機密性
(Confidentiality)
完整性
(Integrity)
可用性
(Auailability)
儲存
(storage)
處理
(Processing)
傳送
(Transmission)

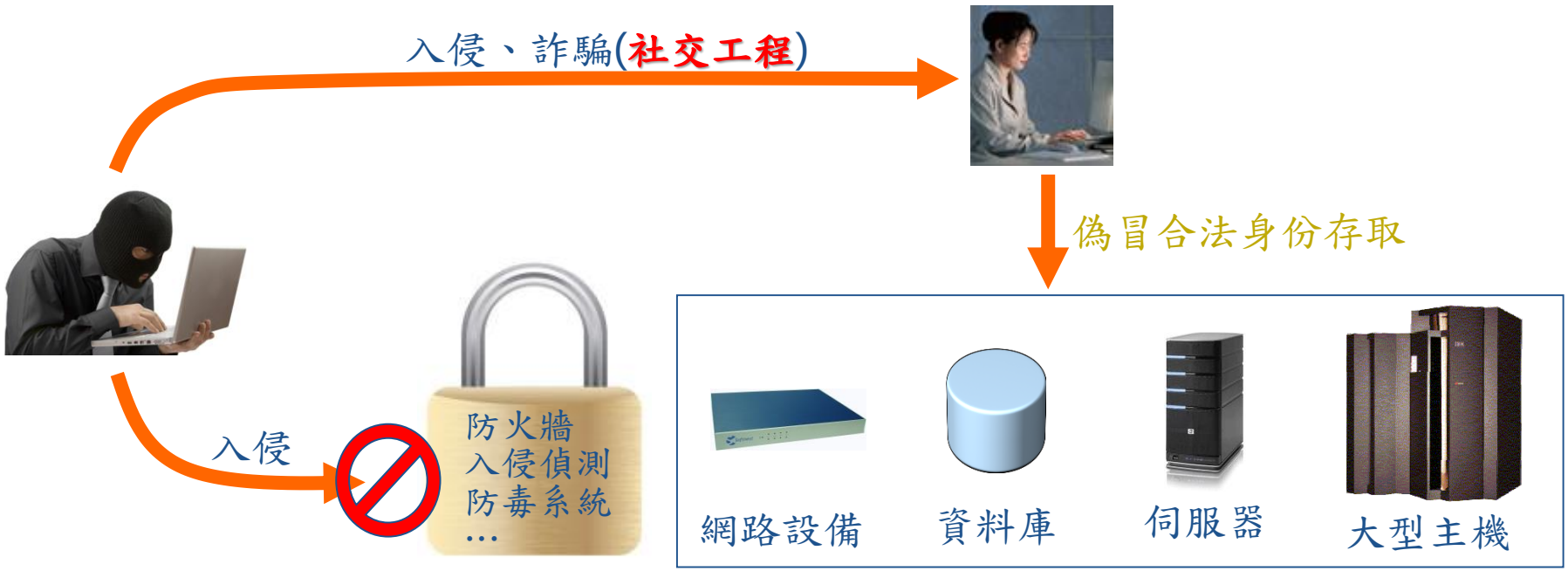
- 前言
- ✓全球資通安全威脅趨勢
- 案例探討及分享
- 造成資料外洩的原因
- 政府資安威脅趨勢
- 政府資安威脅案例分享

全球資通安全威脅趨勢

- 綜整110年全球資安威脅與相關研究報告，歸納全球資安威脅趨勢

資訊安全面面觀

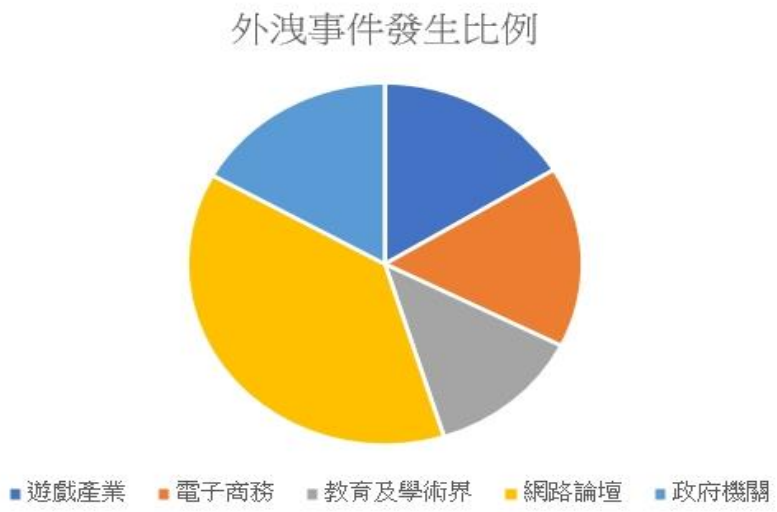
- **The Security is as strong as the weakest link !**
  （系統安全強度＝ 最弱環節）



- **駭客攻擊順序**
  - **先設法取得使用者的帳號、密碼**
  - **再偽冒合法使用者登入重要主機、系統，進行竊密或破壞**

個人資料與憑證外洩攻擊白熱化

- 分析外洩事件發生的產業別
  網路論壇占27.5%位居第一
  政府機關占12.2%居次
  遊戲產業占11.8%
  電子商務網站占11.7%
  教育及學術界則占9.2%



- 網路上流竄之個人身分資料
  有37%係遭駭客攻擊而外洩，其餘63%係因意外曝光。

勒索軟體攻擊風險激增

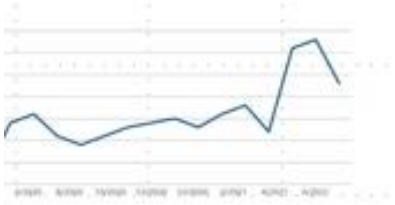
- 什麼是勒索軟體

  勒索軟體為一種網路病毒，旨在控制使用者的電腦或加密資料，隨後要求使用者支付贖金，以恢復正常作業。

- 勒索軟體的感染途徑為何？

  勒索軟體會透過需經由使用者安裝的病毒檔案散佈。

  當病毒入侵網路後，就能在裝置之間橫向蔓延。在此情況下，這類勒索軟體又稱為蠕蟲。



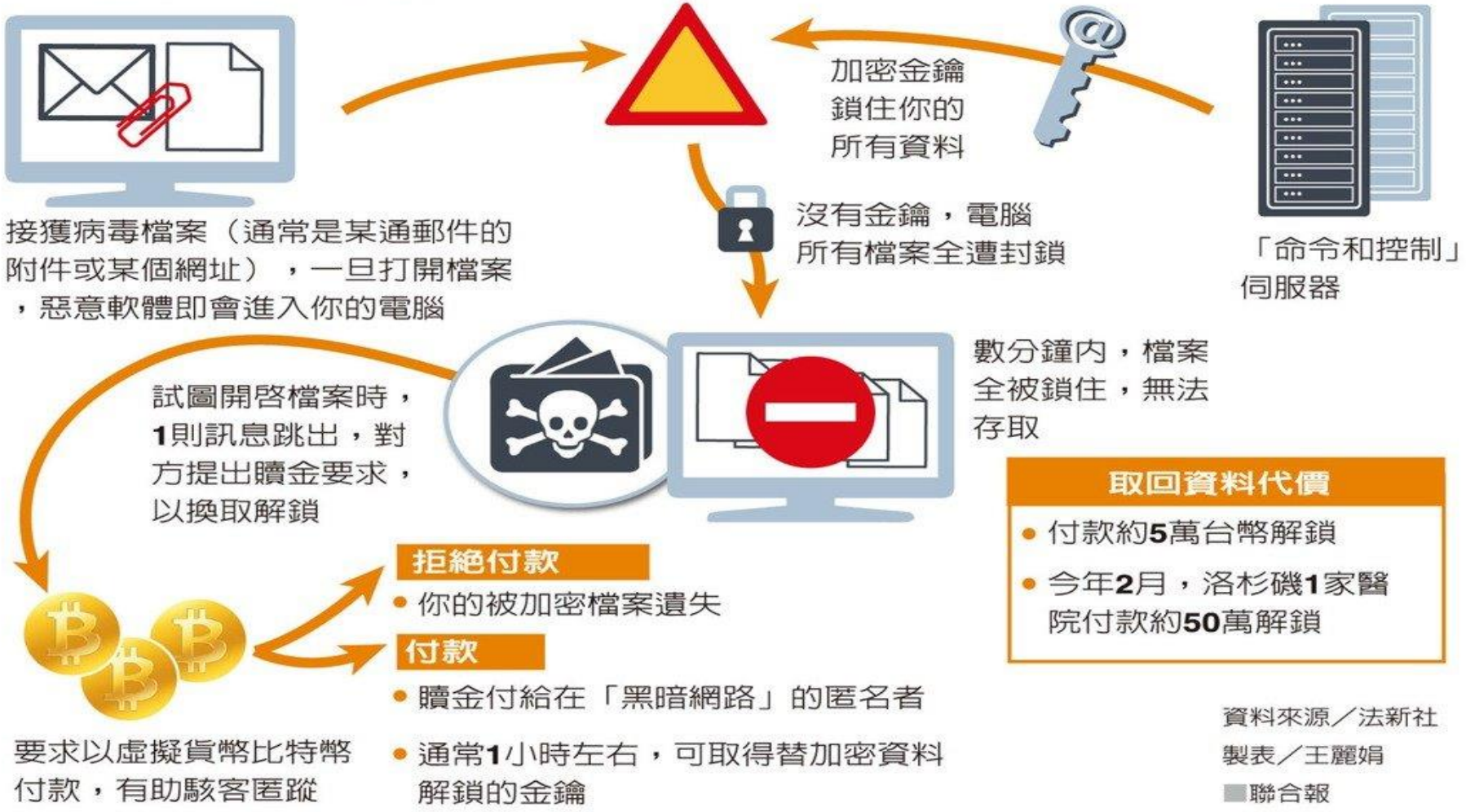
ENISA
109/4~110/6
勒索事件統計

澳洲醫療網路遭勒贖攻擊

勒索軟體的威脅

勒索軟體：駭客綁架資料方法

透過惡意軟體封鎖電腦資料



資料來源／法新社
製表／王麗娟
聯合報

勒索程式

- 勒索程式（ransomware）
  - 又名流氓軟體
  - 將你電腦上的照片、文件等檔案加密
  - 並且在電腦中留下聯繫方式，要求受害者交付贖金，才能取得將檔案解密的解密金鑰

勒索病毒Wanna Cry來勢洶洶

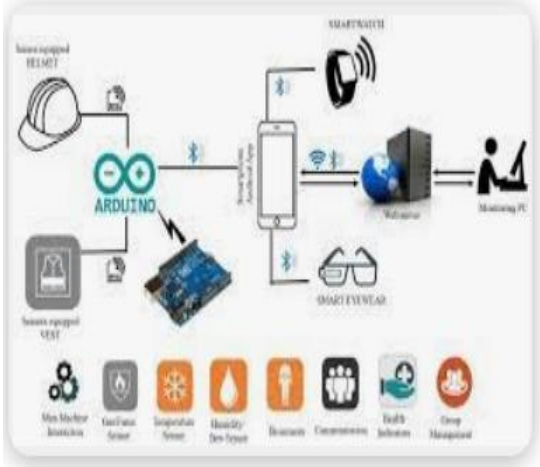
勒索軟體–警告及防患


Ooops, your files have been encrypted!
What Happened to My Computer?
Can I Recover My Files?
How Do I Pay?
午間新聞
12:02:07
醫療系統遭勒索 電腦凍結影響廣


圖片來源: 維基共享資源，作者：Jericho

IoT與行動式設備資安弱點威脅升高

- 什麼是IoT（Internet of Things，IoT）
  指連結到互聯網的設備網絡，可以記錄或接收數據，而不需要任何人機互動。
- 為什麼物聯網 (IoT) 如此重要？
  連結到互聯網的設備可以通過感測器收集訊息，並發送此訊息以進行分析發出動作指令或從過程中學習。
  連結到互聯網可以使任何設備變得更智能。



IoT與行動式設備資安弱點威脅升高

物聯網的五大主要應用

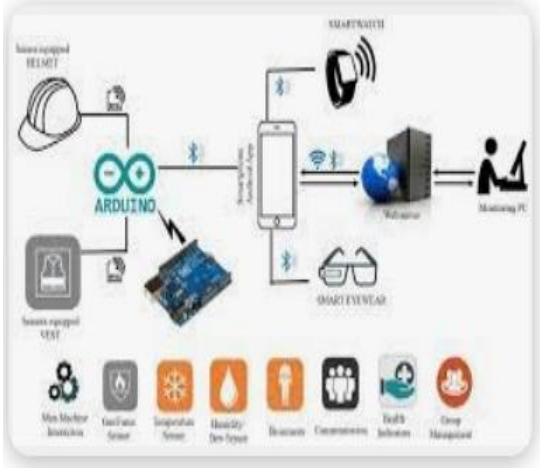
IoT在工廠、城市、身體、零售、以及家庭的主要應用面向與市場價值為何?

	定義	主要應用	潛在價值
工業4.0	工廠透過物聯網驅動轉型，創造一個更實時、更具效率、且更有效益的產線。	• 營運管理 • 提高產能 • 預測性修復	1.4兆-3.3兆美金
智慧城市	智慧城市利用物聯網更好的處理城市的安全、健康、交通、經濟發展等相關領域。	• 智慧交通 • 自動駕駛 • 智慧建築 • 智慧基礎建設	9700億-1.7兆
智慧健康	通過追蹤人體各個健康指標，以及整個智慧健康生態系統，讓人類變得更加健康。	• 身體健康狀況追蹤 • 遠程醫療 • 相關智慧醫療科技	5500億-1.77兆
智慧零售	通過自動化零售的後台與前台流程，以及提高整體供應鏈可視性，建立更具效率的零售組織。	• 自動結帳 • 存貨管理 • 倉儲自動化	6500億-1.15兆
智慧家庭	聚焦在讓家居變得更安全、方便、節能、以及降低支出等面向提消費者的居住品質。	• 家居自動化 • 能源管理 • 安全保護	4400億-8300億

IoT與行動式設備資安弱點威脅升高

- IoT 物聯網裝置的資安風險
  - 蒐集豐富大量的資料
  - 虛擬與實體環境的密切關連
  - 架構集中化

- IoT 的三大攻擊面
  - 裝置
  - 通訊管道
  - 應用程式和軟體

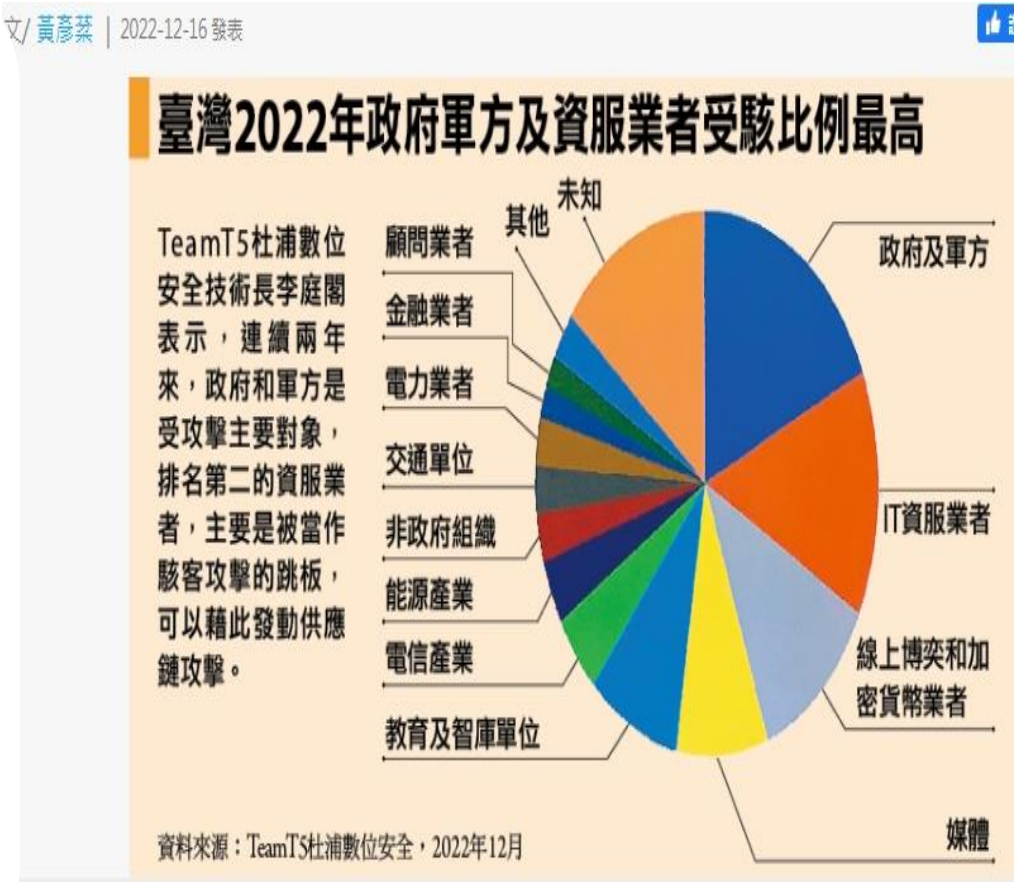


IoT與行動式設備資安弱點威脅升高

- 如何確保 IoT 安全？
  - 所有蒐集的資料和儲存的資訊都必須清楚規劃
  - 每個連上網路的裝置在設定時都確實達到安全
  - 資安策略應該建立在駭客已入侵的假設上
  - 每一個裝置都必須受到妥善的實體防護

APT鎖定式攻擊竊取機敏資料

- 鎖定之攻擊目標？
  - 金融業者
  - 國防單位
  - 社群媒體
  - 政府機關
  - 企業高度仰賴之雲端服務



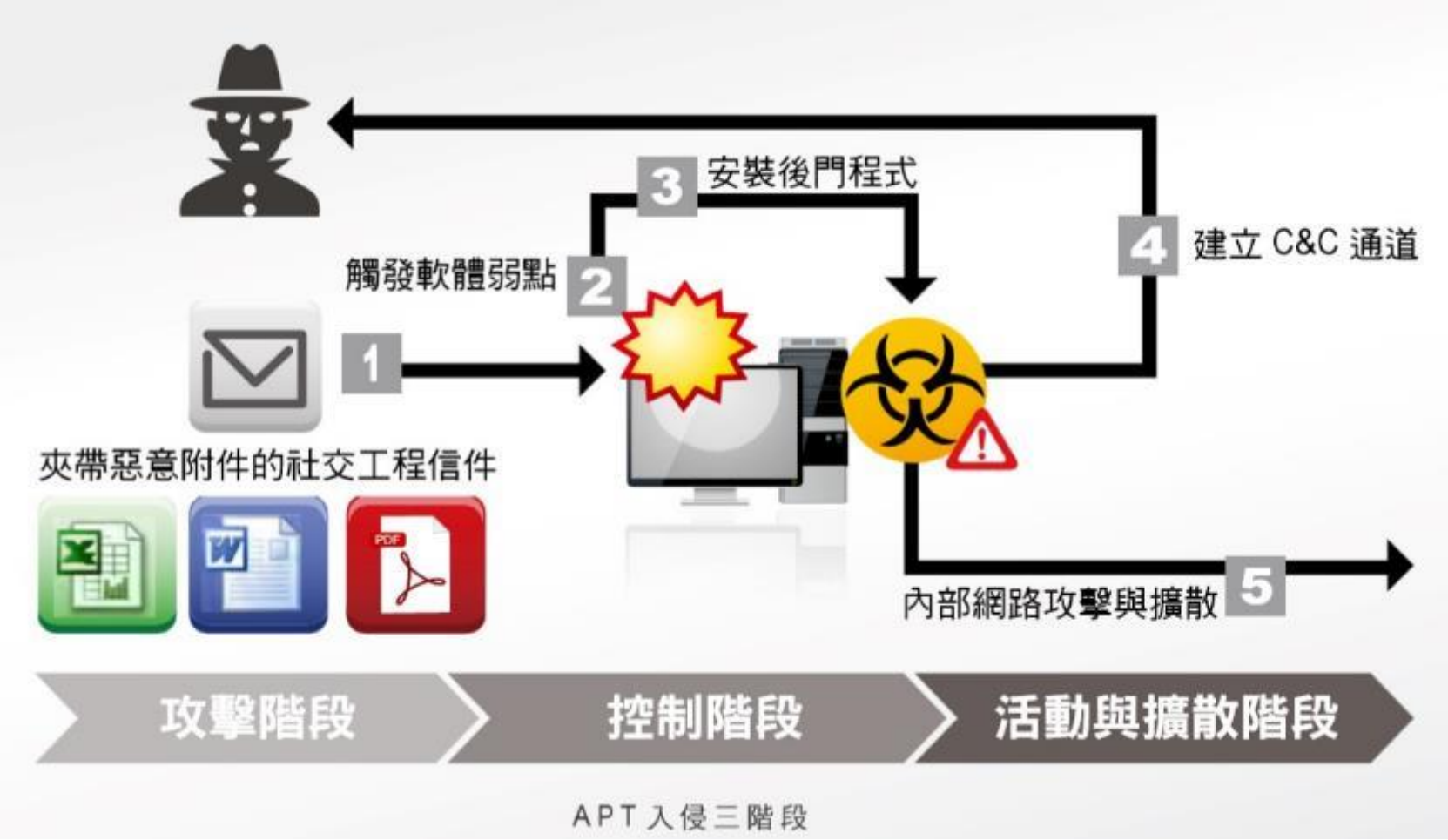
APT進階持續性滲透攻擊

APT攻擊流程

鎖定目標	• 背後通常有豐沛資源或組織支援，亦有針對性目標與範疇，如國防、重要機關、金融及學術界等
收集資訊	• 透過各種公開或地下的管道進行資料收集，包括公開或機密資訊，社群網站、端點防禦設備、網路架構等
攻擊滲透	• 根據收集資訊來規劃設計攻擊策略
建立據點	• 滲透成功後，開啟後門取得控制權並持續滲透攻擊，躲避防毒機制偵測
分析資訊	• 透過監聽、網芳攻擊及檔案伺服器，以蒐集並分析內部機密資訊，如帳密、網路架構機密文件
權限提昇	• 提昇於系統主機或伺服器之權限
回傳機密資料	• 打包並回傳機密資料
消除系統紀錄	• 消除系統主機或伺服器之相關紀錄

APT進階持續性滲透攻擊

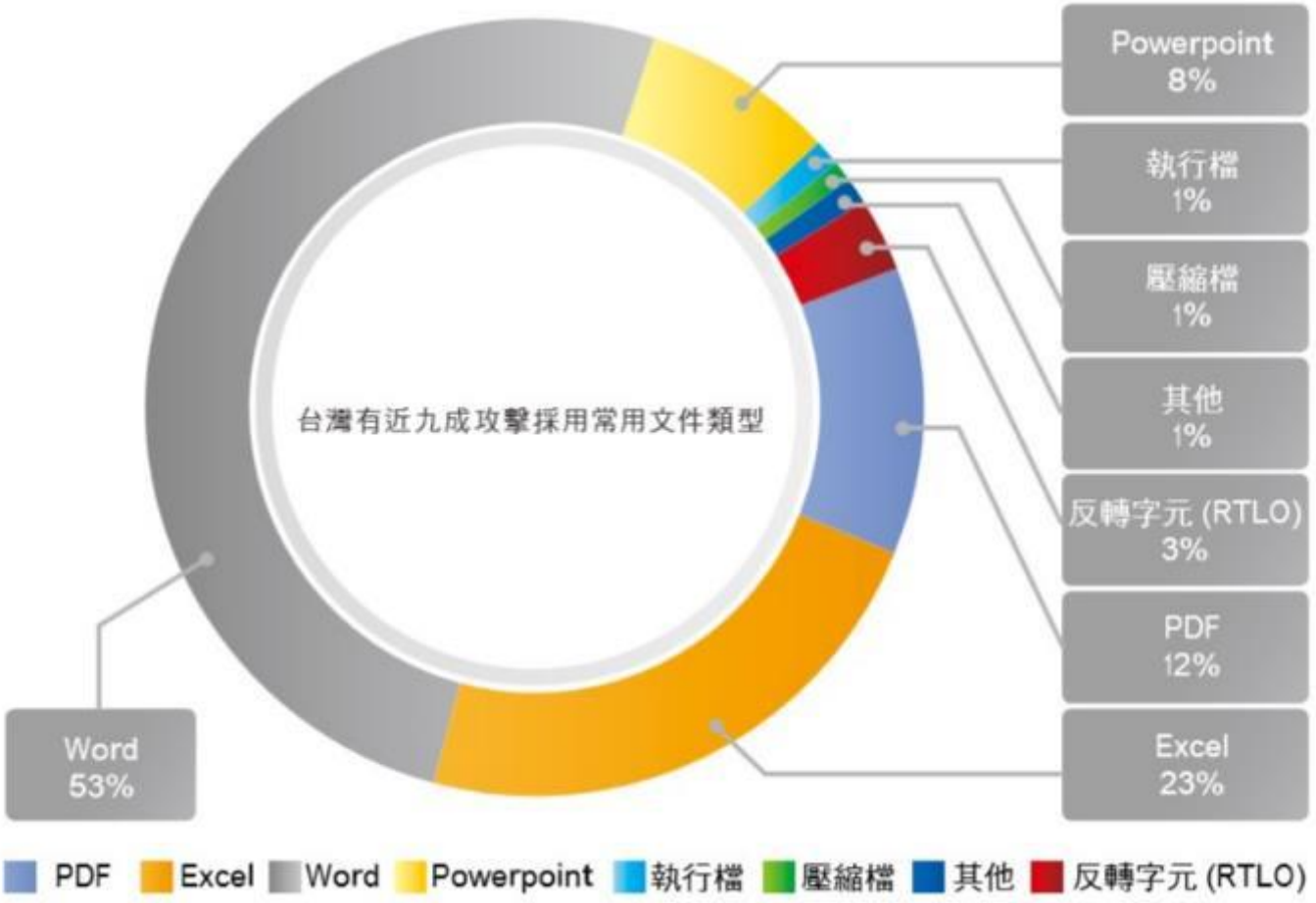
- APT 入侵 三 階 段



資料來源：趨勢科技APT威脅白皮書

APT進階持續性滲透攻擊

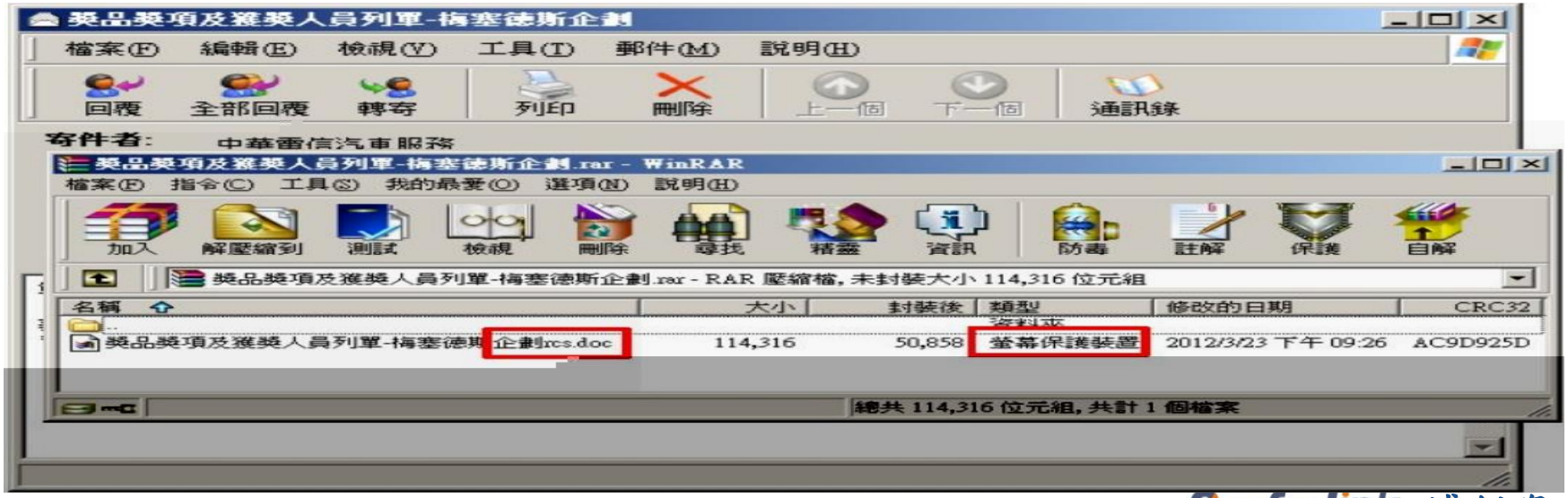
- APT電子郵件社交工程攻擊常用文件類型



資料來源：趨勢科技APT威脅白皮書

APT鎖定式攻擊竊取機敏資料

- 目標攻擊幾種不同類型的社交工程陷阱技術？
  - ◆利用網頁郵件服務的帳號來發送這些電子郵件
  - ◆利用所之前入侵獲得的電子郵件帳號來發送
  - ◆偽裝成特定部門或高階主管的電子郵件地址



APT 針對性攻擊

- **APT（Advanced Persistent Threats）**
  - 針對特定組織進行的多方位網路攻擊
  - 過去APT多以政府為目標，尤其是政治動盪的區域，前年開始針對企業或大型組織，擁有越多用戶資料的網站越是駭客眼中的大肥羊
- **APT特性**
  - 多半不直接攻擊提供外部服務主機(如官方網站)的弱點
  - 常以電子郵件搭配惡意檔案，透過社交工程進行攻擊
  - 惡意檔案多透過文件檔案進行包裹，如PDF、XLS、DOC等
  - 感染目標組織的主機後，不立即進行大規模破壞或擴散、不佔用太多主機資源，網路使用量也低，可長期潛伏不易發現
  - 惡意程式的活動、攻擊、擴散皆具目標性

系統主機遭到入侵

美淨水廠系統遭駭客入侵，差點把強鹼濃度提升100倍

不明人士疑似利用淨水廠員工使用的第三方遠端電腦控制軟體TeamViewer，來駭入水廠內部系統

情境示意圖，Photo by Nathan Dumlao on unsplash

系統主機遭到入侵

- 除新冠肺炎議題相關攻擊外，組織型駭客針對政府機關業務負責窗口，以業務諮詢相關問題為主旨，搭配惡意附檔，發動魚叉式社交工程攻擊

新冠議題

業務諮詢

防護建議

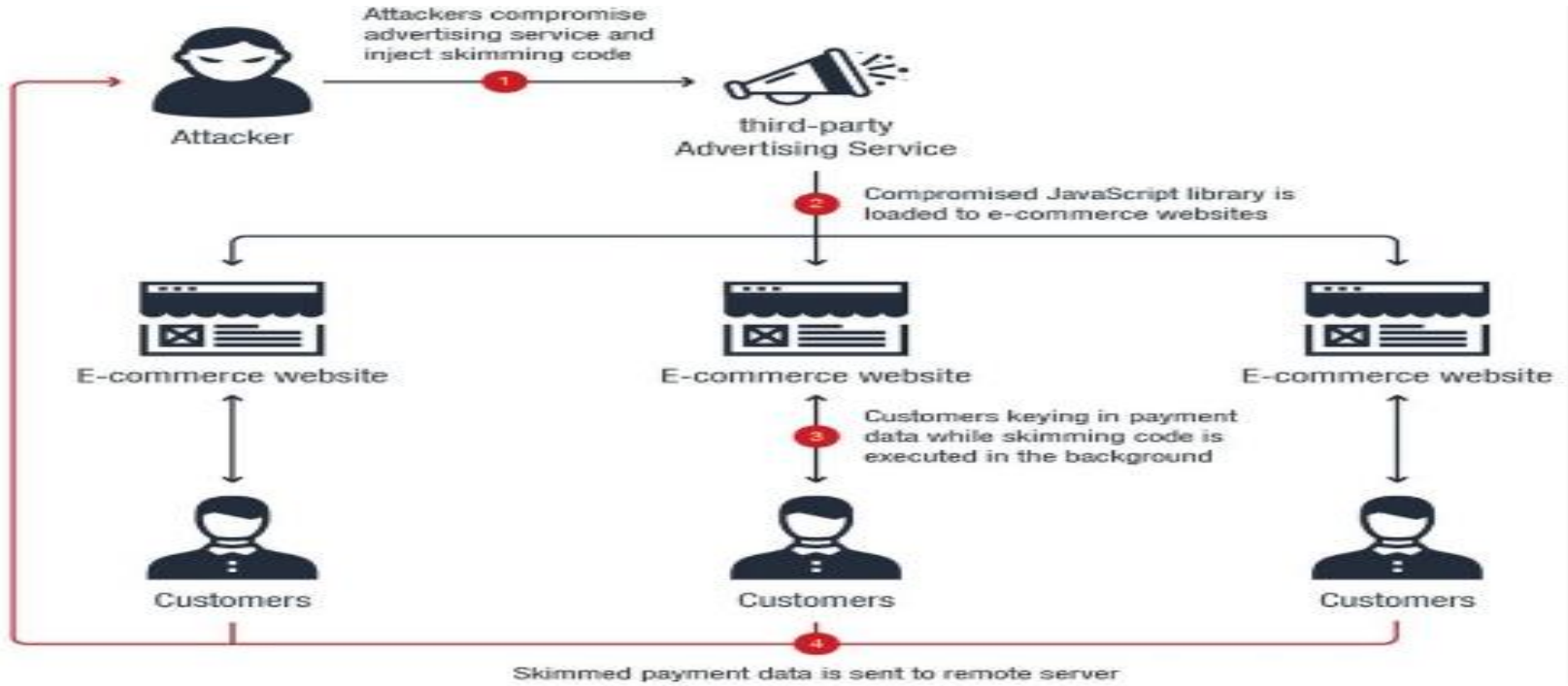
- 注意郵件來源之正確性，勿開啟不明來源之郵件與連結
- 確認電子郵件附檔屬性或檔名後才點擊檔案，提高警覺

系統主機遭到入侵

美國第二大醫療保險公司 Anthem資料外洩事件

資安供應商持續遭駭破壞供應鏈安全

- 攻擊型態趨於多元，供應鏈防護
  - 供應鏈攻擊是如何逐步進行的？



資安供應商持續遭駭破壞供應鏈安全

蒸發78億!台積電資漏洞 傳遭"想哭"攻擊

關鍵資訊基礎設施資安風險

- 關鍵基礎設施(Critical Infrastructure, CI)？
  - 能源
  - 水資源
  - 通訊傳播
  - 交通
  - 金融
  - 緊急救援與醫院
  - 政府機關
  - 科學園區與工業區

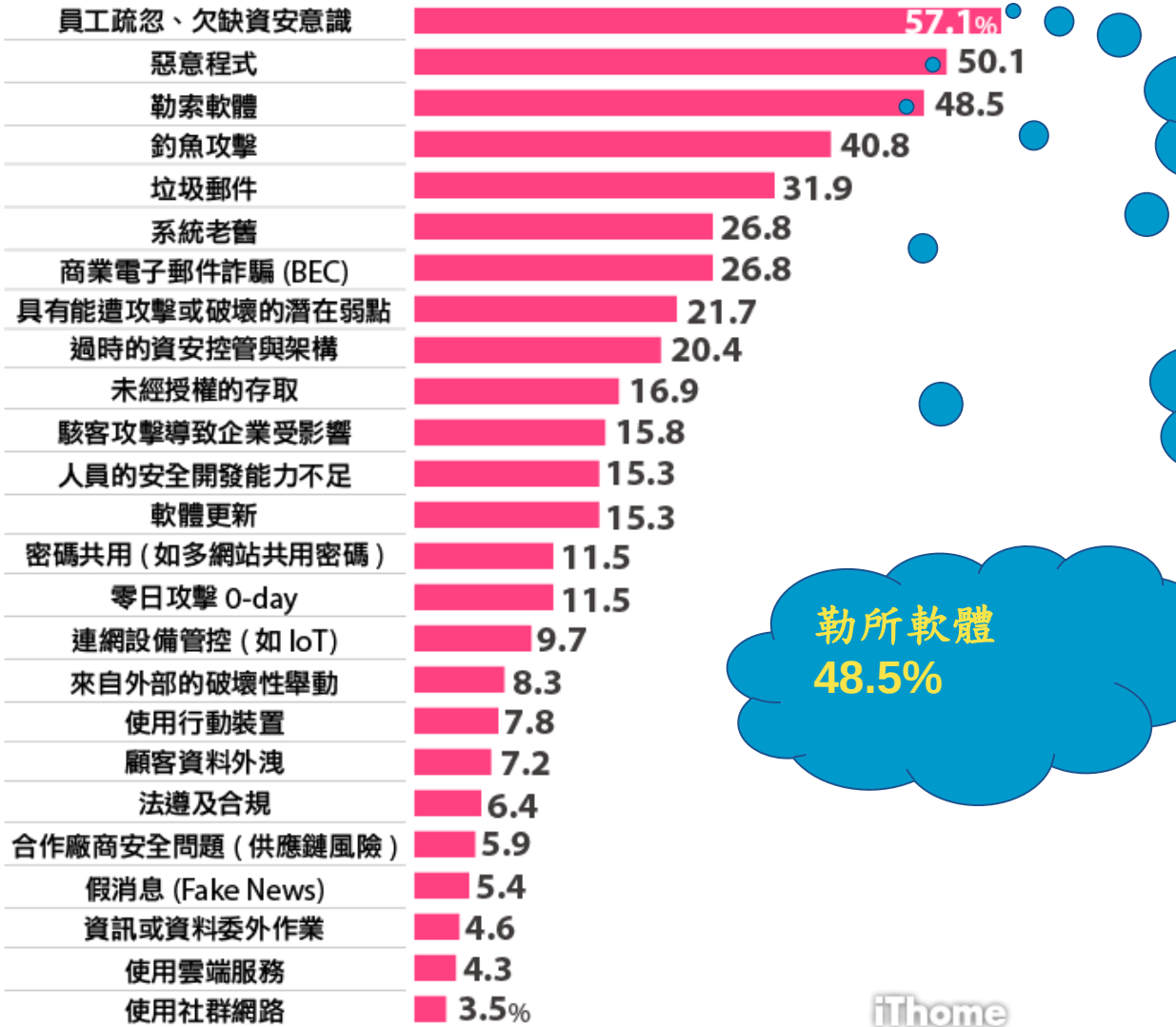
關鍵資訊基礎設施資安風險

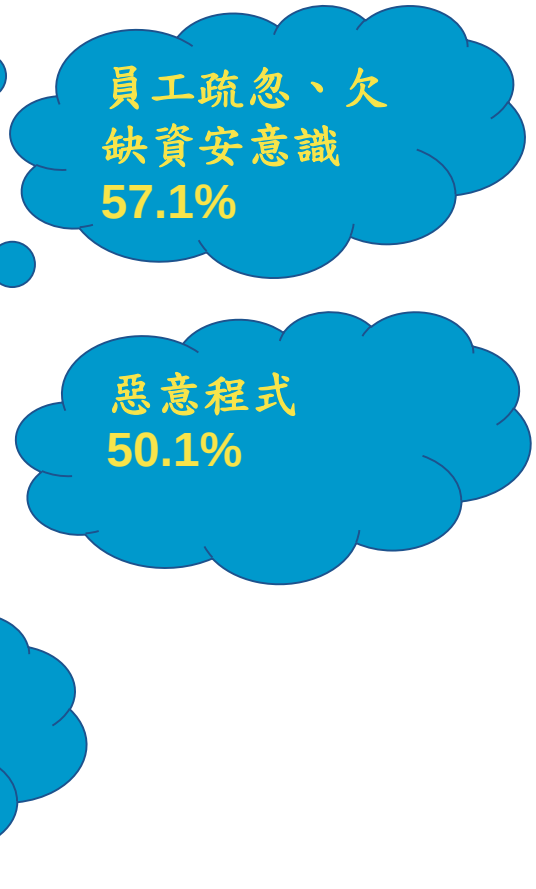
- 關鍵基礎設施(Critical Infrastructure, CI)？
  - ◆能源
  - ◆交通

員工資安意識不足的威脅，比駭客更大

2020 企業資安風險 Top25

BEC 威脅大增，假新聞資安風險開始浮現





iThome

SafeLink 博創資訊

- 前言
- 全球資通安全威脅趨勢
- 案例探討及分享
- 造成資料外洩的原因
- ✓政府資安威脅趨勢
- 政府資安威脅案例分享

政府資安威脅趨勢

- 綜整111年政府領域資安威脅偵測與機關通報資訊，主要威脅趨勢有6大面向

1.社交工程與APT惡意電子郵件仍為主要攻擊手法

2.遠端服務探測與產品漏洞利用為主要網路威脅

3.雲端服務中繼站盛行協助駭客隱匿惡意行為

4.萬物聯網衍生應用造成資安風險

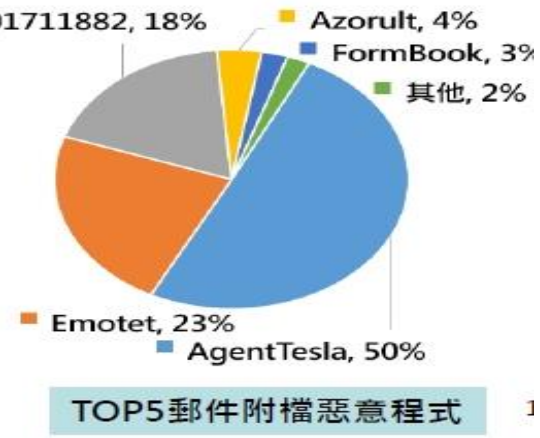
5.供應鏈安全遭破壞成為入侵跳板

6.人員資安意識不足導致資料外洩

政府資安威脅趨勢

偽冒政府機關發動社交工程攻擊

- 111年7月至9月，駭客大規模散布假衛福部紓困訊息，騙取民眾身分個資與網路銀行資訊
  - 偽冒衛福部與政府機關之域名(xxxgov.tw)，架設假官方釣魚網站
- 上半年Emotet仿真郵件大幅增加外，全年度含惡意附檔之惡意電子郵件以散布遠端木馬(AgentTesla)最多
  - AgentTesla於2014年發現，專門竊取機敏資訊，110年2月發現新的變種後，相關攻擊持續顯著增加

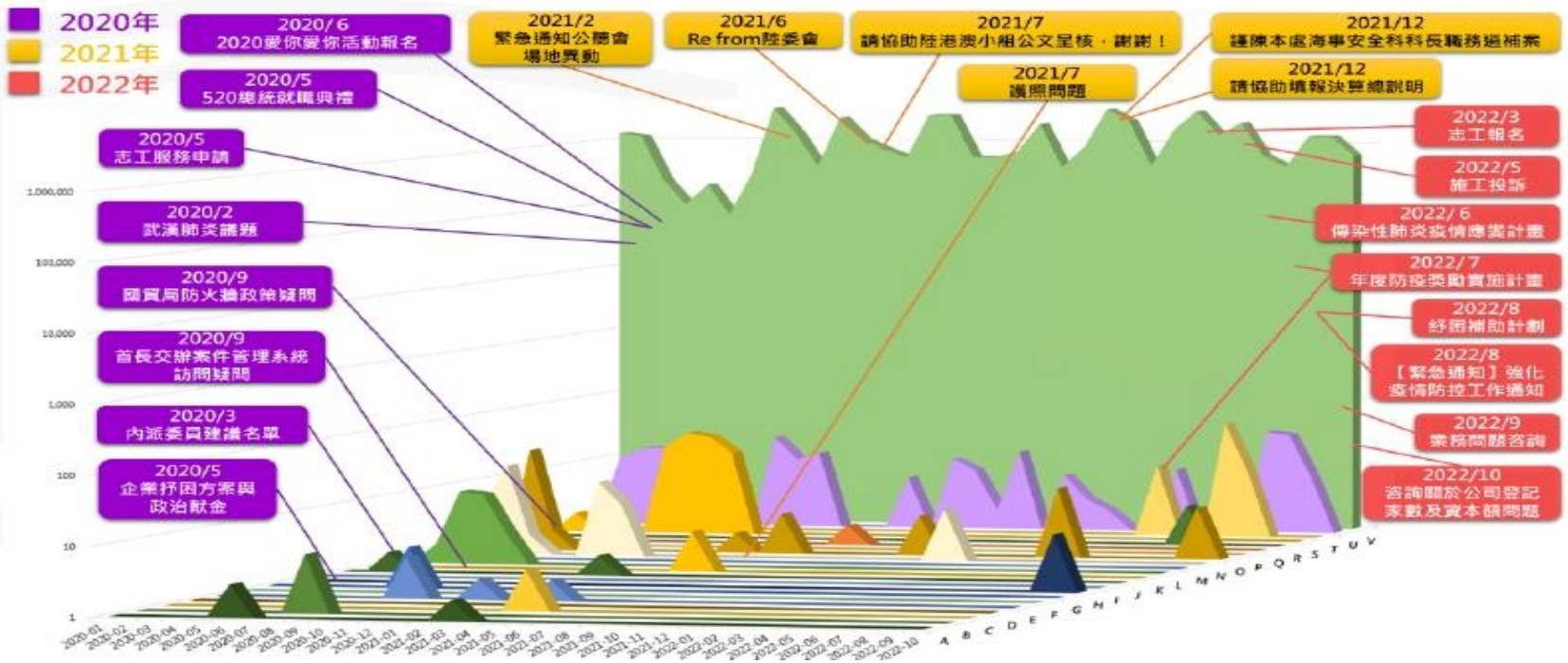


TOP5郵件附檔惡意程式

政府資安威脅趨勢

進階持續性攻擊鎖定業務窗口

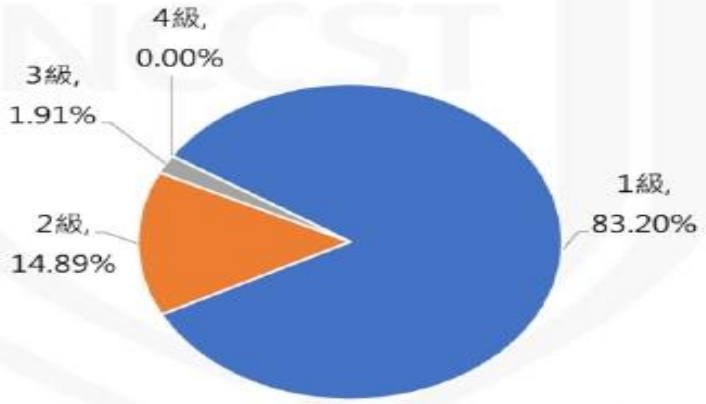
- 111年政府領域APT惡意電子郵件攻擊，駭客持續寄送含惡意附檔之電子郵件，以新冠疫情、業務諮詢等郵件主旨，對政府機關發動魚叉式社交工程郵件攻擊

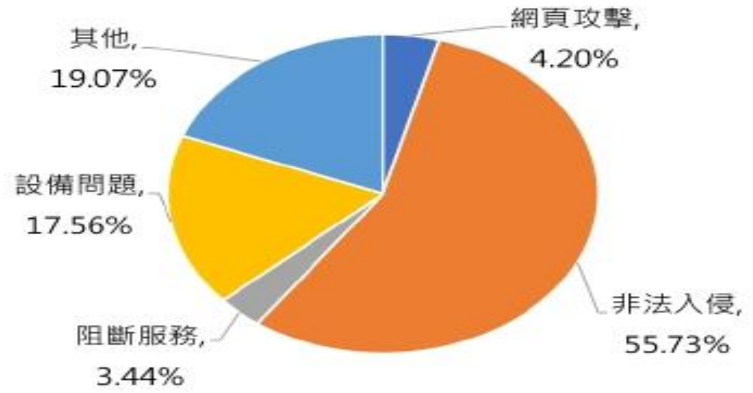


政府資安威脅趨勢

供應鏈安全遭破壞成入侵跳板

- 111年1月至10月共接獲524件之通報事件，仍以1級資安事件為主，惟於非法入侵事件中發現，因供應鏈安全落差成為駭客入侵跳板，導致機關遭入侵
  - 以非法入侵為大宗占55.73%，部分事件肇因於供應鏈廠商維護環境或管理疏失、社交工程及使用者行為，其次為設備問題，例如興達發電廠3月停機事件影響多個政府機關可用性問題
  - 42.56%(223件)為機關接獲技服中心警訊通告後所進行之通報





※統計區間：111/1/1至111/10/31公務機關通報(不含實兵演練)統計

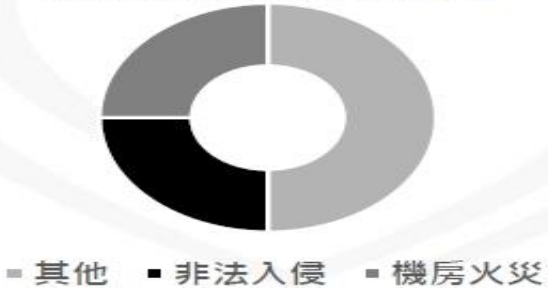
政府資安威脅趨勢

人員資安意識不足造成威脅

- 111年1月至10月共10件之3級資安通報事件，造成之影響為資料外洩與資料或系統異常，分析其發生原因發現造成資料外洩之主因為人員資安意識不足

資料外洩發生原因

資料或系統異常原因



- 人員疏失，誤將未遮蔽之個資公開或錯置
- 點擊釣魚訊息，導致管理者帳號密碼遭竊，進而取得對話內容中之個資
- 前員工濫用權限，撈取機關人員個人資料並進行兜售
- 密碼遭暴力破解，攻擊者入侵後刪除477筆資料
- 軟硬體異常，導致資料異常刪改或系統緩慢
- 機房火災，設備吸入滅火粉塵致故障

- 前言
- 全球資通安全威脅趨勢
- 案例探討及分享
- 造成資料外洩的原因
- 政府資安威脅趨勢
- ✓政府資安威脅案例分享

政府資安威脅案例分享

新冠疫情社交工程攻擊案例

- 駭客利用國人關注新冠肺炎議題，以提供紓困福利為由，架設偽冒衛福部與相關政府域名釣魚網站，散布釣魚郵件與手機惡意應用程式，對政府機關與一般民眾無差別發動攻擊，進行個人資料與網路銀行詐騙

防護建議

- 注意郵件來源之正確性，勿開啟不明來源之郵件與連結
- 確認政府相關域名之正確性，勿隨意提供機敏資訊

政府資安威脅案例分享

偽冒機關帳號散布惡意電郵案例

- 駭客利用政府機關電子郵件伺服器未設定寄件者原則架構(SPF)，大規模偽冒政府機關人員電子郵件帳號，發送大量惡意勒索電子郵件進行社交工程攻擊
  - 111年9月偵測發現，遭駭客偽冒之政府機關，共計87個政府機關、117機關域名未完善SPF設定

未設定SPF之機關責任等級分布	
A級機關	6
B級機關	27
C級機關	38
D級機關	13
其他	3(資安法尚未列管)

防護建議

- 建議可參考寄件者原則架構(SPF)設定，完善郵件安全防護，避免機關電子郵件帳號遭偽冒利用

政府資安威脅案例分享

進階持續性攻擊郵件案例(1/2)

- 除新冠肺炎議題相關攻擊外，組織型駭客針對政府機關業務負責窗口，以業務諮詢相關問題為主旨，搭配惡意附檔，發動魚叉式社交工程攻擊

新冠議題

業務諮詢

防護建議

- 注意郵件來源之正確性，勿開啟不明來源之郵件與連結
- 確認電子郵件附檔屬性或檔名後才點擊檔案，提高警覺

政府資安威脅案例分享

進階持續性攻擊郵件案例(2/2)

- 組織型駭客偽冒技服中心，於郵件中安插技服中心圖示並使用「資安審查」等郵件主旨，針對台灣企業發起魚叉式社交工程釣魚郵件攻擊

防護建議

- 注意郵件來源之正確性，勿開啟不明來源之郵件與連結
- 如感覺有異請先洽技服中心查證，可以利用通報網站或技服信箱進行情資分享

政府資安威脅案例分享

產品漏洞威脅案例

- 網通設備產品一向為駭客鎖定之攻擊目標，111年初F5之BIG-IP產品發現重大安全漏洞(CVE-2022-1388)，可透過iControl REST身分鑑別漏洞存取BIG-IP系統，並遠端執行任意程式碼
- 經異常連線行為偵測，發現某機關疑似受駭，經鑑識調查後，發現駭客利用BIG-IP漏洞入侵該設備以放置後門程式與駭客工具，意圖遠端操控並進行內部橫向擴散

防護建議

- 儘速下載對應版本之更新檔，並將管理頁面功能更新至最新版本
- 若版本因已停止支援而未釋出修補程式，建議升級至仍有支援且已推出修補程式之版本
- 若無法更新至最新版本，請採出官方所建議之緩解措施

政府資安威脅案例分享

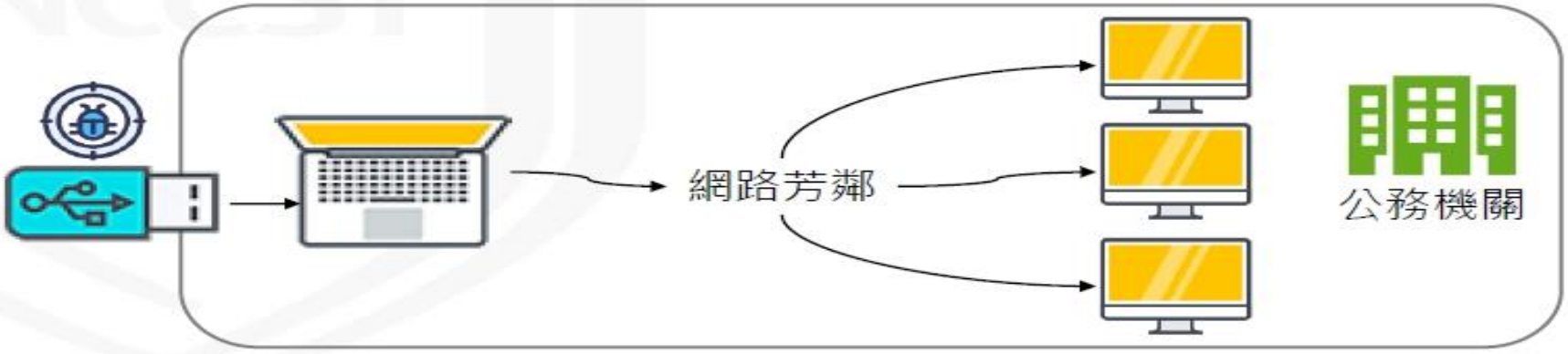
供應鏈攻擊-資訊廠商環境(1/3)

- 案例一：
  - 委外廠商人員電腦遭入侵植入惡意程式，廠商使用遭入侵之資訊設備維護機關資通系統，導致機關遭植入惡意程式
  - 委外廠商兩台電腦皆於相同資料夾路徑，發現相同的惡意程式，判斷該廠商內部存在資安風險

政府資安威脅案例分享

供應鏈攻擊-資訊廠商環境(2/3)

- 案例二：
  - 機關使用駐點廠商閒置電腦建置視訊環境，未先執行系統更新與安全檢測等作業，導致該電腦存在安全性漏洞遭利用，嘗試利用網路芳鄰協定對機關內部其他主機進行攻擊行為
- 案例三：
  - 廠商至機關進行電話交換機設定維護作業，將中毒USB插入機關提供之電腦並連網，連帶資訊設備中毒並嘗試利用網路芳鄰協定(Port 445)對其他主機進行可疑連線行為



政府資安威脅案例分享

供應鏈攻擊-資訊廠商環境(3/3)

防護建議

- 建議機關選任計畫委辦廠商時，依資通安全管理法與子法要求評估適當之受託者，並監督其資通安全維護情形
- 執行計畫時，機關應要求廠商建置環境之設備符合機關資安要求，並循正常流程管道申請使用機關設備，避免未經管制設備於機關環境中使用
- 作業執行前，機關或廠商應將作業系統與防毒軟體更新至最新版本，並持續更新修補漏洞，以降低遭外部入侵風險

政府資安威脅案例分享

物聯網裝置應用風險案例

- 案例一：
  - 111年8月，因美國聯邦眾議院議長裴洛西訪台行程一事，導致台灣攻擊事件頻傳，超商與車站電子看板等物聯網設備遭駭客入侵並置換內容[19]

- 案例二：
  - 111年9月，經偵測發現某機關設備有異常連線行為，進一步確認時發現該機關受駭設備為門禁系統，且存在身分驗證繞過漏洞，駭客透過該漏洞入侵設備，並安裝惡意程式

防護建議

- 管理介面應強化存取控制
- 盤點機關內部相關IT與OT資產並納入風險評估
- 可透過VANS系統定期檢視相關IT與OT設備漏洞並更新

政府資安威脅案例分享

資料外洩/人為疏失案例

- 機關委託廠商辦理競賽活動，並提供活動資訊，欄位包含姓名與行動電話號碼等，廠商工作人員為協助活動宣傳，將參與人員資訊上傳至個人公開網站，造成個資資料外洩

防護建議

- 建議機關選任計畫委辦廠商時，合約中應納入資通安全管理法與個資法相關要求，並監督廠商落實執行
- 資料放置於網站前，應審核確實公告內容含有個資之必要性，不得逾越特定目的之必要範圍
- 資料上傳至公開網站後，應重複確認公開之資訊內容適切性
- 活動結束後，應監督廠商完成資料或相關存取權限等，返還、移交、刪除或銷毀，以及資料自網站下架

政府資安威脅案例分享

勒索病毒/人員資安意識

- 案例一：
  - 機關人員使用公務電腦瀏覽網站，點擊下載與執行偽裝成微軟更新包之惡意程式，大陸影音網即遭植入勒索病毒，並透過網路芳鄰感染網路硬碟，致個人電腦與網路硬碟檔案資料遭加密
- 案例二：
  - 機關人員個人電腦之檔案遭加密，經查為同仁於上班時段瀏覽免費漫畫網站，點擊惡意連結，下載並執行檔案，導致個人電腦感染勒索病毒

防護建議

- 加強內部同仁資安觀念：公務電腦應僅供公務使用
- 軟體更新作業應配合機關政策，並勿下載未經授權軟體

政府資安威脅案例分享

資料維護/網站資料維護

- 機關維護之網站提供外部A單位連結，由於A單位之舊網域租用到期未續約，後由其他公司註冊為色情網站
- 因機關未即時接獲相關消息並更新連結資料，以致使用者點擊該連結時導向至色情網站

防護建議

- 機關人員除定時檢視網站自身內容，亦應確保連結之正確性，避免導致民眾連結至錯誤之網站

政府資安威脅案例分享

設備管理不當/誤用報廢設備

- 某機關設備遭駭客暴力破解遠端桌面登入密碼進而植入惡意程式，由於該設備老舊並規劃報廢，故未進行處置
- 同仁誤使用該設備執行網路維護測試並連網，導致設備再次連線至駭客中繼站

防護建議

- 機關應訂定資訊設備報廢處理相關作業程序，並落實報廢設備管理規定，以避免待報廢設備衍生資安問題之疑慮
- 作業執行前，機關應確認設備已將作業系統與防毒軟體更新至最新版本，並持續更新修補漏洞，以降低遭外部入侵風險

造成資料外洩的原因

1.網路釣魚攻擊

以釣魚郵件將使用者引導至偽裝成真實購物網站、銀行、信用卡公司或網路服務等之合法登入頁面的假網站（釣魚網站），藉以竊取使用者在該網站所輸入的個資。

從你購物的網站偷偷**收集信用卡資訊**。因為新冠狀病毒(COVID-19,俗稱武漢肺炎)封城期間有更多使用者湧向電子商務網站，使得網頁卡號側錄相關的事件在三月增加了26%

2.盜用帳號:

Apple ID或Google、Amazon帳號等可連動多數網站服務的帳號在遭到盜用時，其受害情況很可能會擴及其他的網路服務。並且，帳號中所登記的信用卡資訊或姓名、住址等個人資料、雲端上的郵件或備份資料等私密資訊都可能會被盜取

造成資料外洩的原因

3.惡意軟體或惡意應用程式的未授權操作

透過電腦或智慧型手機之未授權操作，可能會導致儲存資訊或輸入內容被監視，或裝置上的相機及麥克風等功能被用來竊取資訊。因此，不只是電腦，在智慧型手機上也需要安全防護對策

4.終端裝置遭竊或遺失

在電腦或智慧型手機中經常儲存了大量的資訊，例如聯絡方式、照片或影片、文件檔案、網站瀏覽器中儲存的各種網路服務的帳號與密碼，以及社群網站上的動態等。萬一終端裝置因遭竊或遺失落入惡意的第三方手中，可能會發生未授權操作而導致這些個資發生外洩。

造成資料外洩的原因

5.在社群網站上過度公開資訊

當使用Facebook、Instagram、Twitter或LINE等社群網站時，您可能會誤以為只有在朋友間分享，而導致過度公開個人資料。但是，您在網路上公開的個資可能被不特定多數的外人瀏覽。您不知道是什麼人以何種目的在瀏覽您的資料。這些人之中也存在專門收集資訊的第三方，會將資料用於犯罪用途，或賣給惡質的個資名單業者。

6.公共Wi-Fi 分享無線網路

分享無線網路使用上雖然很方便，如果沒有採取適當的安全防護對策，很容易就會發生通訊內容被監視的風險。駭客創造與公共Wi-Fi相似名稱的假熱點，讓您在不知情下登入以竊取個資的犯罪手法。

7.服務業者的過失或網路攻擊

使用網路上的服務一定會伴隨個資外洩風險。截至目前為止發生的使用者相關資料外流事件，都是因為服務業者在安全防護上的過失或內部犯罪，還有網路攻擊的非法存取等原因所導致。

當你個資外洩時會發生什麼事？

詐騙集團可能會拿你的個資做的事情

假冒機構(公務員)詐騙

假冒醫院或警察，告知個資被冒用，需至超商收**法院公文傳真**將存款**領出交付監管帳戶**。

解除分期付款詐騙

佯稱網路購物誤設分期，請您至**ATM**操作、購買遊戲點數**解除分期付款**設定。

假冒網拍交易詐騙

假冒網路賣家，以**低於市價**的商品吸引您下標，並**要求私下交易**，匯款後賣家就人間蒸發。

當你個資外洩時會發生什麼事？

詐騙集團可能會拿你的個資做的事情

110.03.08-110.03.14

高風險賣場

解除分期付款

Check2check
Booking.com
85天空民宿
西堤牛排
金石堂網路書店
臺中愛戀旅店
旭日文旅
東森購物
GOMAJI
Agoda
比價王
明洞國際

1、客服不會來電要求您操作網路銀行或ATM解除錯誤設定。
2、接獲+字號或陌生來電☎，務必提高警覺。

刑事警察局

假網拍

FACEBOOK
奇摩拍賣
旋轉拍賣

FB、LINE、IG沒有安全交易保障機制，請勿於社群平臺購物。

請慎選優良有信用，且提供第三方支付之網購平臺，保障消費權益。

資料來源

- 110年國家資通安全情勢報告。
- 110-113國家資通安全發展方案。
- 111年第2次政府資通安全防護巡迴研討會
- 資安日報https://www.ithome.com.tw/
- 國家關鍵基礎設施安全防護指導綱要
- 資訊系統安全(作者:陳彥銘，2020年出版)
- 打造安全無虞的網站(作者:吳惠麟，2022年出版)
- 資訊安全概論與實務(第三版)(作者:洪小文院長)
- 資訊安全與法律特訓教材(財團法人中華民國電腦技能基金會總策畫出版)

Q&A 問題與討論

Q&A 問題與討論

課後評量