教育機構資通安全風險評鑑與風險處理

鍾沛原

講師簡歷

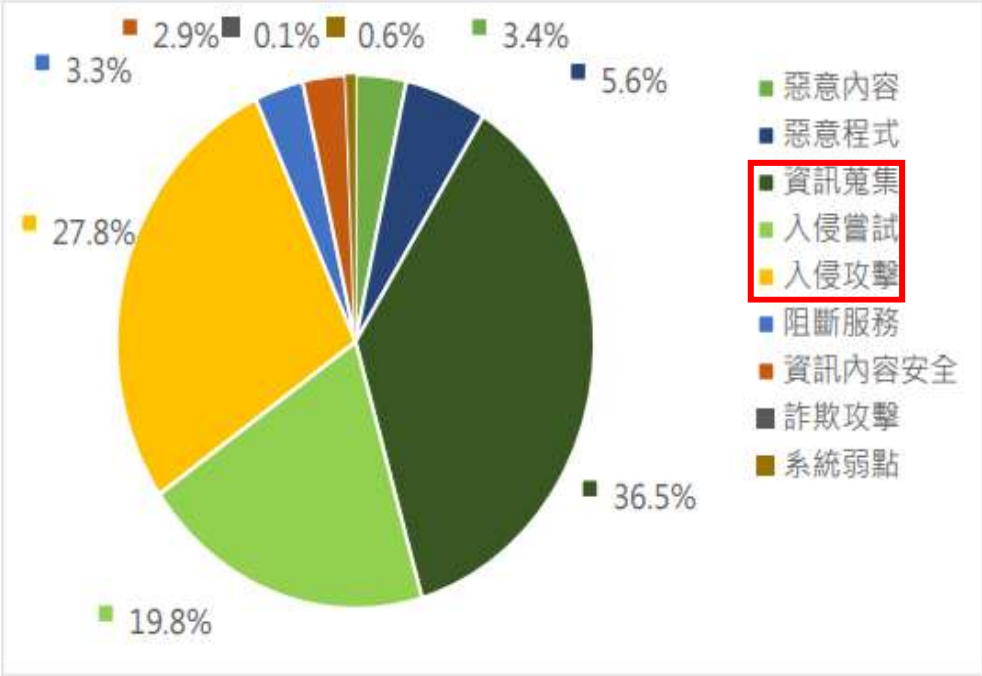
- 鍾沛原
- 經歷：教育機構資安驗證中心資安暨個資主導稽核員
  成大資通安全研究與教學中心 專案經理
  行政院資通安全稽核委員
  教育部所屬公務機關及所管特定非公務機關資通安全稽核委員
  經濟部能源及水資源領域關鍵基礎設施資通安全稽核委員
  衛生福利部資通安全稽核委員
  經濟部水利署資通安全稽核委員
  教育體系資通安全職能訓練課程講師
- 證照： ISO 27001:2022 LA、ISO 27701:2025 LA、ISO 22301:2019 LA、BS 10012 LA:2017、IEC 62443-2-1:2010 LA(TCIC)、CCNA Routing and Switching、CEH、CHFI、經濟部iPAS資訊安全工程師中級能力鑑定...
- 計畫執行：經濟部「關鍵基礎設施資安聯防服務專案」科技部「資安監控與管理技術開發」、經濟部能源局「強化民營能源關鍵資訊基礎設施資安防護計畫」、經濟部水利署「水資源關鍵設施升級及安全管理確保旗艦計畫」、行政院「我國電腦機房異地備援機制委託研究計畫」、教育部「教育單位網站弱點檢測與防洩漏個資資安服務計畫」.....等。

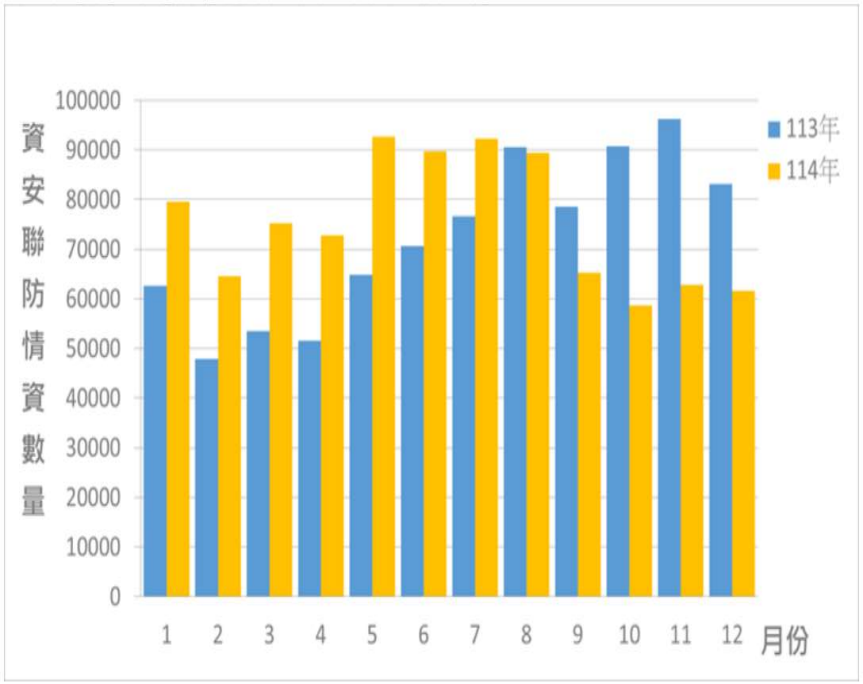
大綱

- 資安攻擊趨勢
- 資產盤點注意事項
- 風險評鑑與處理
- 結論

114年政府資安威脅統計

- 聯防預警情資

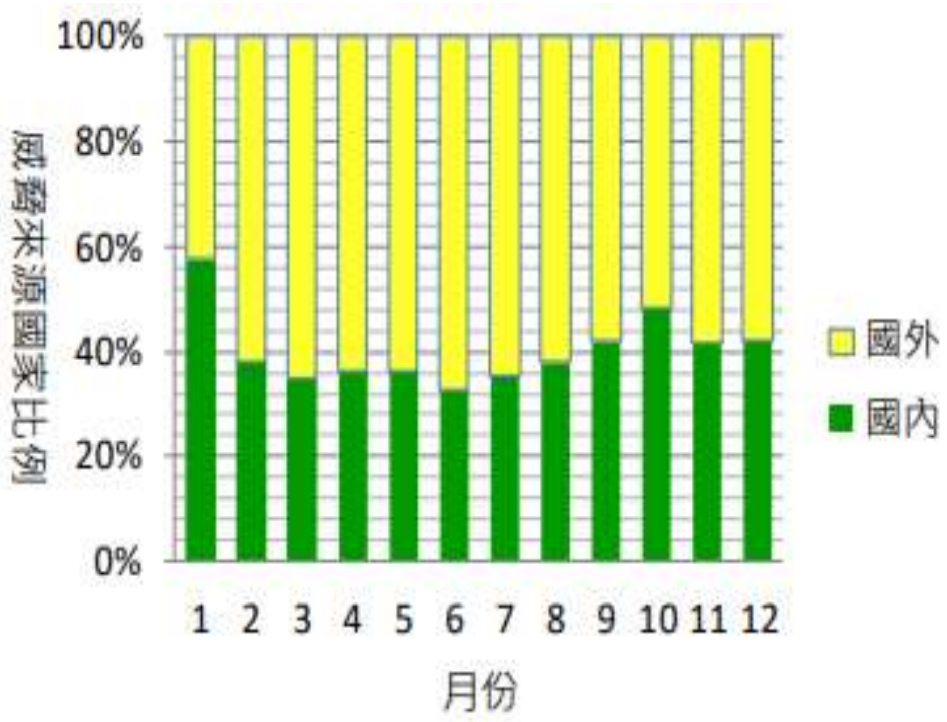




https://www-api.moda.gov.tw/File/Get/acs/zh-tw/xcIAJQzhitab5T1

114年政府資安威脅統計(cont.)

- 攻擊跳板來源 IP



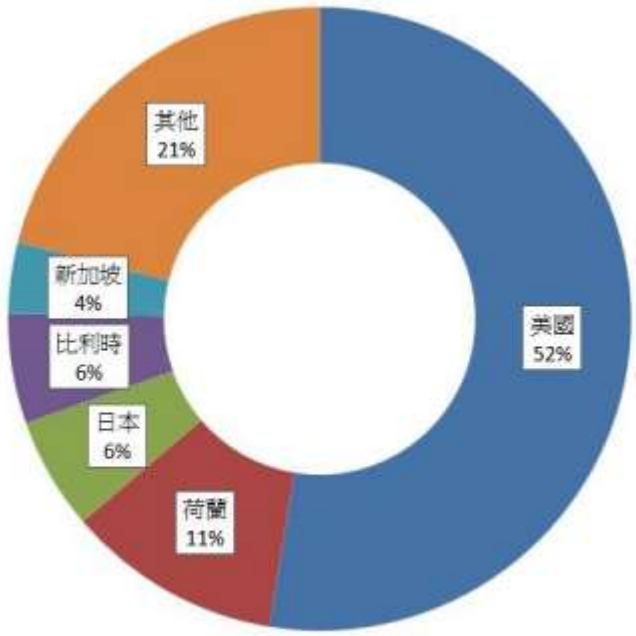


圖 4　114 年國外攻擊跳板來源國家比例

https://www-api.moda.gov.tw/File/Get/acs/zh-tw/xcIAJQzhitab5T1

114年政府資安威脅統計(cont.)

❑ 惡意電子郵件

共檢測1 億餘（109,590,054）封電子郵件，蒐集相關資訊進行分析，發現可疑惡意電子郵件 148 萬餘（1,489,180）封，約占整體 1.36%

114 年 3 月、6 月及 12 月偵測到大量詐騙釣魚郵件散布活動，經分析發現，駭客聲稱已入侵電腦裝置並監控網路活動為由，勒索使用者支付比特幣

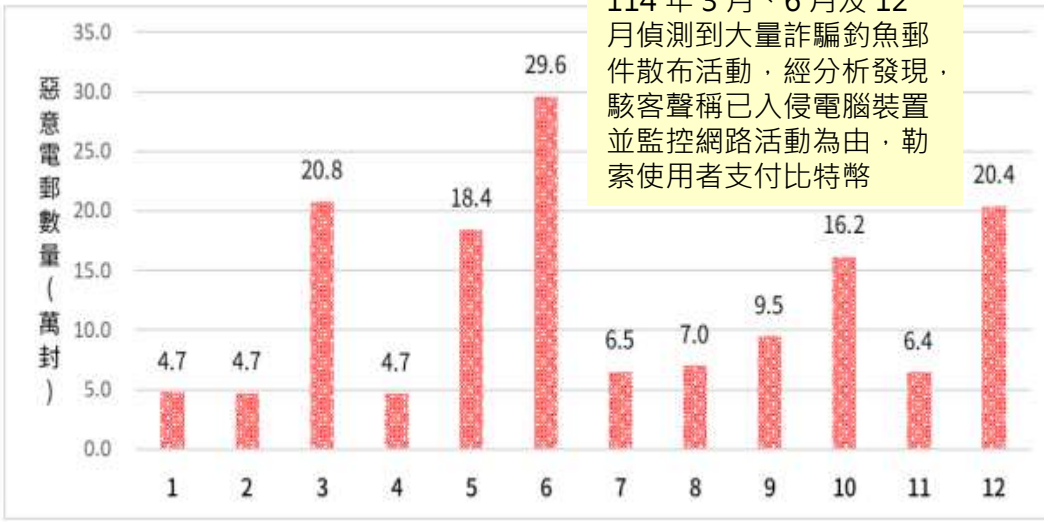


圖 5　114 年政府骨幹每月惡意電子郵件偵測數量

中低風險共占 98.23%，為惡意電子郵件內嵌可疑連結經威脅情資比對或附檔經防毒軟體靜態掃描，具有已知惡意樣態或特徵



圖 6　惡意電子郵件風險分布比例

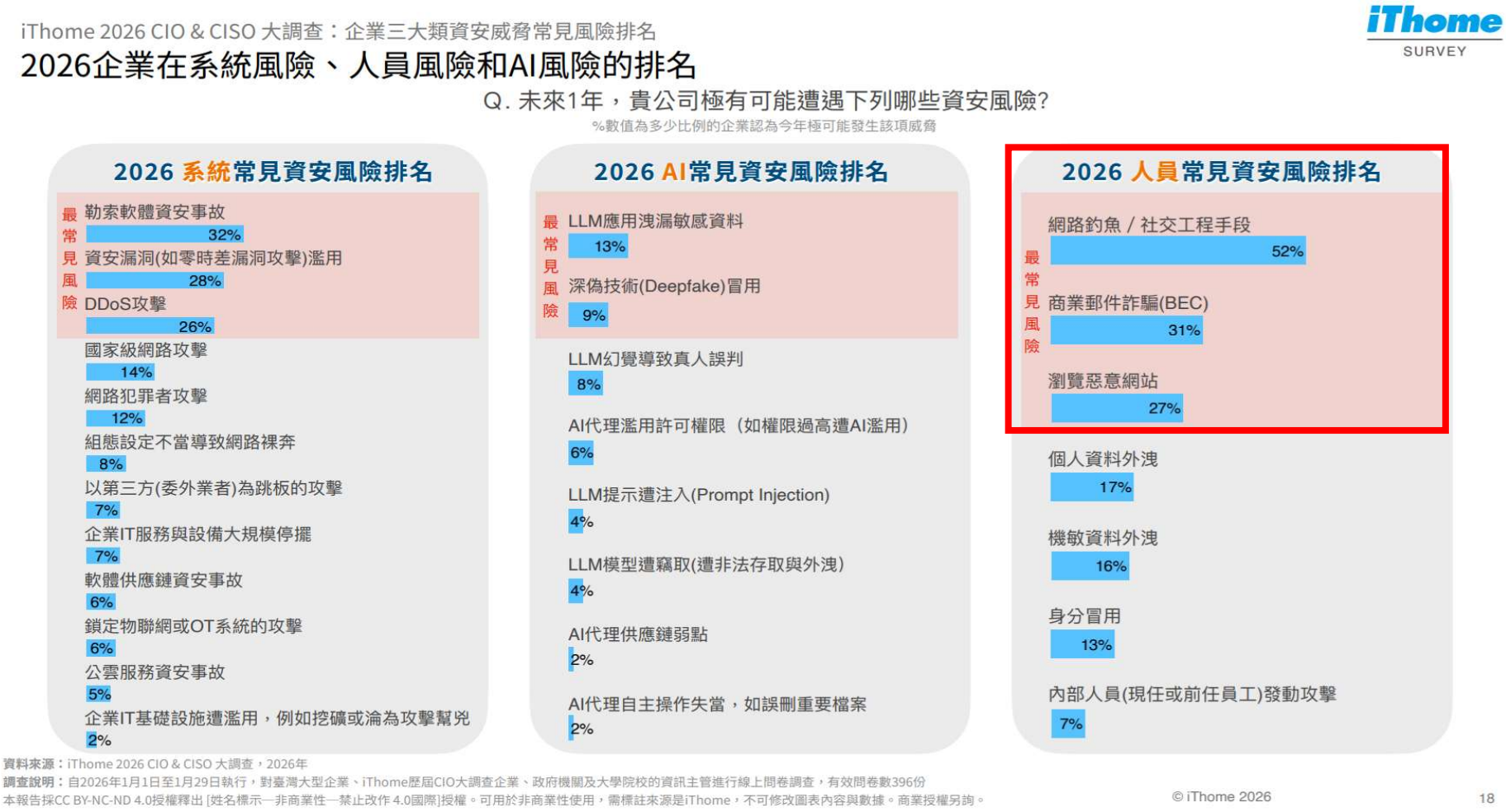
https://www-api.moda.gov.tw/File/Get/acs/zh-tw/xcIAJQzhitab5T1

114年政府資安威脅統計(cont.)

- 綜整 114 年政府進階持續性威脅（Advanced Persistent Threat,APT）惡意電子郵件攻擊手法，可歸納為五波攻擊行動：
  - 第一波攻擊手法著重於前期偵查，駭客透過**偵查電子郵件確認目標帳號有效性**，隨後利用LNK 捷徑檔結合合法系統工具（如 PowerShell）下載並執行惡意程式
  - 第二波攻擊，駭客改以**受駭之合法電子郵件帳號搭配業務與內部公告為主旨寄送惡意電郵**，同時部署多種惡意程式以提升攻擊成功率
  - 第三波攻擊則以**志工招募為由夾帶惡意附件**之社交工程郵件為主要手法，駭客誘使收件人執行附檔後植入 Python 後門程式，最終與中繼站建立連線
  - 第四波攻擊中，駭客透過多層規避與隱蔽技術，包含**通行碼以圖片形式呈現、以壓縮檔包裝惡意內容、透過捷徑檔觸發複合式執行流程**，並利用 DLL 側載函式庫（DLL Sideloading）手法載入惡意程式（Cobalt Strike），成功與中繼站建立連線並完成後門部署
  - 最後一波攻擊改以**合法雲端服務作為惡意檔案散布管道**，透過寄送含下載連結之社交工程郵件誘使目標下載並執行檔案，成功入侵後植入後門程式

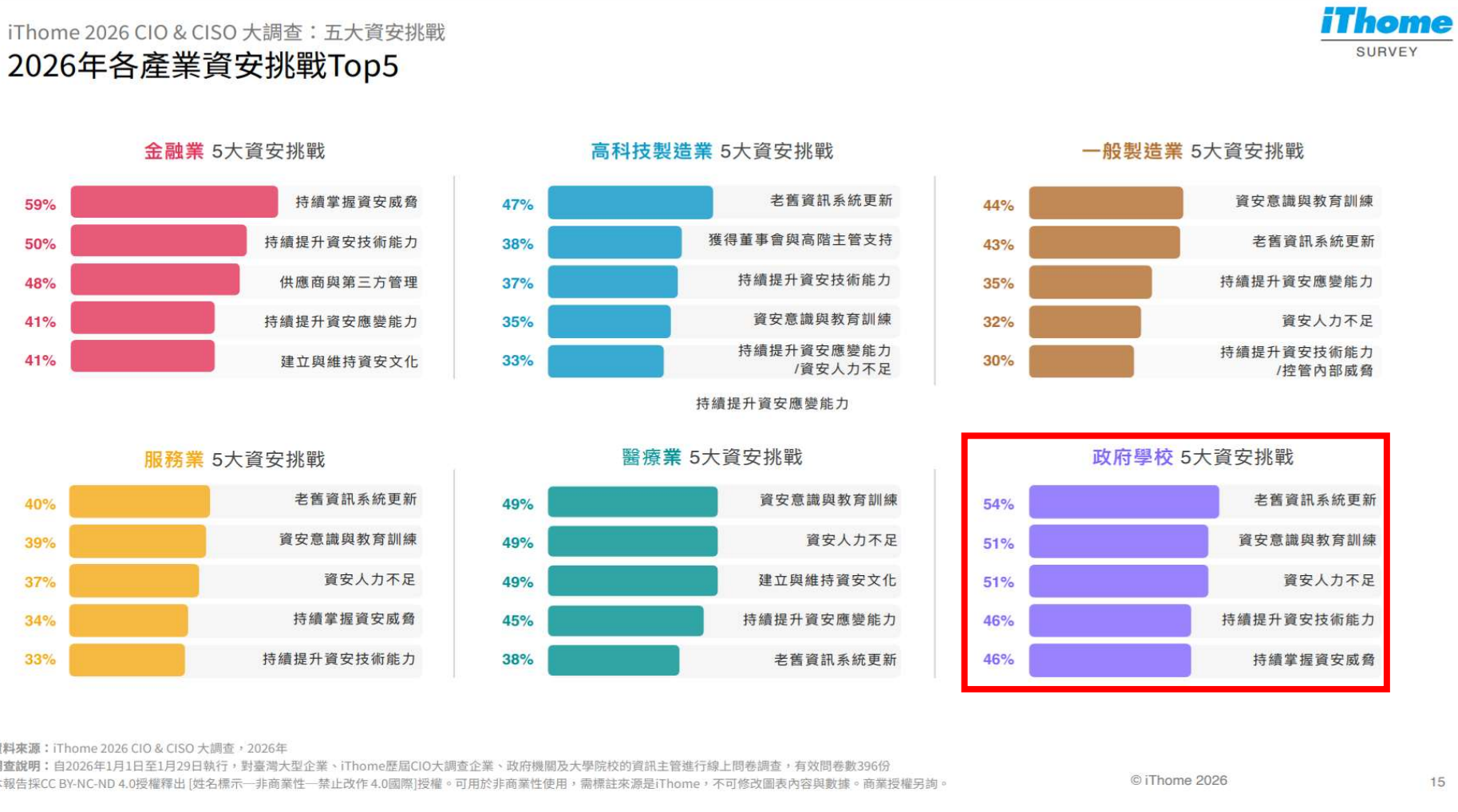
https://www-api.moda.gov.tw/File/Get/acs/zh-tw/xcIAJQzhitab5T1

2026企業三大類資安威脅常見風險排名



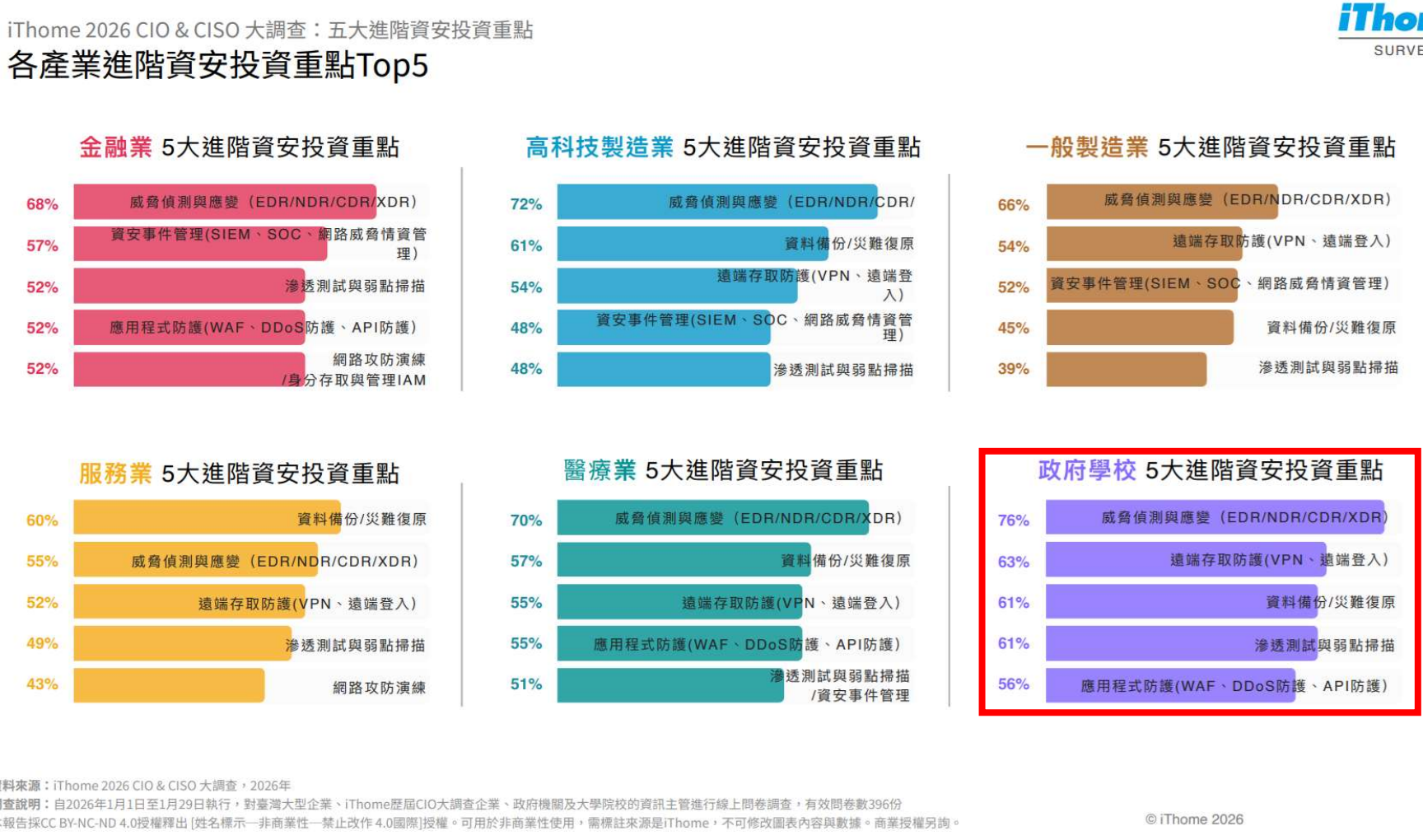
https://s.itho.me/vendor/2026/iThome/iThome_2026_State_of_CIO&CISO_Survey_FINAL-Part6-%E8%B3%87%E5%AE%89%E7%AD%96%E7%95%A5%E5%B8%83%E5%B1%80.pdf

2026年各產業資安挑戰Top5



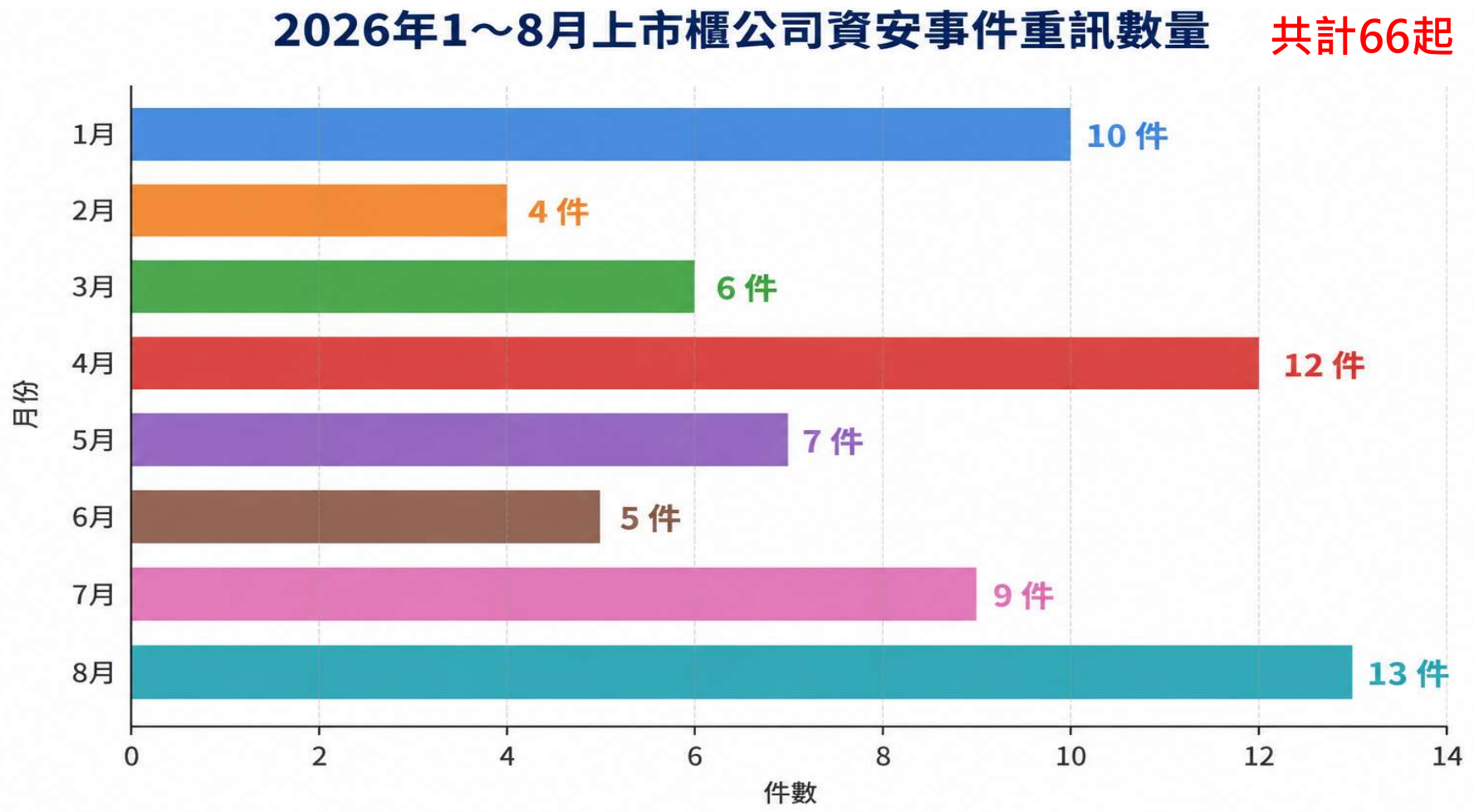
https://s.itho.me/vendor/2026/iThome/iThome_2026_State_of_CIO&CISO_Survey_FINAL-Part6-%E8%B3%87%E5%AE%89%E7%AD%96%E7%95%A5%E5%B8%83%E5%B1%80.pdf

資安投資重點Top5



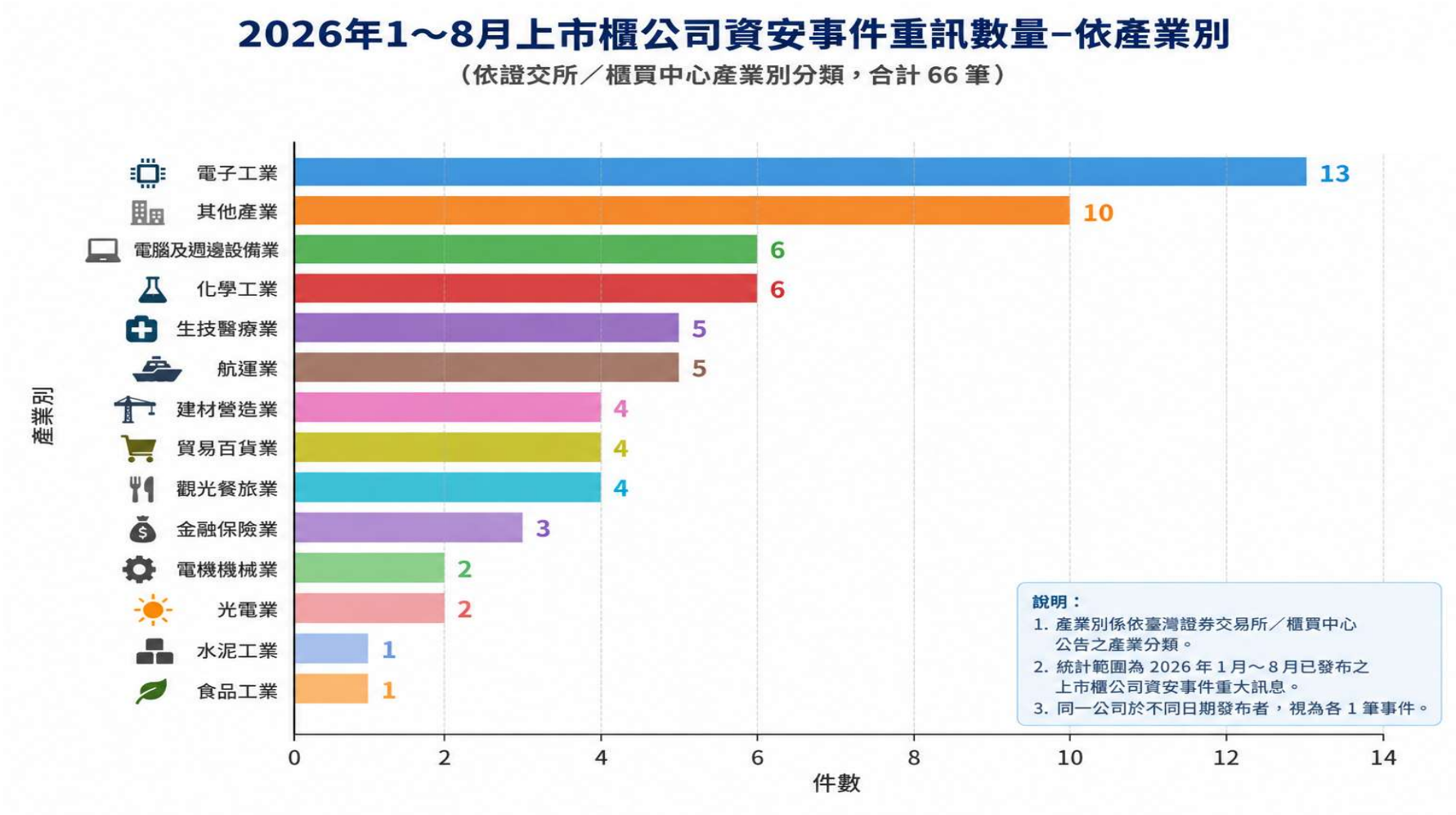
https://s.itho.me/vendor/2026/iThome/iThome_2026_State_of_CIO&CISO_Survey_FINAL-Part6-%E8%B3%87%E5%AE%89%E7%AD%96%E7%95%A5%E5%B8%83%E5%B1%80.pdf

2026年1~8月上市櫃公司資安事件統計



https://www.nics.nat.gov.tw/core_business/information_security_information_sharing/cybersecuritynews/

2026年1~8月上市櫃公司資安事件統計 (cont.)



https://www.nics.nat.gov.tw/core_business/information_security_information_sharing/cybersecuritynews/

被偷走的資料可能在暗網販售無數次

FTV FINANCE 民視財經網

獨家／馬偕再爆醫療資料外洩！駭客點名5醫 「竊密1.2TB」 規模暴增38倍

民視財經網
2026年5月26日

加入為 Google 偏好來源

民視新聞／蘇恩民報導

台灣醫療產業再度傳出重大資安警訊！去年2月馬偕紀念醫院遭知名勒索軟體CrazyHun擊，導致500多台電腦當機，看診系統一度癱瘓，當時駭客聲稱竊密32.5GB，引發社會資安與病患個資外流的關注，沒想到上周馬偕又爆更大規模資料外洩事件，本月18日駭The BlackH4t MD-Ghost點名馬偕全台5家醫院，聲稱取得2025-2026年合計高達1.2TB料，同時在駭客論壇PO出多份病患資料與檢驗系統紀錄作為佐證。

1.2TB與32.5GB的差距　不只是數字放大38倍

若將此次事件與去年 CrazyHunter 事件相比，最直接的差異便是資料規模。去年 CrazyHunter 對外公布的資料量約32.5GB，而此次 MD-Ghost 宣稱掌握的資料量高達1.2TB，相當於前次事件的 38 倍。

對資安調查人員而言，這個數字背後所代表的意義遠超過容量增加。32.5GB的資料量可能來自單一業務系統、檔案伺服器或部分資料庫內容；但當規模達到TB 等級時，通常意味著攻擊者已接觸到更大範圍的核心資訊資產，包括跨院區資料庫、歷史病歷、檢驗系統紀錄、內部文件以及其他關鍵資訊系統，也代表其取得的存取範圍與權限層級，很可能比外界目前所認知的更深入。

對此，馬偕醫院回應表示，本案經內部瞭解，疑似為2025年發生之駭客攻擊事件，而該起事件後，本院已嚴密進行資安維護與內部查核，監測網路流量均無異常。而昨天得知此事後，本院已向調查局報案，將全力配合檢調偵查，也再次呼籲，現今網路詐騙充斥，只要進行個資買賣或下載，都會觸犯個人資料保護法。患者若對本院就醫資訊有疑慮，可撥打資安服務電話：（02）2543-3535轉分機3564。

https://tw.stock.yahoo.com/news/%E7%8D%A8%E5%AE%B6%EF%BC%8F%E9%A6%AC%E5%81%95%E5%86%8D%E7%88%86%E9%86%AB%E7%99%82%E8%B3%87%E6%96%99%E5%A4%96%E6%B4%A9%EF%BC%81%E9%A7%AD%E5%AE%A2%E9%BB%9E%E5%90%8D5%E9%86%AB%E9%99%A2%E3%80%8C%E7%AB%8A%E5%AF%8612tb%E3%80%8D-%E8%A6%8F%E6%A8%A1%E6%9A%B4%E5%A2%9E38%E5%80%8D-034746048.html

WHY資產盤點與風險評估！？

- 資通安全管理法施行細則第9條
  - 本法第十三條、第二十條第二項及第二十一條第一項所定資通安全維護計畫，應包括下列事項：
    - 一. 核心業務及其重要性。
    - 二. 資通安全政策及目標。
    - 三. 資通安全推動組織。
    - 四. 專職人力及經費之配置。
    - 五. 資通安全長之配置。
    - **六. 資通系統之盤點，並標示核心資通系統及相關資產。**
    - **七. 資通安全風險管理。**
    - 八. 資通安全防護及控制措施。
    - 九. 資通安全事件通報、應變及演練相關機制。
    - 十. 資通安全情資之評估及因應機制。
    - 十一. 資通系統或服務委外辦理之管理措施。
    - 十二. 所屬人員辦理業務涉及資通安全事項之考核機制。
    - 十三. 十資通安全維護計畫與實施情形之持續精進及績效管理機制。

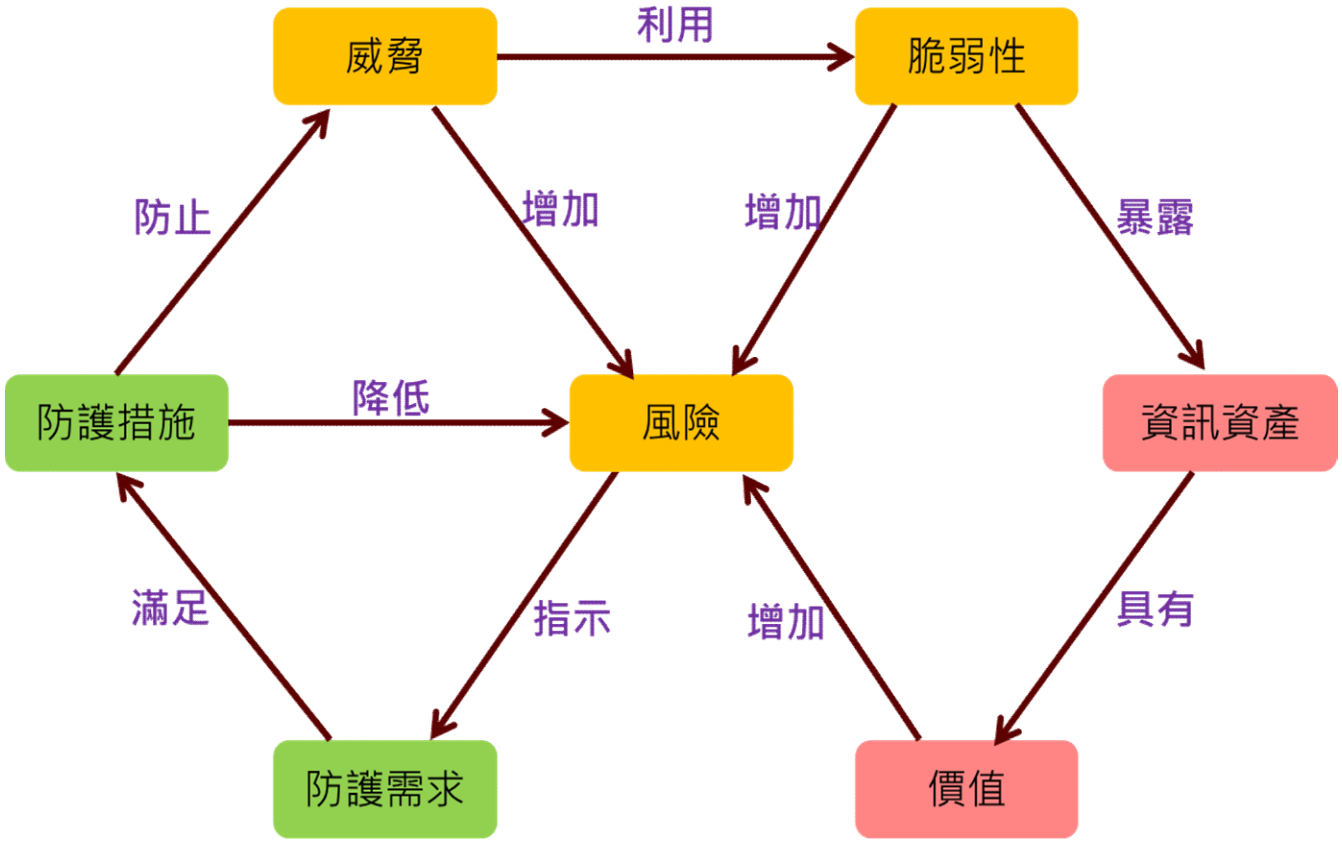
資通安全責任等級分級辦法應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級及其防護基準之妥適性。
	資訊安全管理系統之導入及通過公正第三方之驗證		全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，完成公正第三方驗證，並持續維持其驗證有效性。

WHY資產盤點與風險評估！？(cont.)

- 風險評估準則(CNS 27005)
  - 宜發展風險評估準則以評估組織之資訊安全風險，考量下列項目：
    - 營運資訊過程之策略價值
    - 所涉及資訊資產之關鍵性
    - 法令及法規要求，以及契約義務
    - 可用性、機密性及完整性之運作及營運重要性
    - 利害相關者之期望與感受，以及對商譽與聲譽之負面效果
- 範圍及邊界(CNS 27005)
  - 組織宜定義資訊安全風險管理之範圍及邊界
  - 需定義資訊安全風險管理過程之範圍，以確保風險評鑑已考量所有相關資產

風險管理流程關係圖(ISO13335)



資產盤點注意事項

資產與資訊

- 資產是甚麼？
  - 組織直接賦予價值並需要組織的保護
  - 相關於資訊安全管理系統的範圍
- 資訊是組織資產的一部份，具有價值且需要持續被適切地保護

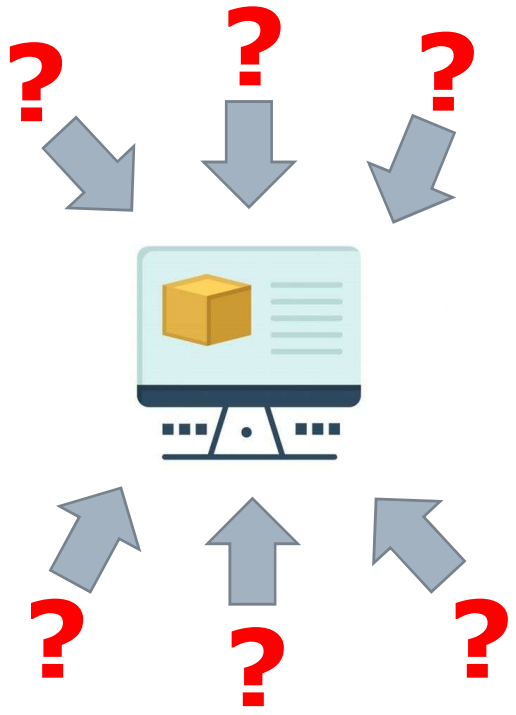


資產清冊建立

- 權責單位應建立「資訊資產清冊」
  - 清點及鑑別所管轄之資訊資產
  - 定期更新與維護
  - 彙整資訊資產清冊，陳報至資訊安全管理小組予以統一控管，確保資訊資產編號及清冊之完整性

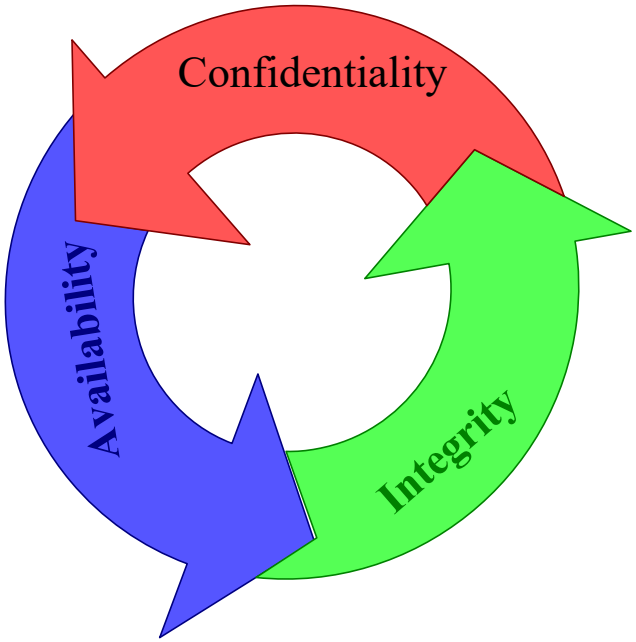
資產鑑別

- 資訊資產分類
  - 人員：同仁、廠商
  - 文件：紙本存在之文書資料，公文、報表等
  - 資料：存放於儲存媒介之數位資訊
  - 軟體：作業軟體、套裝軟體、原始碼、資料庫等
  - 通訊：網路設備、資訊傳輸或服務
  - 硬體：主機設備
  - 環境：基礎設施與服務、環控、電力



資訊資產價值鑑別

- 不被洩露與確保機密（機密性，C）
- 資訊、系統、服務等正確性被扭曲（完整性，I）
- 系統不會因破壞而影響持續運轉（可用性，A）



機密性評估標準

- 範例

評估標準	數值
一般：此資訊資產無特殊之機密性要求	1
限閱：此資訊資產含敏感資訊，但無特殊之機密性要求，且僅供組織內部人員或被授權之外部單位使用	2
敏感：此資訊資產僅供內部相關業務承辦人員存取	3
機密：此資訊資產所包含資訊為組織或法律所規範的機密資訊	4

完整性評估標準

- 範例

評估標準	數值
資產本身完整性要求極低	1
資產本身具有完整性要求，但是完整性被破壞不會對本會造成傷害	2
資產具有完整性要求，且完整性被破壞會對組織造成傷害，但不至於太嚴重	3
資產具有完整性要求，且完整性被破壞會對組織造成傷害，甚至會造成業務終止	4

可用性評估標準

- 範例

評估標準	數值
該資訊資產容許失效 3 天以上，不用被修復或是尋找替代品。	1
該資訊資產容許失效 8 小時以上，3 天以下，不用被修復或是尋找替代品。	2
該資訊資產容許失效 4 小時以上，8 小時以下，不用被修復或是尋找替代品。	3
該資訊資產容許失效 4 小時內不用被修復或是尋找替代品。	4

資產價值鑑別

- 資產價值=MAX(C,I,A)

  註：資產價值計算也可以是SUM(C,I,A) 或PRODUCT (C,I,A)

資產編號	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資產價值
HW-001	個人電腦	中心辦公室電腦20部	資訊中心	網管組	網管組	1	1	1	1
HW-002	重要系統主機	WWW、DNS、Mail、FTP、Proxy	資訊中心	網管組	網管組	2	2	4	4
HW-003	一般系統主機	一般伺服器硬體	資訊中心	網管組	網管組	1	1	2	2
SW-001	一般系統(軟體/應用程式)	知識管理系統	資訊中心	使用者	使用者	1	2	2	2
SW-002	重要系統(軟體/應用程式)	重要伺服器軟體	資訊中心	網管組	網管組	2	4	2	4

資產價值標示與使用

- 實體設備(沒有一定要標示)
  - 資產價值1→紅色
  - 資產價值2→綠色
  - 資產價值3→黃色
  - 資產價值4→藍色
- 文件資料
  - 一般、限閱、敏感、機密
- 程序書
  - 實體安全管理、存取控制管理、系統開發與維護...

資產管理循環



資產複核與銷毀

- 權責單位每年至少進行1次資產盤點與資產清冊複核。
- 當範圍內有以下的狀況發生之時，則實施不定期的複核
  - 有新增、變更或移除資訊資產
  - 系統有重大異動
  - 作業環境改變
- 資訊資產之報廢（或銷毀）應視其機密等級，採取適當之方式進行銷毀

資產盤點範例

產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	擁有者	機密性	完整性	可用性	資產價值
PE-001	PE	管理階層人員	校長、教務主任、資訊組長	人事室	人事室	人事室	1	1	1	1
PE-002	PE	網路、系統維護人員	代理資訊教師	人事室	人事室	人事室	1	1	1	1
PE-003	PE	一般使用人員	教職員	人事室	人事室	人事室	1	1	1	1
IF-001	IF	作業文件	資料庫與資料檔案、備份資料	教務處	資訊組	資訊組長	1	1	1	1
IF-002	IF	系統文件	網路架構圖	教務處	資訊組	資訊組長	1	1	1	1
IF-003	IF	資訊紀錄（電子/紙本）	啟用與報廢紀錄單、資訊工作日誌、系統特權帳號清單、設備進出紀錄表	教務處	資訊組	資訊組長	1	1	1	1
IF-004	IF	系統紀錄（Log）	防火牆Log紀錄(一個月一次)	教務處	資訊組	資訊組長	1	1	1	1
HW-001	HW	伺服器	學校Web主機	教務處	資訊組	資訊組長	1	1	1	1
HW-002	HW	其他硬體	印表機、影印機	總務處	總務處	總務處	1	1	1	1
HW-003	HW	個人電腦	桌上型電腦	教務處	資訊組	資訊組長	1	1	1	1
HW-004	HW	可攜式電腦	筆記型電腦	教導處	教導處	教導主任	1	1	1	1
HW-005	HW	資安設備	Zyxel防火牆	教務處	資訊組	資訊組長	1	1	1	1
HW-006	HW	網路設備	Zyxel交換器、L3交換器	教務處	資訊組	資訊組長	1	1	1	1
HW-007	HW	可攜式儲存媒體	USB、記憶卡、CD、DVD、投影機。	教務處	資訊組	資訊組長	1	1	1	1
SW-001	SW	作業系統	KMS	教務處	資訊組	資訊組長	1	1	1	1
SW-002	SW	資訊安全系統	防火牆軟體(Zyxel)	教務處	資訊組	資訊組長	1	1	1	1
EV-001	EV	一般辦公區域	辦公室、會議室。	學校	學校	學校	1	1	1	1
EV-002	EV	資訊機房	電腦機房	教務處	資訊組	資訊組長	1	1	1	1
EV-003	EV	建築保護設施	不斷電系統、穩壓器、機櫃、滅火器、發電機	總務處	總務處	總務處	1	1	1	1

類別：人員 (PE)、資訊 (IF)、硬體 (HW)、軟體 (SW)、環境 (EV)

表單之前，請確認表單版本是否已更新

資產盤點常見問題

- 盤點不完整
  - 既存設備、第三方元件
- 資訊不完整
  - 版本、型號、品牌
- 群組化不恰當
- 未正確識別資產價值

新聞

三星英國分公司第三方應用漏洞被駭，致客戶資料外洩

三星英國分公司證實近期發生網路攻擊事件，駭客利用該公司使用的第三方應用程式漏洞，盜走電子商務平臺用戶個資

https://www.ithome.com.tw/news/159944

新聞

合勤緊急修補NAS重大漏洞

影響合勤三款NAS產品的安全漏洞CVE-2023-27992，可讓未經驗證的攻擊者傳送惡意HTTP呼叫，而在NAS裝置OS上遠端執行指令，合勤在6月20日釋出更新版韌體

https://www.ithome.com.tw/news/157456

終止支援的產品

將於 2023 年終止支援下列受固定原則規範的產品與版本。

2023 年 10 月 10 日

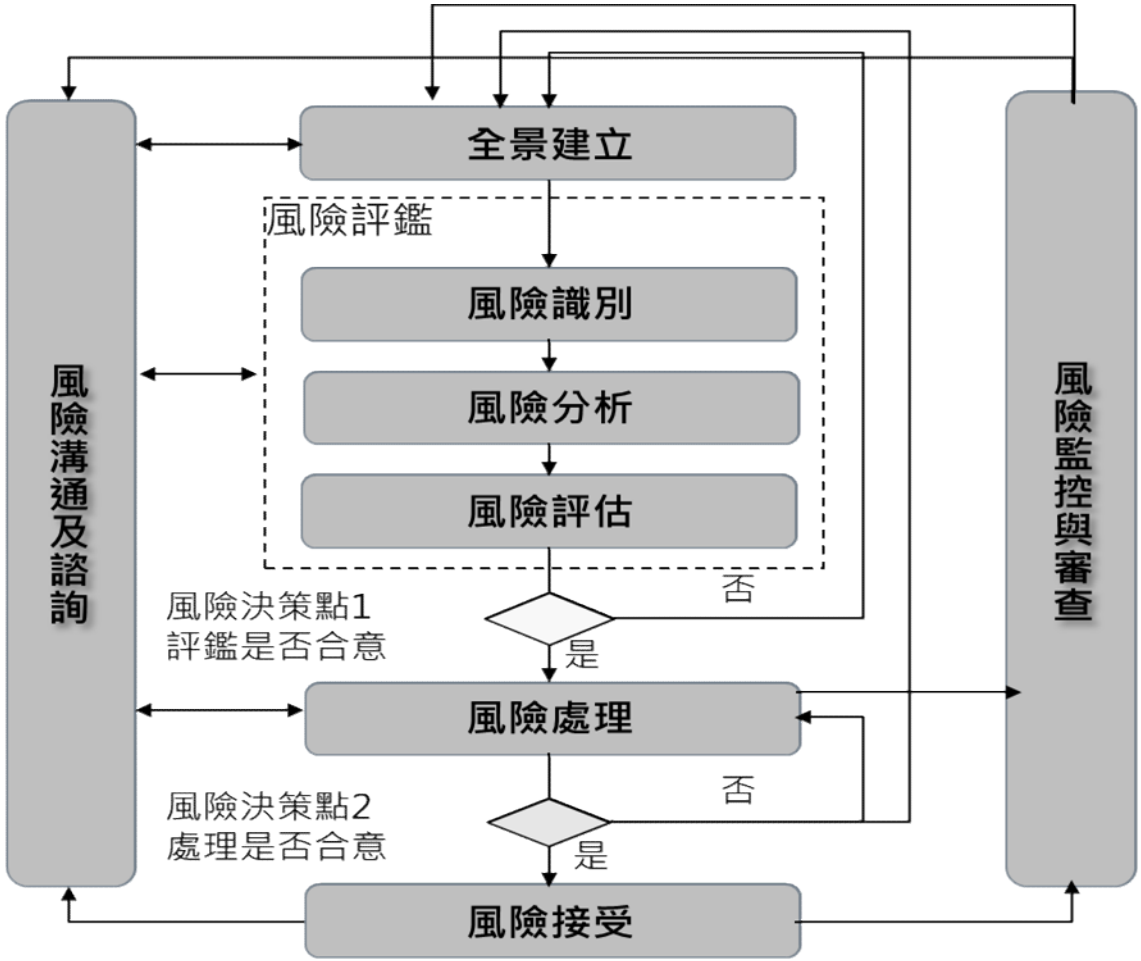
Excel 2019 for Mac
Hyper-V Server 2012
Hyper-V Server 2012 R2
Internet Explorer 7
Internet Information Services (IIS)、Windows Server 2012 上的 IIS 8
Internet Information Services (IIS)、Windows Server 2012 R2 上的 IIS 8.5
Mac 版 Microsoft Office 2019
Microsoft Office Audit and Control Management Server 2013
Mac 版 Outlook 2019
PowerPoint 2019 for Mac
Windows Embedded Compact 2013
Windows Embedded POSReady 7 延伸安全更新第 2 年*
Windows Embedded Standard 7 延伸安全更新第 3 年*
Windows MultiPoint Server 2012
Windows Server 2012
Windows Server 2012 R2
適用於 Windows Server 2012 的 Windows Server Update Service
適用於 Windows Server 2012 R2 的 Windows Server Update Services
Windows Storage Server 2012
Windows Storage Server 2012 R2
Word 2019 for Mac

風險評鑑與處理注意事項

資訊安全風險評鑑(ISO27001)

- 建立及維持包含下列準則之資訊安全風險準則
  - 風險接受準則
  - 執行資訊安全風險評鑑之準則
- 確保重複之資訊安全風險評鑑產生一致、有效及可比較的結果
- 識別資訊安全風險
  - 應用資訊安全風險評鑑過程，以識別資訊安全管理系統範圍內與喪失資訊之機密性、完整性及可用性相關聯的風險
  - 識別風險擁有者
- 分析資訊安全風險
  - 評鑑若所識別之風險實際發生時，可能導致的潛在後果
  - 評鑑所識別之風險發生的實際可能性
  - 判定風險等級
- 評估資訊安全風險
  - 以建立之風險準則，比較風險分析結果
  - 訂定已分析風險之風險處理優先序

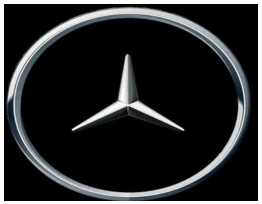
資訊安全風險管理過程(CNS27005)



資產的風險評估與處理

資產

價值與影響



自身弱點





外來威脅





外來威脅



需求評估
與控制



降低風險



轉移風險

接受風險



避免風險

風險(Risk)

- 風險是特定威脅利用弱點直接或間接造成組織一個或一群資產的損失或損害的可能性。

- Risk is the potential that a given threat exploit vulnerabilities to cause loss or damage to an asset or group of assets, and hence directly or indirectly to the organization.

威脅(Threat)

- 可能對系統或組織造成傷害之意外事件
  - 天災–洪水、暴風雨、地震、閃電
  - 人為–人員短缺、錯誤維護、使用者錯誤
  - 科技–網路故障、流量超過負荷、硬體故障
  - 蓄意的威脅
  - 意外的威脅
  - 威脅頻率

資訊資產可能面臨的威脅

人為因素		環境因素
計畫性	意外/隨機發生	
1.罷工、炸彈、武力、火災 2.蓄意破壞 3.偷竊 4.未經授權使用儲存媒體 5.偽裝合法使用者識別 6.惡意程式碼 7.非法輸入/出軟體 8.網路被未授權人使用 9.網路設備被未授權的方式使用 10.偷聽 11.通訊滲透 12.流量分析 13.更改訊息傳遞路徑 14.拒絕合作 15.資訊竄改 16.系統入侵 17.資源不當使用	1.水力,電力中斷 2.空調中斷 3.實體故障 4.操作錯誤及遺漏 5.維護錯誤 6.軟體錯誤 7.軟體被未授權的人使用 8.軟體被未被授權的方式使用 9.非法使用軟體 10.網路元件故障 11.傳輸錯誤 12.電路損毀 13.流量超過負載 14.檔案刪除 15.訊息的錯誤傳遞 16.網路服務中斷 17.員工不足 18.使用者造成錯誤	1.地震 2.閃電 3.水災 4.能源不穩定 5.溫度,溼度 6.灰塵 7.電磁輻射 8.靜電 9.儲存媒體退化

威脅等級(可能性)

- 範例

評估標準	評估值
威脅發生之可能性為低	1
威脅發生之可能性為中	2
威脅發生之可能性為高	3

弱點(Vulnerability)

- 因資訊資產本身狀況或所處環境之下，可能受到威脅利用而造成資產受到損害之因子。弱點本身不會造成傷害。
  - 關鍵人員的缺席
  - 不穩定的動力
  - 未保護的電纜線
  - 安全意識的缺乏
  - 密碼權限的錯誤分配
  - 安全訓練的不足
  - 未安裝防火牆
  - 未鎖的門

弱點等級(影響程度)

- 範例

評估標準	評估值
該弱點不容易被威脅利用	1
該弱點容易被威脅利用	2
該弱點非常容易被威脅利用	3

風險值

- 評估威脅發生的可能性及弱點受到威脅利用的容易度(影響程度)
  - 合理評估原則：經驗、過去的異常事件或資安事件、同業的狀況、資安通報或新聞.....等
- 風險值 = 資產價值 x 威脅等級 x 弱點等級
  - 能計算出風險值高低差異的方法即可
- 每種資訊資產可能有多種威脅利用多種弱點

風險評鑑

項次	資產編號	資產名稱	資產說明	權責單位	資產價值	風險事件		可能性	影響程度	風險值
						威脅	弱點			
1	HW-002	重要系統主機	WWW、DNS、Mail、FTP、Proxy	資訊中心	4	硬體故障	維護回應服務不足	2	3	24
2	SW-002	重要系統(軟體/應用程式)	重要伺服器軟體	資訊中心	4	軟體失效	缺乏測試程序	3	3	36
3	SW-002	重要系統(軟體/應用程式)	重要伺服器軟體	資訊中心	4	軟體失效	維護回應服務不足	3	2	24

風險評鑑範例

編號	資產類別	資產名稱	資產價值	威脅	弱點（被利用而造成威脅）	威脅等級（發生之可能性）			弱點等級（受到威脅利用之容易）			風險值
						低(1)	中(2)	高(3)	低(1)	中(2)	高(3)	
-PE-1	PE	管理階層人員	2	人員不足	缺乏職務代理機制	1			1			2
				人員不足	職責分工不當	1			1			2
				重要人員異動	工作負荷過重	1			1			2
				重要人員異動	缺乏適當之人事管理制度	1			1			2
				使用者失誤	複雜的使用者介面	1			1			2
				使用者失誤	教育訓練不足	1			1			2
				操作失誤	複雜的操作介面	1			1			2
				操作失誤	操作文件不足	1			1			2
				操作失誤	專業訓練不足	1			1			2
				操作失誤	機密資料的外洩(E-mail or 儲存媒體)	1			1			2
				資料外洩	缺乏人員安全審查程序	1			1			2
				使用非法軟體	未使用合法版權軟體或下載受控管之軟體	1			1			2
				使用非法軟體	未定期審查軟體使用情形	1			1			2
-PE-2	PE	網路、系統維護人員	2	人員不足	缺乏職務代理機制	1			1			2
				人員不足	職責分工不當	1			1			2
				重要人員異動	工作負荷過重	1			1			2
				重要人員異動	缺乏適當之人事管理制度	1			1			2
				使用者失誤	複雜的使用者介面	1			1			2
				使用者失誤	教育訓練不足	1			1			2
				操作失誤	複雜的操作介面	1			1			2
				操作失誤	操作文件不足	1			1			2
				操作失誤	專業訓練不足	1			1			2
				操作失誤	機密資料的外洩(E-mail or 儲存媒體)	1			1			2
				資料外洩	缺乏人員安全審查程序	1			1			2
				使用非法軟體	未使用合法版權軟體或下載受控管之軟體	1			1			2
				使用非法軟體	未定期審查軟體使用情形	1			1			2
-PE-3	PE	一般使用人員	2	人員不足	缺乏職務代理機制	1			1			2
				人員不足	職責分工不當	1			1			2
				重要人員異動	工作負荷過重	1			1			2
				重要人員異動	缺乏適當之人事管理制度	1			1			2
				使用者失誤	複雜的使用者介面	1			1			2
				使用者失誤	教育訓練不足	1			1			2
				操作失誤	複雜的操作介面	1			1			2
				操作失誤	操作文件不足	1			1			2

風險處理-計畫

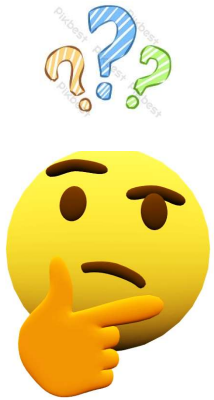
- 風險處理計畫是定義行動以降低無法接受的風險，和實施所需的控制措施以保護資訊的一種「合作文件」
  - 針對高風險(超過可接受風險)項目或認為應該要處理的項目
  - 避免偶發、特殊或超過組織處理能力的風險
  - 預估風險處理後之殘餘風險(若無法低於可接受風險即應重新擬定風險處理計畫)



風險處理-方向

- 接受殘餘(剩餘)的風險
- 避免風險
- 轉移風險
- 降低風險到可接受程度







可接受風險的等級

- 要達到完全的安全是不可能的
- 總是有殘餘的風險
- 甚麼樣程度的剩餘風險能為組織所接受

〔即時新聞／綜合報導〕嚇死人！新竹竹北大風來襲，路上的紅路燈被吹倒，有車輛當場受到波及，所幸車主沒有大礙。

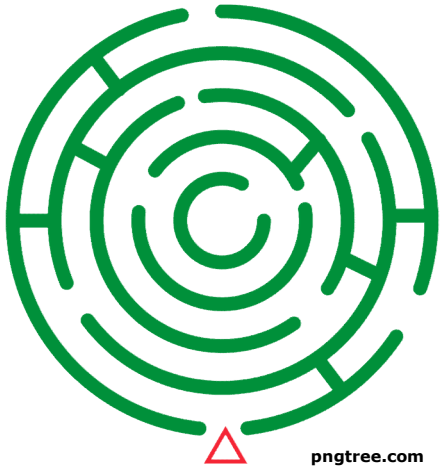
在東北季風、熱帶性低氣壓外圍環流的影響下，北部多處地區下起豪大雨，全台18個縣市也出現強風，「我們新竹竹北的風不是開玩笑的大」，有網友在臉書社團「爆廢公社」分享新竹竹北某處道路的行車紀錄器畫面，可以看到道路中央的紅綠燈突然倒下，硬生生直接倒在車子上，擋風玻璃被砸出裂痕，駕駛嚇到當場飆髒話，所幸無人傷亡，恐怖畫面讓原PO不禁驚呼，「這個風都可以演絕命終結站了」。

資料來源：自由電子報



風險處理

- 地點
- 已存在的安全
- 攻擊者的數量
- 可用的設施
- 累積的機會
- 宣傳層次
- 營運持續計畫

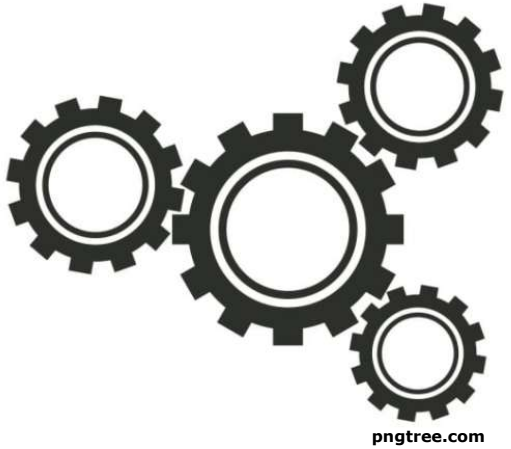


風險處理(cont.)

- 定義一個可接受的殘餘風險等級(可接受風險)
- 持續的審查威脅和脆弱性
- 對已存在之安全控制措施的審查
- 應用其他的安全控制...ISO 27001(ISMS)
- 政策和程序介紹

控制措施的選擇

- 針對風險
- 要求的保證程度
- 成本考量
- 實施的容易性
- 服務內容
- 法律和法規的要求
- 客戶和其他的合約要求



成本

- 預算限制
- 應用控制措施的成本是否會超過資產的價值？
- 也許必須選擇〝最佳價值〞範圍內的控制措施



實施的容易性

- 環境是否支援控制措施？
- 控制措施需要多久才有辦法開始實施？
- 控制措施是否立即可用的？



服務

- 可獲得的技術是否能夠管理控制措施？
- 是否能夠立即的升級？
- 設備是否有當地工程師/協力廠商的支援？



最佳作業的控制措施

- 資訊安全政策文件
- 資訊安全責任的分配
- 資訊安全教育和訓練
- 報告安全意外事件
- 營運持續管理



營運持續計畫生命週期（Business continuity planning life cycle）的中文翻譯

https://zh.wikipedia.org/zh-tw/%E7%87%9F%E9%81%8B%E6%8C%81%E7%BA%8C%E8%A8%88%E7%95%AB#/media/File:Business_continuity_planning_life_cycle's_chinese_translation.png

經過事件的淬鍊方知風險所在

台鐵網站、訂票App大停擺 通勤族氣跳腳 官網公告：系統維護

2026-07-08 06:35 聯合報／記者楊德宜／台北即時報導

+ 台鐵

國營臺灣鐵路股份有限公司

臺鐵公司票務機房冰水主機異常，經緊急處理後於今（8）日早上6:23恢復正常服務

發佈日期：2026/7/8 上午 8:50

臺鐵公司票務系統今日（7/8）早上2:53左右經監測發現票務機房冰水主機異常，於第一時間啟動緊急應變機制，通報車站改為離線版售票模式，並全力進行故障排除及系統復原作業。經處理，上午6時23分已恢復票務系統正常服務，目前持續監控設備及系統運行情形，確保票務服務穩定。

此次票務系統異常期間，造成旅客購票及相關票務服務不便，臺鐵公司深表歉意，並感謝旅客的體諒與配合。

temporarily. We're sorry for any inconveniences.

公司地址：臺北市中正區北平西路三號（郵遞區號100230）
公司電話：(02)2381-5226
版權所有 © 2024 國營臺灣鐵路股份有限公司 Taiwan Railway Corporation, Ltd.

https://udn.com/news/story/7266/9613878

風險評鑑常見問題

- 風險評鑑執行過於僵化
  - 萬年不變的無高風險結果
  - 可接受風險值設定過高或不符現況需求
- 忽略可能的殘餘風險
  - 他山之石可以攻錯
  - 未能蒐集與分析相關資安訊息
- 為了改善而改善



https://www.hudsonrock.com/fortinet

AI 摘要

「FortiBleed」事件**導致全球逾 7.3 萬台 Fortinet 裝置（包含 FortiGate 防火牆）的 VPN 憑證外洩，臺灣受影響數量高居全球第三**。攻擊者可竊取憑證並攔截 VPN 流量，進而繞過安全管制、橫向移動入侵內網，對跨國企業及關鍵基礎設施構成嚴重資安威脅。 iThome +3

企業具體防範與應對建議：

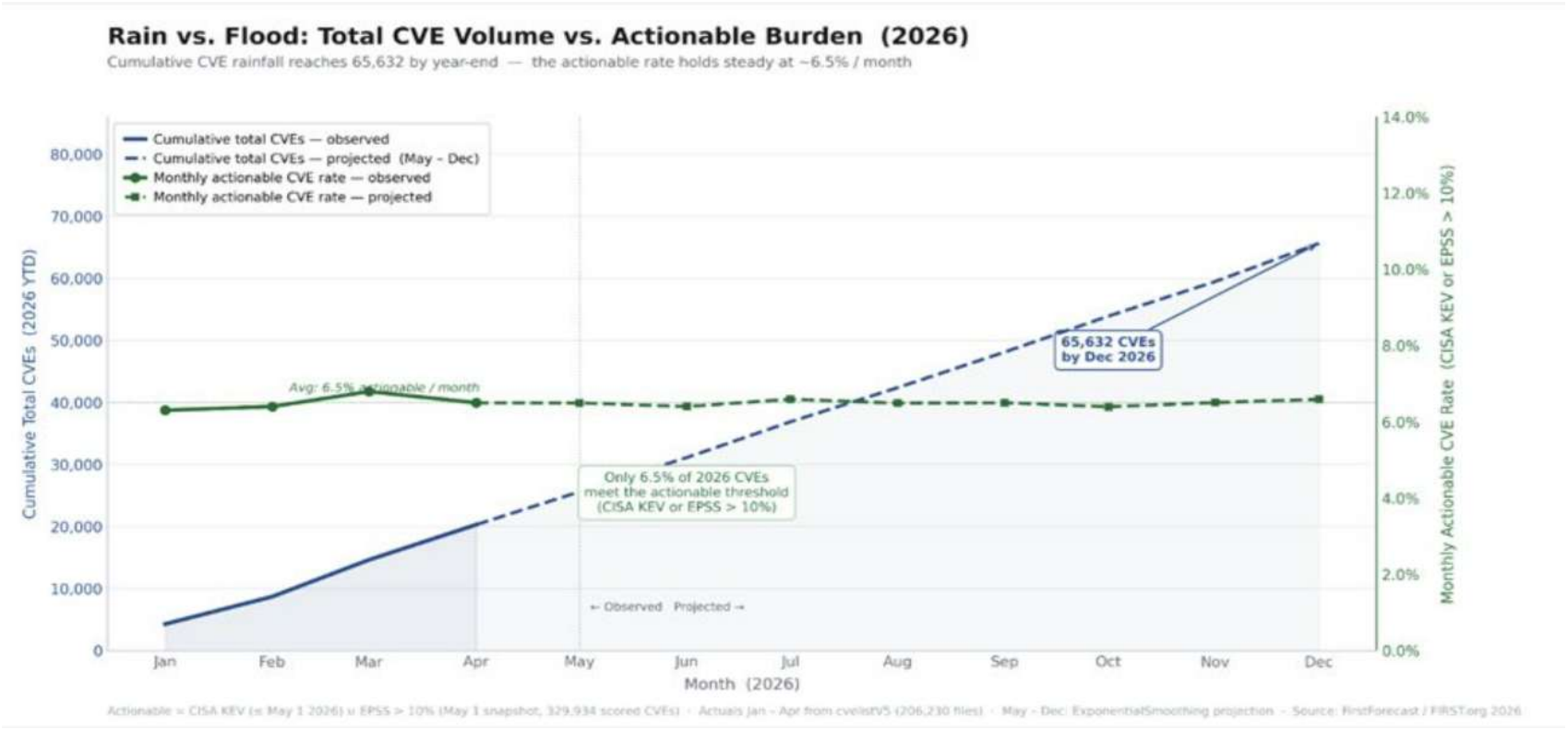
1. **關閉公網曝險：** 立即停止將 FortiOS 管理介面直接暴露於網際網路。
2. **更新與強化防護：** 儘速將 FortiOS 升級至最新版本。
3. **憑證與登入管理：** 強制所有管理員重新登入，並改用 PBKDF2 雜湊。
4. **啟用多因素驗證 (MFA)：** 全面啟用 MFA 以防堵憑證外洩後的未授權存取。
5. **官方指引查閱：** 詳閱 數位發展部國家資通安全研究院 (NICS)

可能的潛在風險-CVE漏洞數量大增

https://www.ithome.com.tw/news/176666

新聞

CVE漏洞數量大增，FIRST進一步說明致災風險並未隨總量而增加的理由



可能的潛在風險-CVE漏洞數量大增

https://www.ithome.com.tw/news/175144

新聞

漏洞數暴增263%，NIST縮減CVE分析範圍轉向風險優先

隨CVE數量5年暴增263%，美國國家標準暨技術研究院（NIST）坦言已無法全面分析漏洞，改採「風險優先」策略，僅優先處理已被利用與關鍵系統漏洞，其餘將列為Not Scheduled

文/ 陳曉莉 | 2026-04-17 發表



以cvss分數來判斷漏洞的嚴重性並不準確

NIST表示，此次調整主因在於CVE數量快速成長已超出處理能力，2020年至2025年間漏洞數量暴增263%，2025年新增約4.8萬筆CVE，比前一年多出45%，且即便去年已完成約4.2萬筆漏洞分析，仍無法跟上新增速度；而2026年前三個月提交量亦比去年[illegible]約三分之一，導致NVD持續累積大量未處理案件。

[illegible]所有漏洞提供分析與評分已不可持續，因此改採風險導向策[illegible]處理已被利用或具關鍵影響的漏洞。而未被列入優先分析範圍的CVE，將被歸類為未排程（Not Scheduled）。

具體而言，NIST將不再全面分析所有漏洞，而是優先處理已被美國網路安全暨基礎設施安全局（CISA）列為已知遭利用漏洞清單（Known Exploited Vulnerabilities，KEV）的項目，目標是在一個工作天內完成分析，同時也會優先處理政府與關鍵系統相關漏洞。

可能的潛在風險-供應鏈攻擊

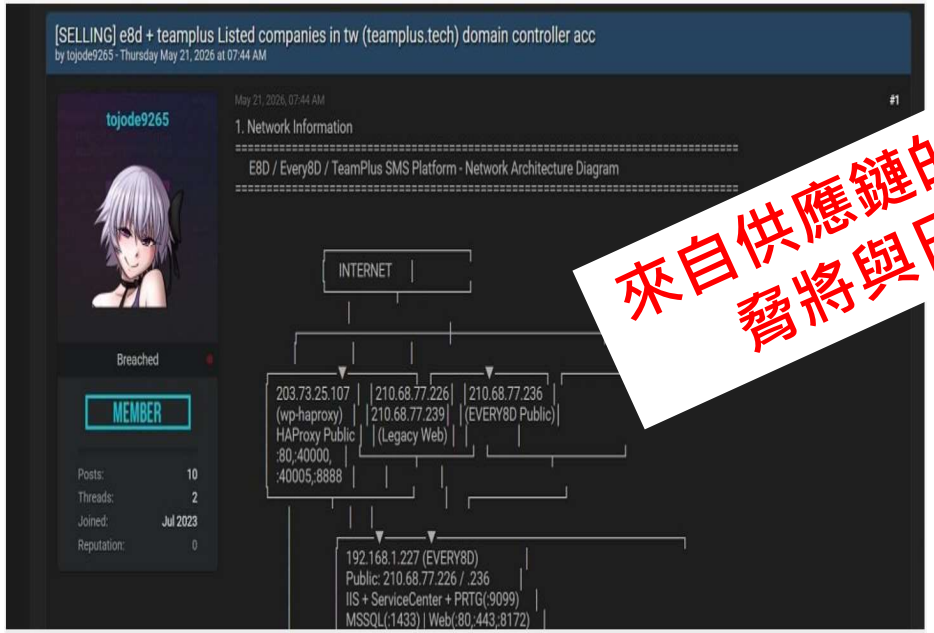
https://www.ithome.com.tw/news/176142

新聞

市占第一OTP簡訊平臺EVERY8D遭駭，F-ISAC發布黃燈級資安事件警訊

臺灣資服務業互動資通，旗下全臺市占第一的企業簡訊龍頭EVERY8D，日前疑遭勒索軟體入侵，包括網路拓樸與簡訊平臺相關內容等機敏資料遭外洩，並於駭客論壇公開兜售；社群媒體瘋傳企業簡訊服務癱瘓已逾一週，牽動銀行、電商、金流業者的身分驗證命脈，供應鏈資安韌性也面臨重大考驗。

文/ 黃彥棻 | 2026-05-26 發表



知名駭客地下論壇，駭客以「SELLING」為標題，公開兜售互動資通的上市公司網域控制器帳號，以及EVERY8D企業簡訊平臺的相關資料。

來自供應鏈的資安威脅將與日俱增

根據駭客論壇公布的外洩網路架構圖與拓樸可以顯示，駭客應該早就已經深度潛伏於互動資通的內網中，將第一層反向代理伺服器（HAProxy）、內部主機名稱、IP位址配置、[illegible]結構以及服務連接埠資訊全部摸透。從外洩的資訊更可以看到[illegible]SH遠端管理服務更直接暴露在外網，讓駭客有長驅直入的通[illegible]

[illegible]壇的外洩資訊顯示，互動資通內部多達兩百多臺活躍主機、簡訊[illegible]（ServiceCenter）、排程元件（RabbitMQ），以及用於硬體層級控制[illegible]LO管理介面，均遭到全面控制。

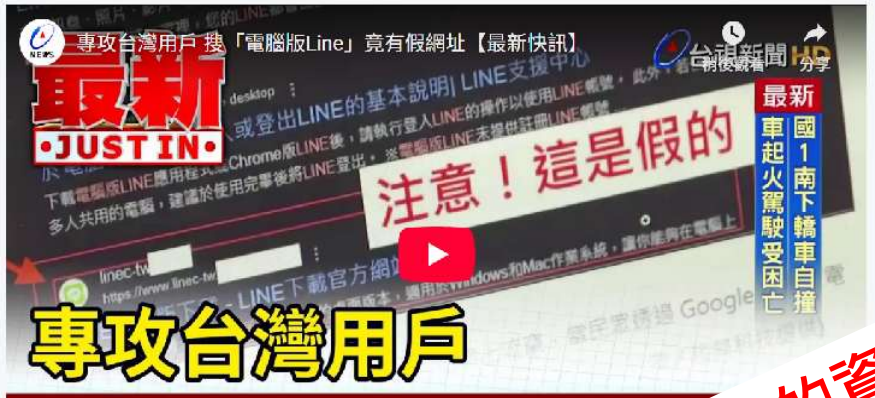
最讓人擔心的是，駭客已經成功攻破生產環境的微軟網域控制器（Domain Controller），掌握網域之間的最高信任關係。這意味著駭客已奪取了企業IT環境的最高權限帳號，能夠以最高管理員身分，在整個網路中自由地橫向移動、讀取任意機敏資料。

駭客為了證明已經確實掌握EVERY8D企業簡訊平臺，更直接在駭客論壇上，公布涉及臺灣五院、總統府、軍隊、各部會，以及民眾的真實簡訊的日誌紀錄，甚至連文化部驗證碼、軍醫院收發室聯絡訊息與政治核心輿情都被駭客公開；隨後服務主機也被鎖上加密勒索訊息，顯示其防禦體系已被徹底瓦解。

可能的潛在風險-誤載惡意程式與不慎點選惡意郵件

https://www-api.moda.gov.tw/File/Get/acs/zh-tw/ynSogYbKmbnxlFE

「電腦版LINE」竟有假網址！專攻台灣用戶 下載個資恐外洩



近期有駭客集團假冒通訊軟體LINE的電腦版應用程式，若民眾不[illegible]木馬程式，導致個資外洩。

知名網路資安廠商指出，駭客慣用木馬程式攻擊，並包含將其包裝成熱門APP或知名搜尋引擎等，誘騙民眾誤點，近期發現有木馬程式假冒LINE電腦版應用程式。

廠商表示，當民眾透過Google搜尋「電腦版LINE」，可能會在搜尋結果看到不同類型仿造的假網址，這類網頁內容大多為繁體中文，顯示這起攻擊針對台灣使用者。一旦民眾點選假冒網站下載，電腦便會被植入惡意木馬程式，恐怕導致個資外洩，並讓駭客取得裝置的存取與控制權，甚至感染到其他連線裝置等。例如搜尋後看到www[.]linee-tw[.]000、line-chinese[.]000、line-tw[.]000、windows-line[.]000等，就是仿造的假網址。

https://news.ttv.com.tw/news/114041200057005/amp

免費軟體暗藏陷阱！勿莫名成為攻擊跳板，請使用者提高警覺!

上版日期：2023-08-15

隨著數位時代的蓬勃發展，免費軟體已融入人們的生活，然而最近Bright Data（前身為Luminati Networks）公司代理之服務被不肖份子濫用，使個人設備成為攻擊跳板，並造成國內知名租賃公司大批會員帳號遭受入侵，再次喚醒我們警覺免費軟體背後潛在的風險。本文提供移除惡意程式之建議，[illegible]經安裝過相關免費軟體之使用者盡快處理，以免淪為攻擊打手。

[illegible]軟體（FormatFactory、Alcohol或HOLA VPN），隨即啟動BrightData Service，即Proxy [illegible]_updater64.exe程序。使用者之設備即成為BrightData公司所屬代理服務器（即BrightData公司網路節[illegible]系團則利用BrightData公司所屬網路節點入侵攻擊目標，而使用者之電腦或手機莫名被利用作為攻擊跳板。

使用者的資安觀念仍需持續加強

建議措施:

移除跳板程式，步驟如下:

1. 移除「C:\ProgramData\BrightData」路徑下所有檔案（取消隱藏）。
2. 移除上述免費軟體路徑下所有檔案。
3. 以工具Autoruns.exe或procexp.exe檢查程序net_updater64.exe、net_updater32.exe及brightdata.exe或服務Brightdata Service是否持續運行；若有，則將該程序所在資料夾內檔案移除。

https://www.cc.ntu.edu.tw/chinese/cert/cert20230815.asp

可能的潛在風險-供應鏈因遭遇資安事件致系統受牽連服務中斷

https://www-api.moda.gov.tw/File/Get/acs/zh-tw/ynSogYbKmbnxlFE

微軟當機「台大醫院也受衝擊」　門急診、住院一度暫停

民視新聞網

更新於 2024年07月19日16:21 • 發布於 2024年07月19日16:19

追蹤



即時中心／顏一軒報導

微軟今（19）日下午傳出大當機的消息，稍早網路安全公司「CrowdStrike」認了是其更新出狀況釀禍。不只美國911、銀行及機場航班受到衝擊，台灣的台大醫院門診、住院與急診稍早都傳出暫停的消息。對此，院方早證實，院內報到、影像等與Windows等系統確實受到影響，但不到半小時就已經順利復原。

微軟大當機　桃機6航空採人工劃位

#交通　#震宇　#桃機　#微軟　#當機　more

蔡明、李侑珊／台北報導

資安公司「CrowdStrike」於19日進行資安更新時出現問題，導致全球微軟用戶電腦出現藍屏當機現象，並於當天波及全球各行各業，其中對航空業影響最為嚴重。而桃園國際機場有8家航空公司遭波及，離境報到卡關，6家緊急改採人工劃位，地勤人員埋頭苦寫，櫃檯大排長龍，有旅客因此等候超過2小時，更苦笑「第一次拿到手寫機票」。台鐵公司與台灣高鐵公司皆表示，營運未受影響。

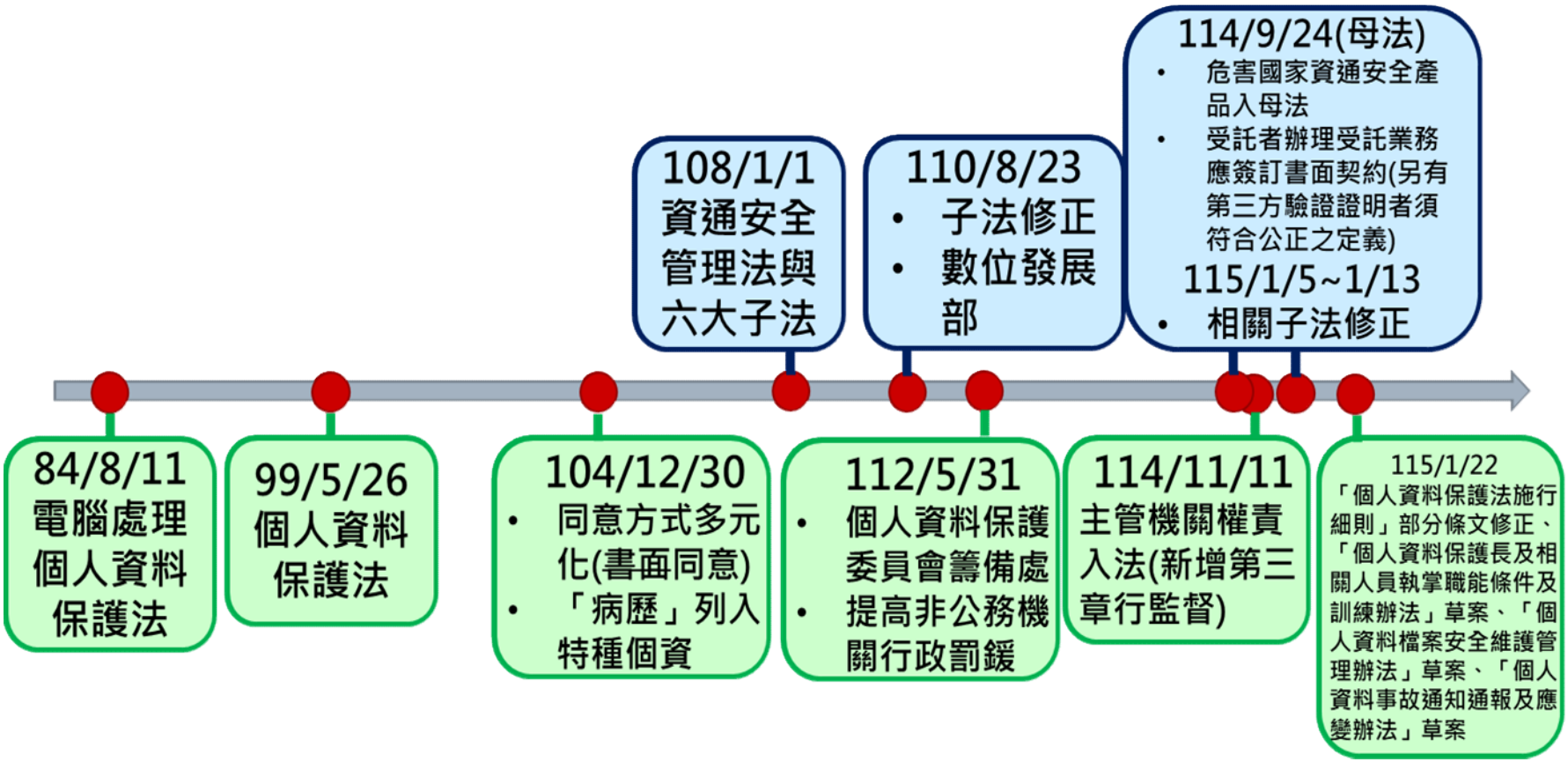
資安工具也可能是造成資安事件的元兇

https://news.housefun.com.tw/news/article/147366430899.htm

https://today.line.me/tw/v2/article/60eKJY1

結論

法規修正歷程


84/8/11
電腦處理個人資料保護法
99/5/26
個人資料保護法
104/12/30
• 同意方式多元化(書面同意)
• 「病歷」列入特種個資
108/1/1
資通安全管理法與六大子法
112/5/31
• 個人資料保護委員會籌備處
• 提高非公務機關行政罰鍰
110/8/23
• 子法修正
• 數位發展部
114/11/11
主管機關權責入法(新增第三章行監督)
114/9/24(母法)
• 危害國家資通安全產品入母法
• 受託者辦理受託業務應簽訂書面契約(另有第三方驗證證明者須符合公正之定義)
115/1/5~1/13
• 相關子法修正
115/1/22
「個人資料保護法施行細則」部分條文修正、「個人資料保護長及相關人員執掌職能條件及訓練辦法」草案、「個人資料檔案安全維護管理辦法」草案、「個人資料事故通知通報及應變辦法」草案

IT共同發現事項-策略面

1 系統備份及備援機制未臻妥適

- ⚠ 高等級資通系統未辦理異地備份
- ⚠ 未定期驗證備份媒體可靠性及備份資訊完整性
- ⚠ 未妥適評估RPO(資料復原點目標)、RTO(復原時間目標)及MTPD(最大可容忍中斷時間)

2 業務持續運作演練規劃未臻完善、未涵蓋備份還原測試

- ⚠ 未納入新興資安威脅及複合式情境、無業務單位參與
- ⚠ 演練範圍未包含全部核心資通系統
- ⚠ 高等級系統未將系統備份還原納入演練

3 系統分級及防護基準

- ⚠ 無系統分級評估紀錄，且無核定程序
- ⚠ 未依C(機密性)、I(完整性)、A(可用性)、L(法律遵循性)綜整評估系統分級妥適性
- ⚠ 系統分級未建立客觀或量化之一致性衡量標準

資料來源：資安署114年資安稽核結案會議簡報

IT共同發現事項-管理面

1 未落實委外管理措施

- ⚠ 未定期稽核廠商執行情形、無後續追蹤改善機制
- ⚠ 未建立系統第三方元件清單
- ⚠ 機關未自行或另行委託第三方進行安全性檢測

2 未確實盤點資產、盤點範圍未涵蓋全機關

- ⚠ 部分資產漏未盤點、未建立資產異動管理程序
- ⚠ 僅盤點資訊單位維運管理之設備
- ⚠ 資產清冊與實際情形不符

3 資安風險評估機制未臻妥適

- ⚠ 僅由資訊單位負責風險評鑑作業，未納入業務單位
- ⚠ 未適當檢討可接受風險值
- ⚠ 未針對委外業務項目進行風險評估

資料來源：資安署114年資安稽核結案會議簡報


QUESTIONS
ANSWERS