



長庚科技大學

113年度資通安全教育訓練

☑資通安全系列課程

★課程名稱：資訊安全威脅趨勢與防護作為

★授課日期：113.06.27

★授課時數：3 小時



講師：鍾文魁 Mark

學歷：東吳大學法律學系科技法律組 碩士
(關鍵資訊基礎設施保護法制面建構與分析)

華梵大學資訊管理學系資通安全組 碩士
(惡意電子郵件攻擊之研究)

經歷：



大綱

一 資訊科技發展

二 常見網路攻擊手法

三 面對網路攻擊威脅應有之認知與作為

四 結論

大綱子題

一 資訊科技發展

1 資訊科技發展趨勢

2 資訊安全威脅現況

一 資訊科技發展

資訊科技發展



5G行動通訊

Chat GPT

自駕車

物聯網

智慧城市

Others...



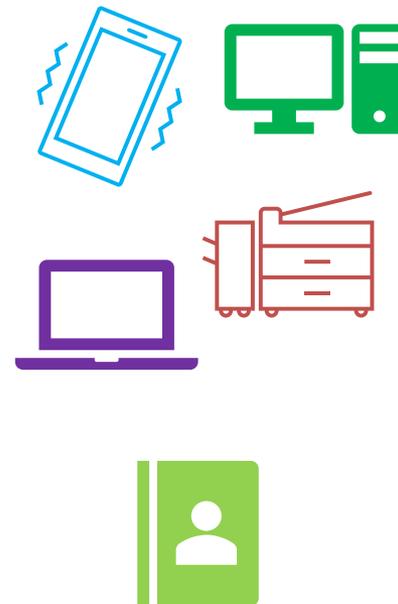
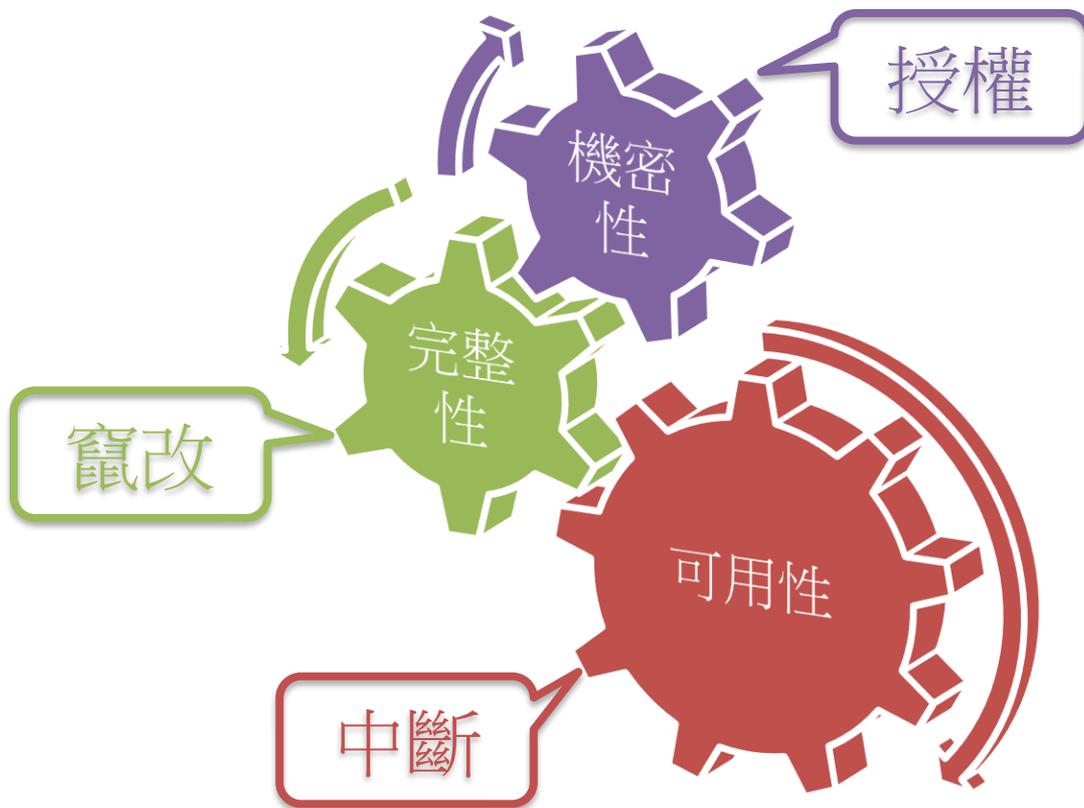
萬物聯網所帶來的便利

??



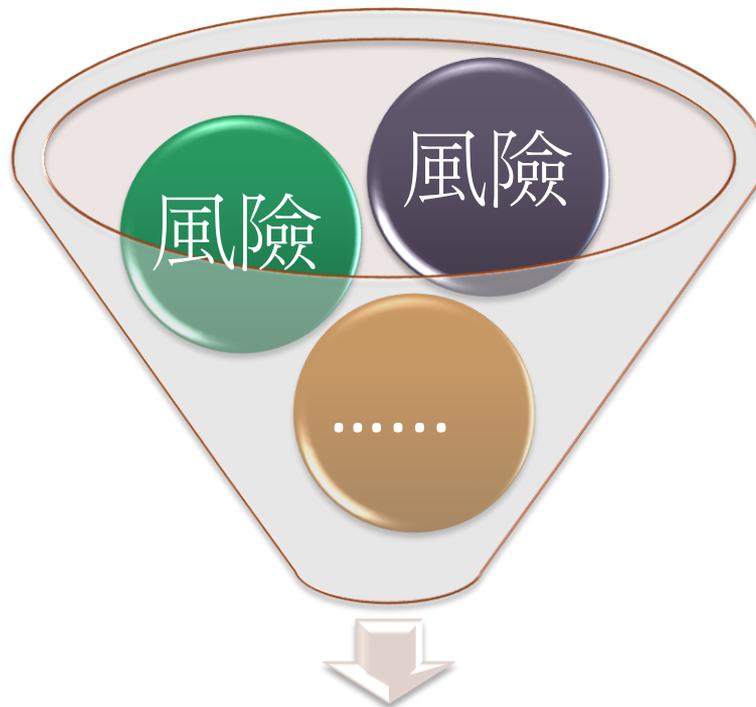
一 資訊科技發展

資通安全核心



一 資訊科技發展

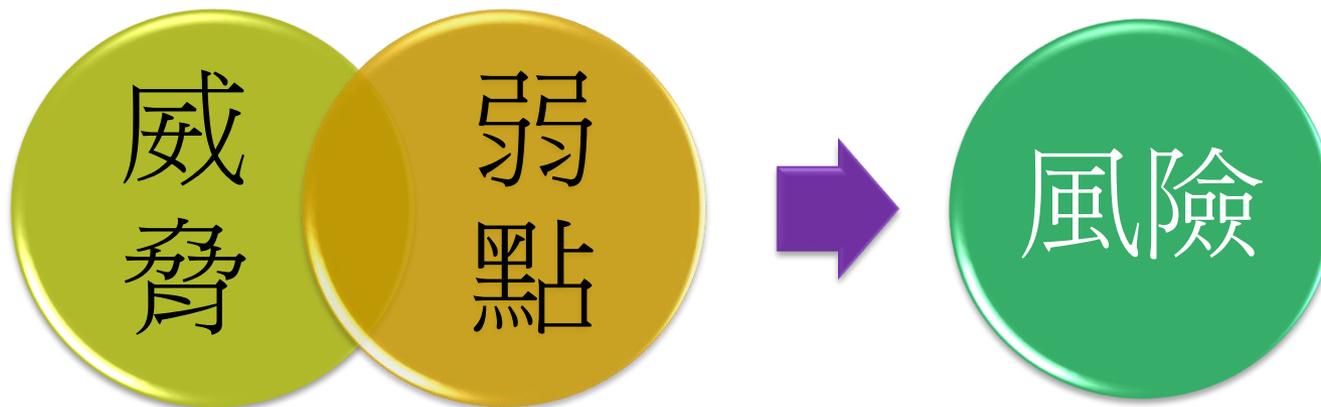
資通安全
風險管理



資通安全解決的問題

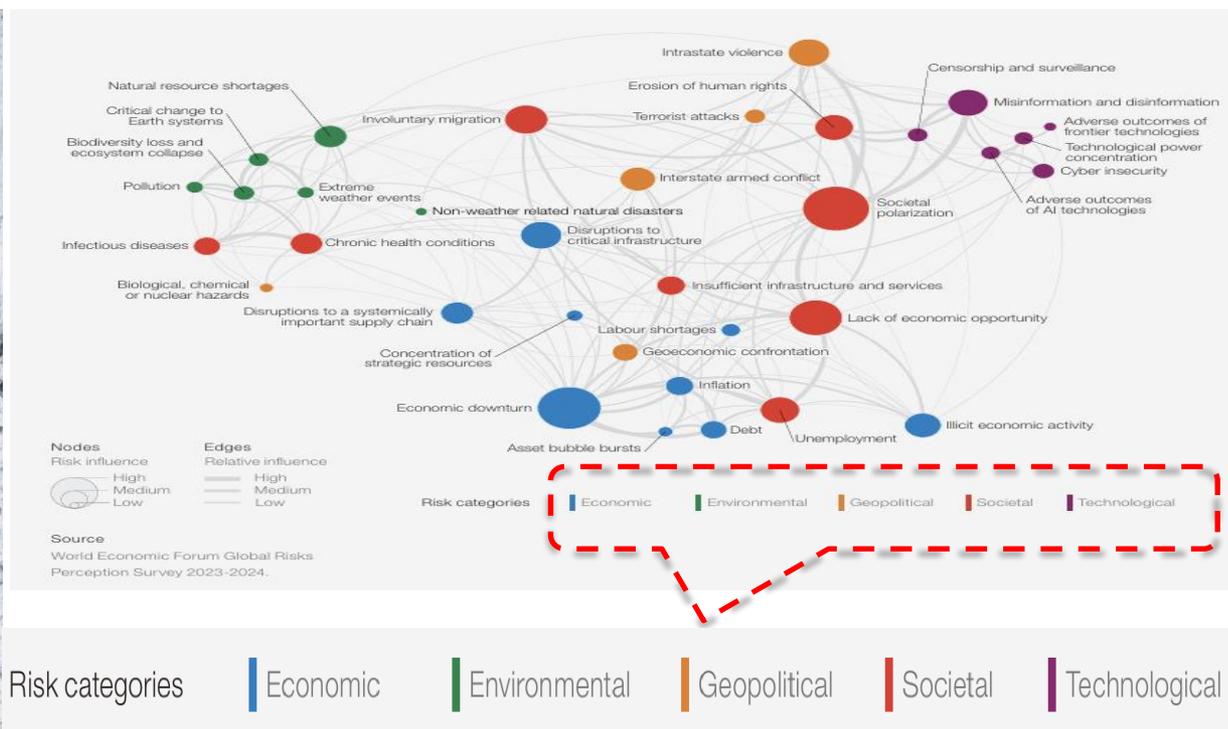
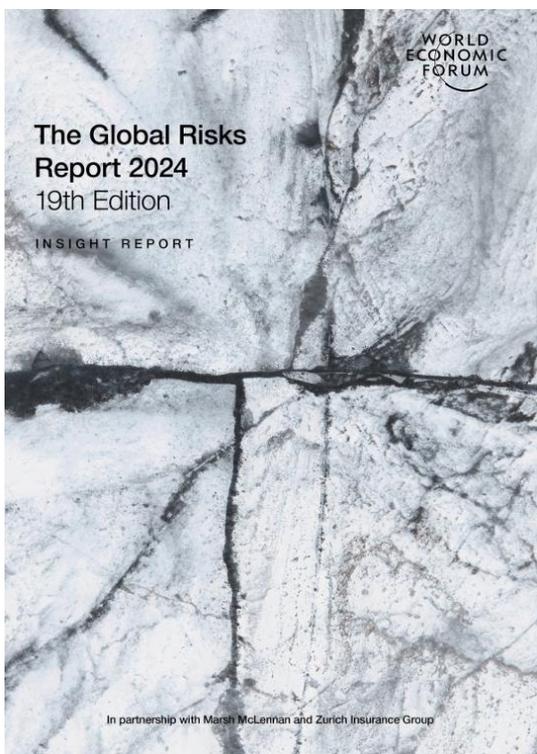
一 資訊科技發展

資通安全
風險管理



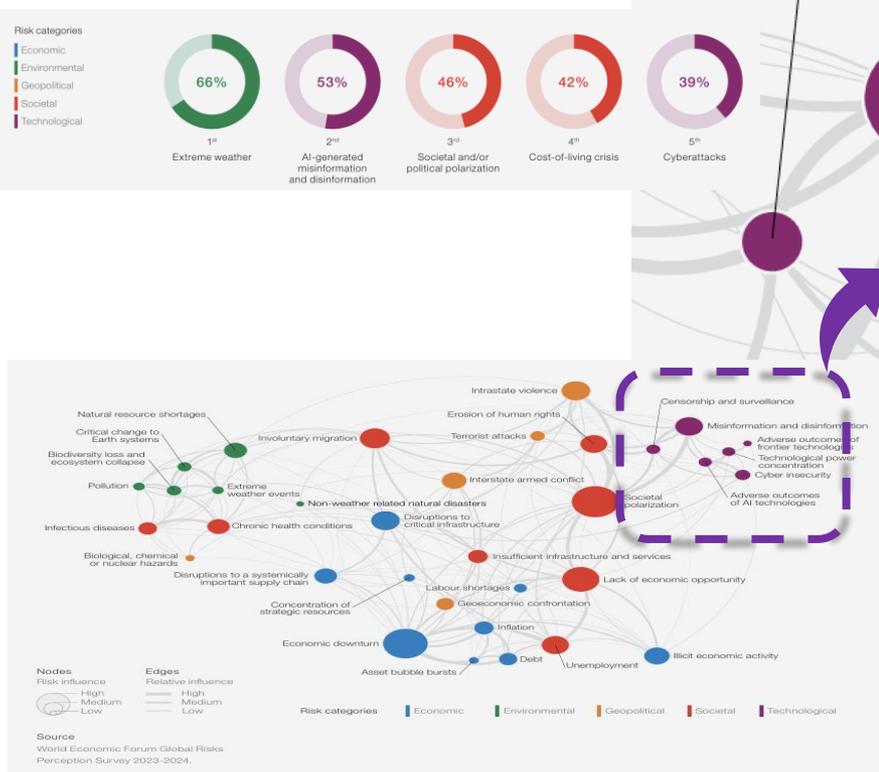
一 資訊科技發展

資訊安全 威脅現況



一 資訊科技發展

資訊安全 威脅現況



Censorship and surveillance

fake news

Misinformation and disinformation

Adverse outcomes of frontier technologies

Technological power concentration

Cyber insecurity ★

Adverse outcomes of AI technologies

一 資訊科技發展

資訊安全 威脅現況

傳產西進 遭商業間諜入侵系統

作者：張維君 -11/28/2011



許多企業認為自己不是機敏政府單位、也不是知名大廠，不會是駭客攻擊目標。但現今傳出有傳統產業業者到大陸設廠擴點，就被對手僱用商業間諜駭客入侵系統，導致商業機密疑似外洩。西進大陸前，請先做好資安。即便不是設點，只是一般商務出差，也有人使用智慧手機連接無線網路使用 Skype 通話，導致談話內容全被側錄外洩，研判是因為連結到偽冒的無線基地台。出差大陸前，請先確保行動裝置安全。上週六在淡江大學舉辦的2011聯合國際研討會，與會專家談到現今企業成爲入侵攻擊目標的問題已逐漸擴大。

資安人
INFO SECURITY
作對事、用對方法、找對夥伴

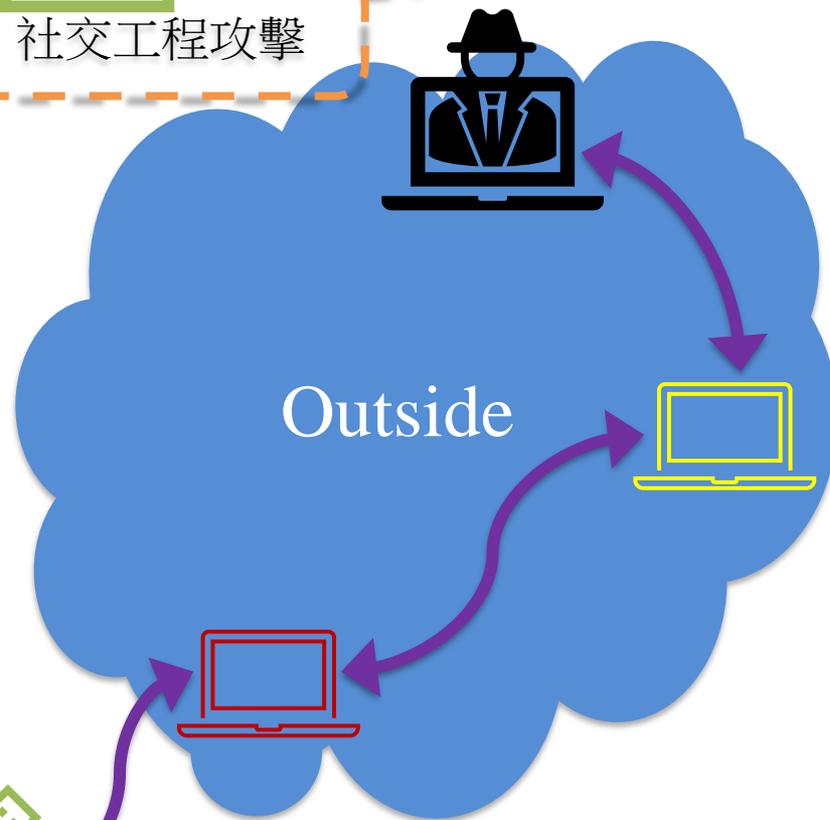
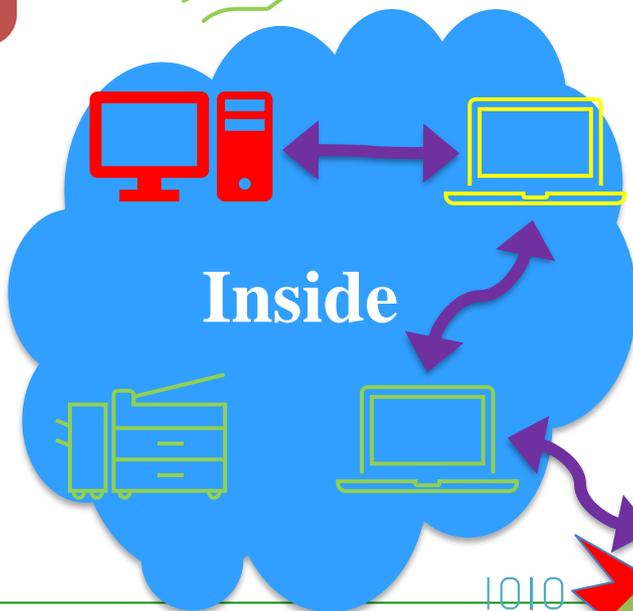
警政署資訊室巡官叢培侃指出，駭客攻擊有一套標準作業程序，一旦進到內網就先攻擊 AD 伺服器，接著側錄所有員工密碼，在更多電腦上安裝木馬、後門程式，以便後續利用。只要一台電腦沒有清理乾淨，駭客還是會繼續自由進出，所以現在的入侵事件很難完全清理乾淨。企業 IT 人員需要提升對惡意程式的偵測監控能力，不能認爲只靠廠商進行一兩次事件調查處理就能解決。

許多的入侵事件，不管是一般駭客入侵，或是所謂進階持續威脅 (APT, Advanced Persistent Threat) 攻擊。都是從使用者好奇開啓一封信的附件或點選惡意連結開始的。Secure Lab 線上提供免費 APT 鑑識服務 XeScan，如果收到可疑郵件，可將附件檔案上傳做分析，可判別是否爲惡意文件及 CVE 漏洞編號等資訊。

一 資訊科技發展

資訊安全 威脅現況

網路區隔之迷失



一 資訊科技發展

資訊安全 威脅現況



內政部警政署 165全民防騙網
National Police Agency, Ministry of the Interior

165反詐騙諮詢專線

首頁 網站導覽

我要報案 我要檢舉 檢舉詐騙廣告

首頁 新聞快訊 涉詐資訊公告 檢舉詐欺報案 識詐宣導 常見詐騙手法 常見QA 檔案下載 相關連結

請選擇類型

拒絕詐騙簡訊 請依據個人使用習慣
若無使用iMessage 可直接關閉

阻絕惱人詐騙簡訊 一勞永逸

113年第一季民眾通報高風險業者排名

高風險業者報案排名

饗賓集團:59件

World Gym:35件

LiTV線上電視:12件

喜樂時代影城:11件

CACO服飾:8件

如接獲假冒業者之客服電話
除撥打165專線舉報外，**建議**
速向業者反映遭詐情事，以維
護您的權益！

! WARNING

如接獲以上業者客服來電，謊稱「訂單錯誤、解除分期付款、誤設會員等級」等，稱稍後會有銀行人員致電協助解除設定，請注意這一定是詐騙！
銀行人員不會主動致電指示操作ATM或網路銀行

ATM及網路銀行
沒有解除錯誤設定
或認證之功能

一 資訊科技發展

資訊安全
威脅現況

常見詐
騙手法

假網拍

假投資

ATM解除
分期付款

假愛情交
友

猜猜我是
誰

假冒機構(
公務員)

假求職

盜(冒)用
網路帳號

一 資訊科技發展

資訊安全 威脅現況



客戶個資外洩達1.4萬人！金管會開罰上海商銀 1000萬元創歷來最高

113/1/1-113/6/30

Cloud Bank by SCSB 數位帳戶優惠專案

2.085%台幣活存利率 (限額NTD20萬，條件加碼至NTD30萬)
定期儲蓄存款一年期固定利率+0.36%

3.85%美金活存利率* (限額USD5,000)

1.3%人民幣活存利率* (限額CNY100,000)

2 / 5

一 資訊科技發展

資訊安全 威脅現況

政府機關、民間企業都遭殃

——近 3 年國內重大個資外洩事件

時間	事件	受害人數
2021/04	臉書用戶個資外洩，受害者所在地區包含美國、英國、印度、台灣等。	台灣 73.4 萬人
2021/08	13 個非營利組織上榜刑事局公布的「高風險賣場」名單，多位捐款人遭詐騙。	未知
2021/09	LINE Pay 誤將 13.3 萬筆交易資訊傳上公開網路。	台灣 7.1 萬人
2022/04	博客來網路書店個資外洩，導致消費者被詐騙，財損總額上億元。	3 個月 2725 人
2022/10	網路論壇 Breach Forums 出現兜售台灣人戶政資料的貼文。	2357 萬人
2023/01	健保署官員涉集體盜賣個資至中國，但健保署表示無證據顯示有資料外洩，全案調查中。	未知
2023/01	國外論壇有駭客陸續公布華航會員個資，包含多位政商人士、藝人。	未知
2023/01	和泰集團旗下和雲行動服務共享汽機車品牌 iRent，被國外白帽駭客發現，資料庫沒有密碼保護，用戶個資曝險長達 9 個月。	40 萬人
2023/02	格上租車 App 雲端儲存空間設定不當，導致所有會員訂單資料可以被查詢列出。	1.6 萬人

資料來源：公開資訊 整理：張如嫻

一 資訊科技發展

資訊安全
威脅現況

反思



他山之石
學習了什麼？

大綱子題

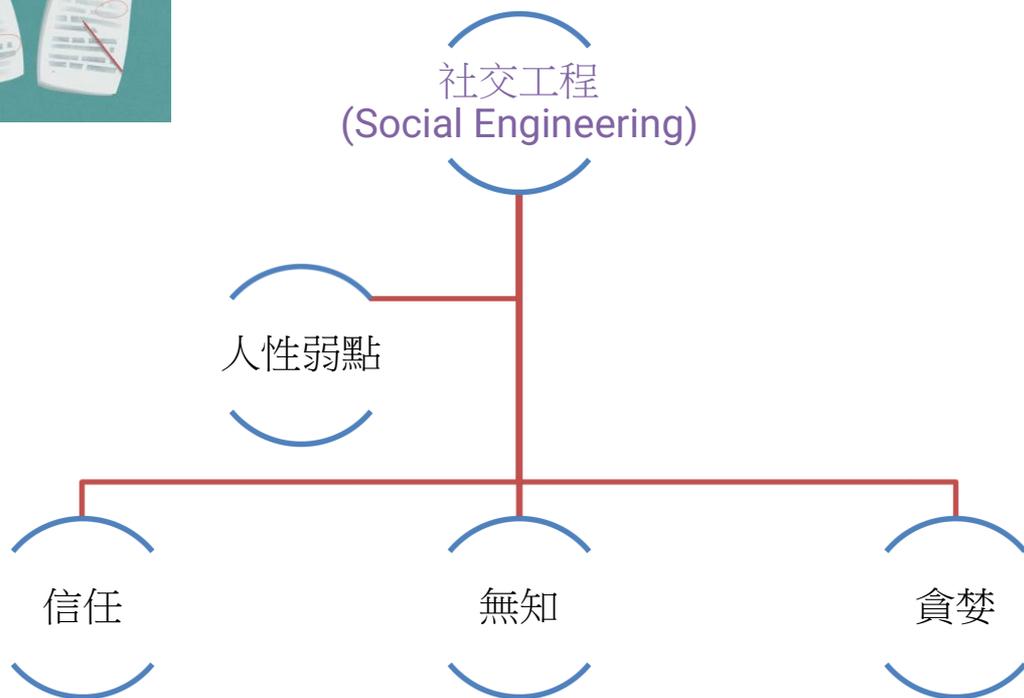
二 常見網路攻擊手法

1 社交工程攻擊

2 勒索病毒攻擊

3 其他類型攻擊

社交工程攻擊



社交工程攻擊

Uber 疑遭駭侵者透過社交工程攻擊，入侵內部系統

2022 / 09 / 19 - 編輯部



紐約時報進一步指出，該名駭侵者為了取得兩步驟登入驗證密碼，更透過大量發送垃圾通知的手法讓該名遭駭員工不斷收到推送通知，接著再於 WhatsApp 上假冒 Uber IT 人員和該員工對話，進而取得兩步驟驗證碼的存取權。

資安專家也指出，該名駭侵者在取得兩步驟驗證碼後，隨即進入 Uber 內部網路，同時很快就在其內網的某個檔案中找到許多具有極高權限的登入資訊；該名駭侵者立即使用這些登入資訊存取 Uber 內部各項系統，包括產品系統、企業 EDR 控制台、Uber 內部的 Slack 管理介面等等。

駭侵者甚至還公開 Uber 各個內部系統的螢幕擷圖，甚至包括內部財務系統的報告畫面，以及 Uber 透過 HackerOne 舉辦漏洞發現懸賞的多份報告在內。資安專家擔憂駭侵者可能會將這些漏洞資訊對外販售。

二 常見網路攻擊手法

社交工程攻擊

俗話說得好，資安最大的漏洞就是「人」。社交工程攻擊用的不是高深的電腦技術，而是用詐騙的方式要到關鍵人物的驗證資訊，進而取得登入權限。

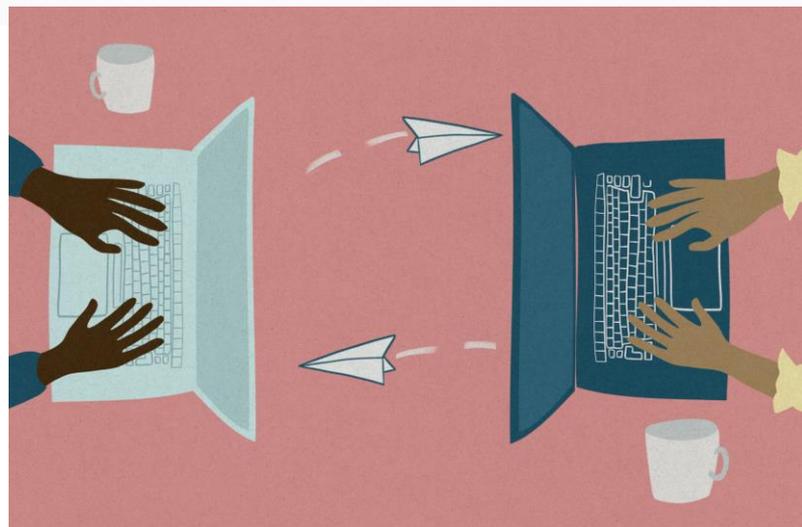


二 常見網路攻擊手法

社交工程攻擊

上市櫃公司陸續遭駭 數位部為何示警社交工程欺騙？

近期陸續有上市櫃公司遭駭客攻擊，數位部資安署長謝翠娟指出，企業發生類似事件大多是有人員受到社交工程欺騙，「並不是有防護漏洞，而是被社交工程攻擊，例如同仁不小心收了mail，或者是點了某些連結，合法地把壞人引進來。」



社交工程攻擊



Hi 各位同仁

附件是本次課後之評量參考文件
請各位下載閱讀
謝謝各位

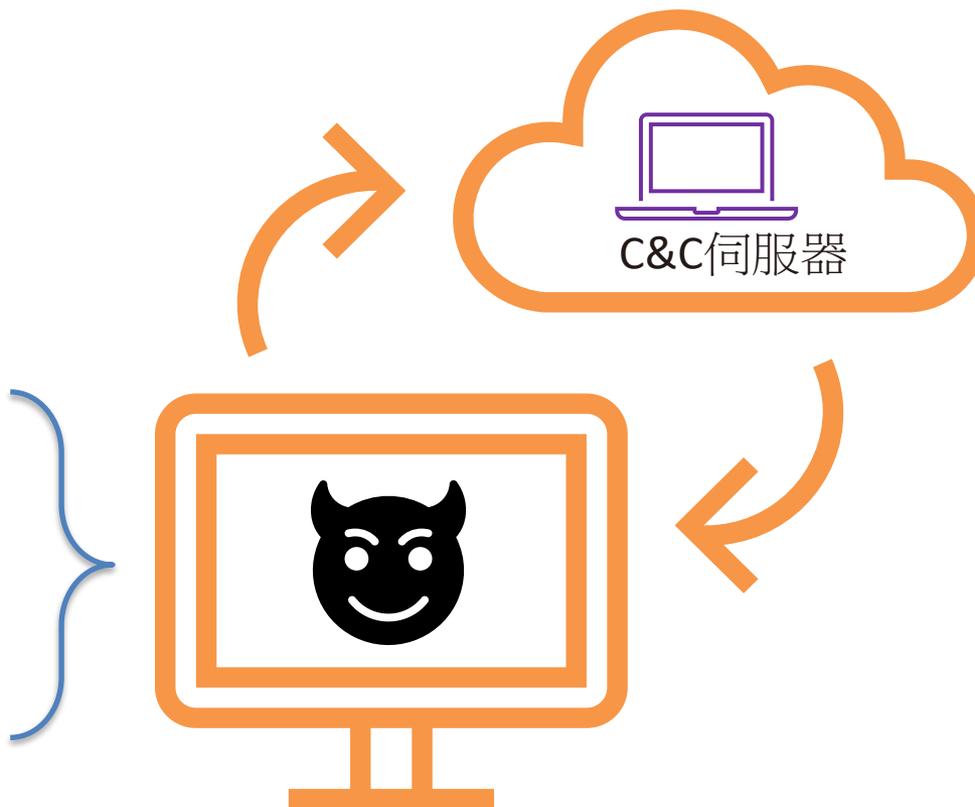
Mark 敬



二 常見網路攻擊手法

勒索病毒攻擊

- ✓ 網站瀏覽
- ✓ 電子郵件感染
- ✓ 非法軟體感染
- ✓ 被已遭受勒索軟體攻擊的電腦或裝置感染



二 常見網路攻擊手法

勒索病毒攻擊



勒索軟體 (Ransomware)

破壞受駭者對
設備存取權

破壞受駭者對
資料存取權

非加密型

加密型

二 常見網路攻擊手法

勒索病毒攻擊

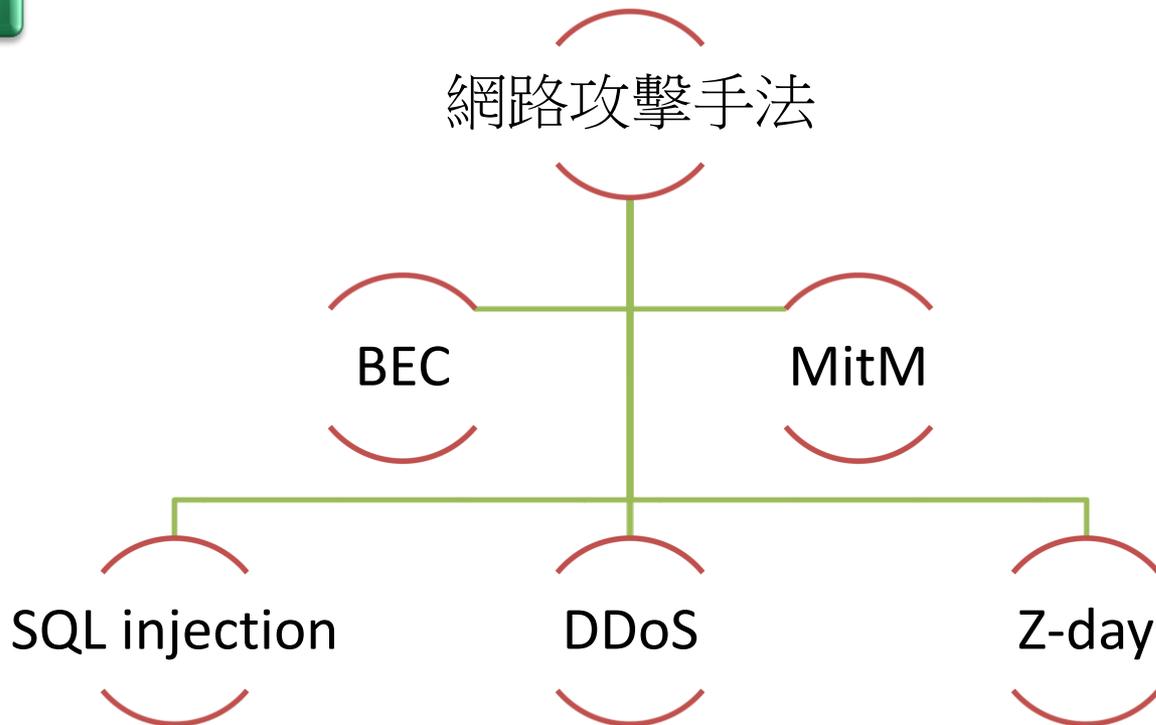
RaaS

- ✓ 勒索留言通常是.txt檔或是.html檔
- ✓ 發現文件被加密無法開啟
- ✓ 怪異副檔名
.crypt、.VVV、.CCC、.ZZZ、.ABC、.XXX、.TTT
- ✓ 瀏覽器遭鎖定
- ✓ 瀏覽器工具列發現奇怪的捷徑
- ✓ 畫面顯示勒索訊息。

Ransomware

二 常見網路攻擊手法

其他類型攻擊



大綱子題

三 面對網路攻擊威脅應有之認知與作為

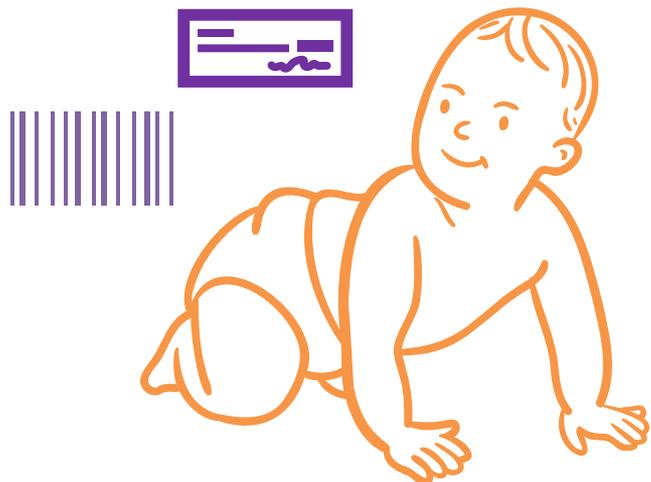
1 個人應有之認知

2 組織應有之作為

三

面對網路攻擊威脅應有之認知與作為

個人應有
之認知



網路好奇寶寶

個人應有
之認知

社交工程攻擊退散

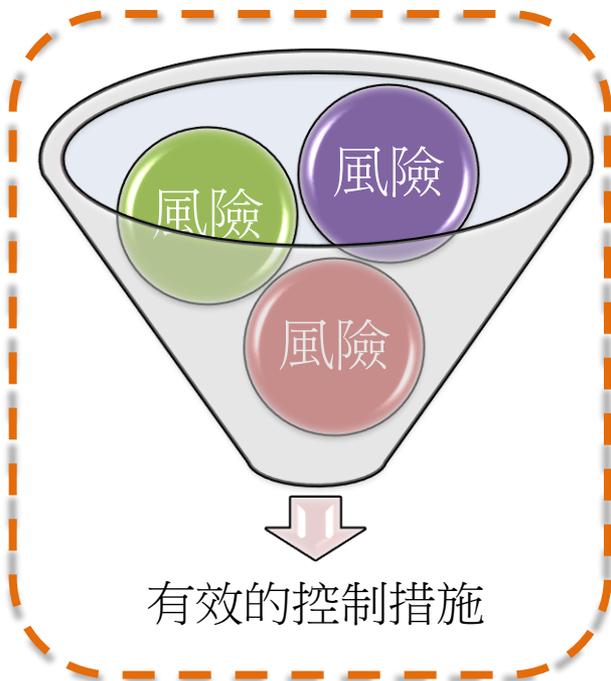
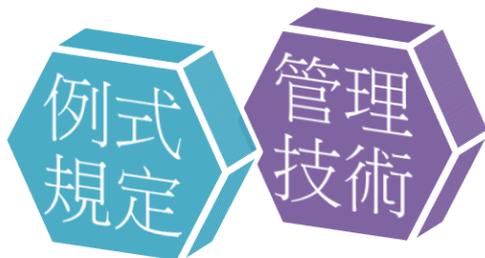
不隨意開啟來路不明之電子郵件
不隨意點擊來路不明之連結或附件
安裝防毒軟體並更新病毒碼
定期執行病毒掃描
隨時注意電腦或網路使用狀態



三

面對網路攻擊威脅應有之認知與作為

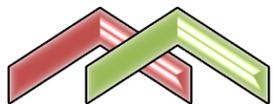
組織應有
之作為



三

面對網路攻擊威脅應有之認知與作為

組織應有之作為



面對網路攻擊威脅應有之認知與作為

組織應有
之作為

What ?

How ?

Risk

防止

思考
邏輯

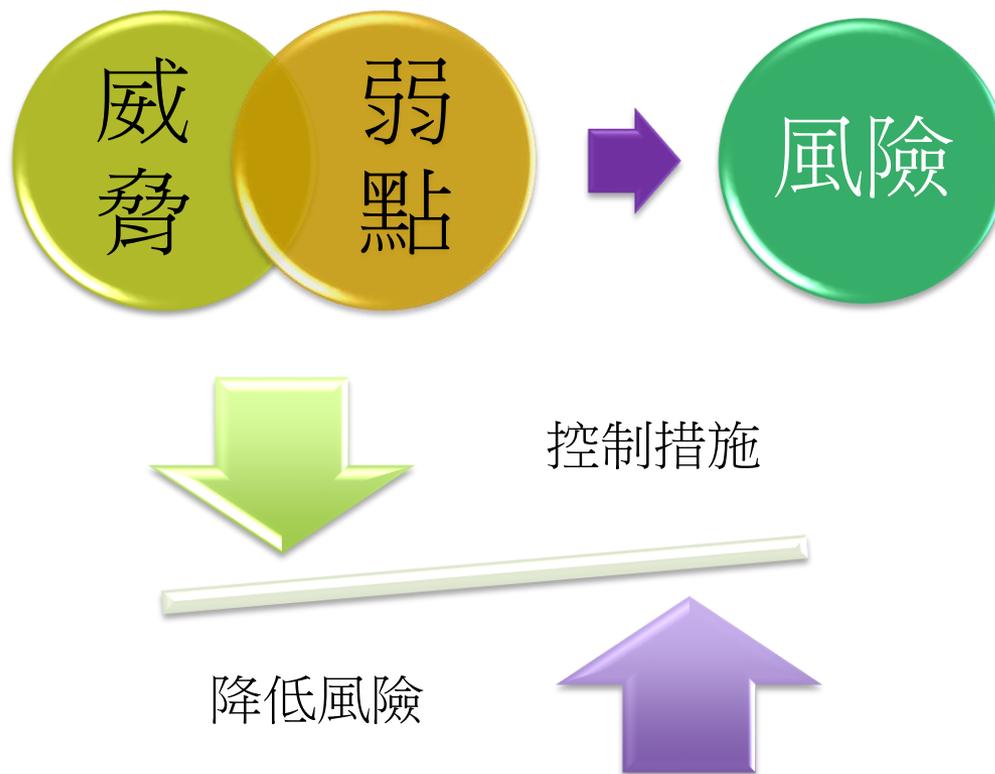
證明

資安
技術

查明

面對網路攻擊威脅應有之認知與作為

組織應有
之作為



面對網路攻擊威脅應有之認知與作為

組織應有
之作為

What ?

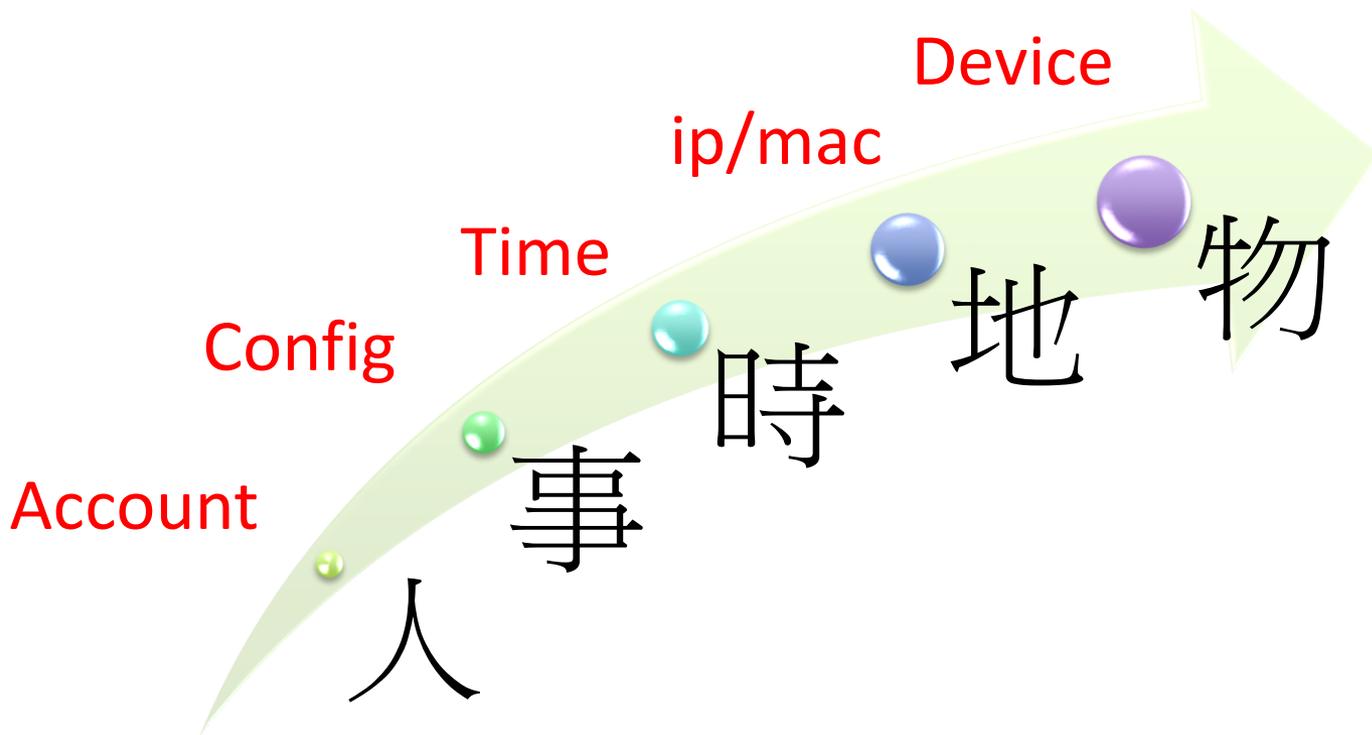
How ?

資安
技術

Log

查明

組織應有
之作為



組織應有
之作為

What ?

How ?

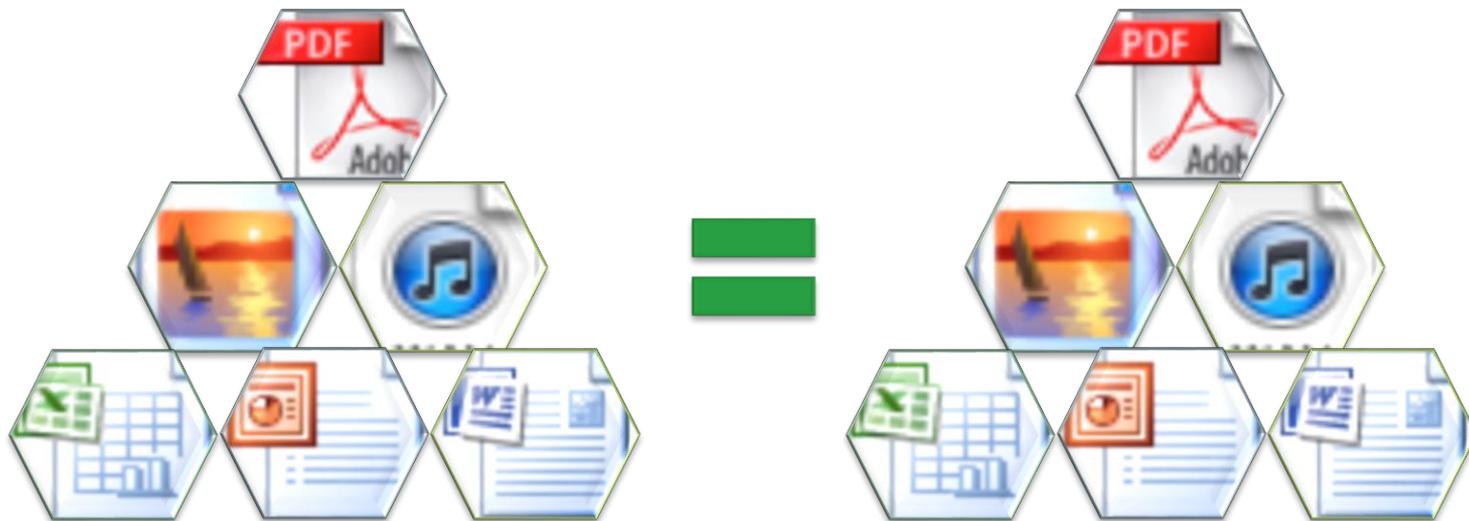
Identity

證明

資安
技術

組織應有
之作為

Case Study



組織應有之作為

7 大構面	29項控制措施
存取控制	帳號管理;最小權限;遠端存取
事件日誌與可歸責性	記錄事件;日誌紀錄內容 ;日誌儲存容量;日誌處理失效之回應 ;時戳及校時 日誌資訊之保護
營運持續計畫	系統備份;系統備援
識別與鑑別	內部使用者之識別與鑑別;身分驗證管理;鑑別資訊回饋;加密模組鑑別 ;非內部使用者之識別與鑑別
系統與服務獲得	系統發展生命週期需求階段;系統發展生命週期設計階段;系統發展生命週期開發階段 ;系統發展生命週期測試階段 ;系統發展生命週期部署與維運階段;系統發展生命週期委外階段 ;獲得程序;系統文件
系統與通訊保護	傳輸之機密性與完整性;資料儲存之安全
系統與資訊完整性	漏洞修復;資通系統監控;軟體及資訊完整性

面對網路攻擊威脅應有之認知與作為

組織應有之作為

風險管理機制

風險評鑑



風險處理



控制措施

資通
安全
維護
計畫

- 資通安全管理政策
- 資通安全組織架構管理作業程序
- 資訊資產盤點管理作業程序
- 風險管理作業程序
- 資通管理作業程序
- 資通安全事件通報及應變作業程序
- 資通安全教育訓練管理作業程序
- 內部稽核管理作業程序
- 資通安全管理審查作業程序
-

面對網路攻擊威脅應有之認知與作為

組織應有之作為

制度框架

事前

資通安全政策

資通安全管理架構

個人資料管理架構

資訊面

個人資料盤點

個人資料

電子文件管理

電子文件

基礎架構

事中

伺服器/電腦

網路設備

資料庫

機房

應用系統

商用系統

自行開發

事件處理

事後

證據保全

事件通報

緊急應變

程序規範

管理框架



四 討論