114年多元意識及跨域產業資安課程

資安教育與防範意識提升

07.23(三)

13:30~15:30

純線上授課

- 資安意識強化
- 風險控管
- 企業資安管理

魏國瑞 Ray
kjwei@aaasec.com.tw

魏國瑞 Ray

- **組織角色**：三甲科技-總經理 / 逢甲大學 - 助理教授(兼)
- **專長領域**：密碼學、電子商務安全、資訊安全管理、攻防演練、資安診斷、...
- **學/協會**：中華民國資訊安全學會、台灣E化資安分析管理協會、台灣國際認證資安專家協會、台灣資安產業發展協會、台灣資訊安全協會、...(依筆畫排序)
- **專業證照/課程**：
  - ISC2 Certified Information Systems Security Professional(CISSP)
  - CompTIA Security+ Certified Professional
  - EC-Council Ethical Hacker(CEH)
  - ISO/IEC 27001:2022 ISMS Lead Auditor Course/Auditor
  - ISO/IEC 27701:2019 PIMS Lead Auditor Course/Auditor
  - ISO/IEC 42001:2023 AIMS Lead Auditor Course/Auditor
  - IEC 62443-2-1 CSMS Lead Auditor Course/Auditor
  - Certificate of Cloud Security Knowledge(CCSK)
  - iPAS資訊安全工程師-初級、中級能力鑑定
  - CMMS CCP Course、PMI Project Management Professional(PMP)、...

公司簡介

三甲科技是由一群擁有資訊安全背景的工程師所共同創立，內部工程師皆具備資安相關專業證照。服務團隊經驗相當豐富，主要服務對象擴及學校單位、政府機關、科技產業、房產集團、金融企業和第三方支付產業等機構。

「三甲」取名於「AAA Security」，代表著資訊安全當中的三大面向，認證(Authentication)、授權(Authorization)、紀錄(Accounting)。另外一方面也意味著我們期望：

透過 A級專業 → 提供 A級服務 → 達到 A級安全

資訊安全管理系統驗證 ISO/IEC 27001

TAF測試實驗室認證 ISO/IEC 17025

通過數位發展部數位產業署
資安能量登錄
資通安全自主產品認定
SecPaas 資安整合服務平臺 合作夥伴

核心服務

- ✓ISMS導入/驗證
- ✓資安管理制度導入
- ✓教育訓練服務
- ✓源碼安全檢測服務
- ✓精準資安規劃服務
- ✓其他資安服務
  - 資安顧問服務
  - 紅隊演練服務
  - DDoS演練服務
  - 攻防演練服務

找出企業漏洞風險

輔導企業進行改善

強化資安防護水準

大綱

- 資安威脅無所不在，安全意識人人須有
- 企業資安管理，從政策到推動

資安趨勢

- 參考114年上半年全球資安威脅情資

PII 與憑證外洩
導致保護機制失效

雲端應用服務衍生多元威脅

資通系統弱點
頻遭揭露利用

社交工程泛濫
致APT鎖定與勒索軟體風險增加

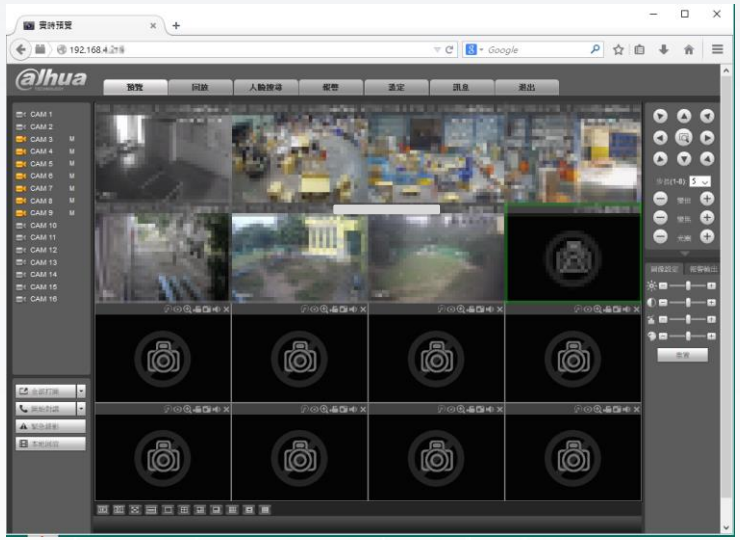
資安(訊)供應鏈遭駭
破壞邊界信任與防護

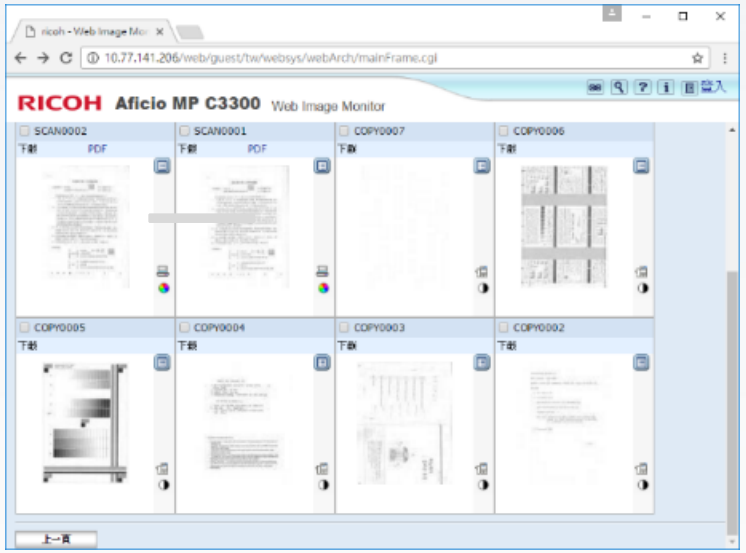
駭客利用AI技術
開發新型攻擊與惡意詐欺

資料來源：數位發展部資通安全署

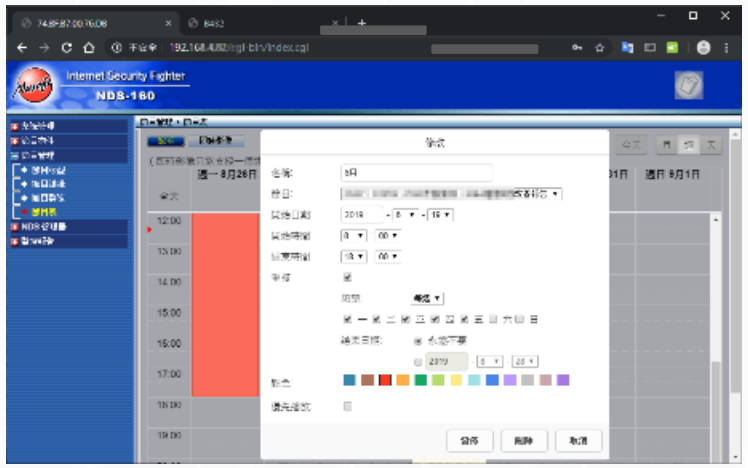
實務上案例

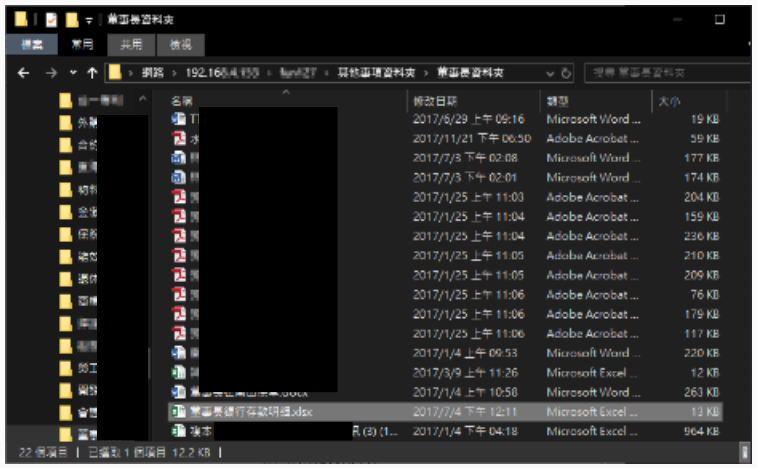
一種可以被看光光的感覺





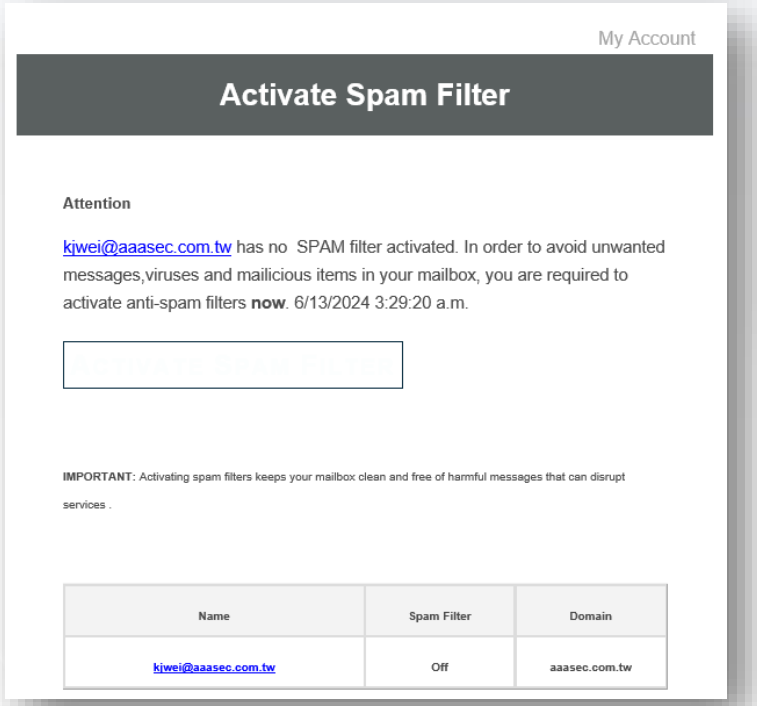
Name	Last modified
Parent Directory	
0/	11-Apr-2019 07:56
1/	11-Apr-2019 22:17
2/	12-Apr-2019 12:42
3/	13-Apr-2019 03:05
4/	13-Apr-2019 17:33
5/	14-Apr-2019 07:54
6/	14-Apr-2019 22:19
7/	15-Apr-2019 12:43
8/	16-Apr-2019 03:04
9/	16-Apr-2019 17:29
A/	21-Apr-2019 12:43
B/	22-Apr-2019 03:06
C/	22-Apr-2019 17:32

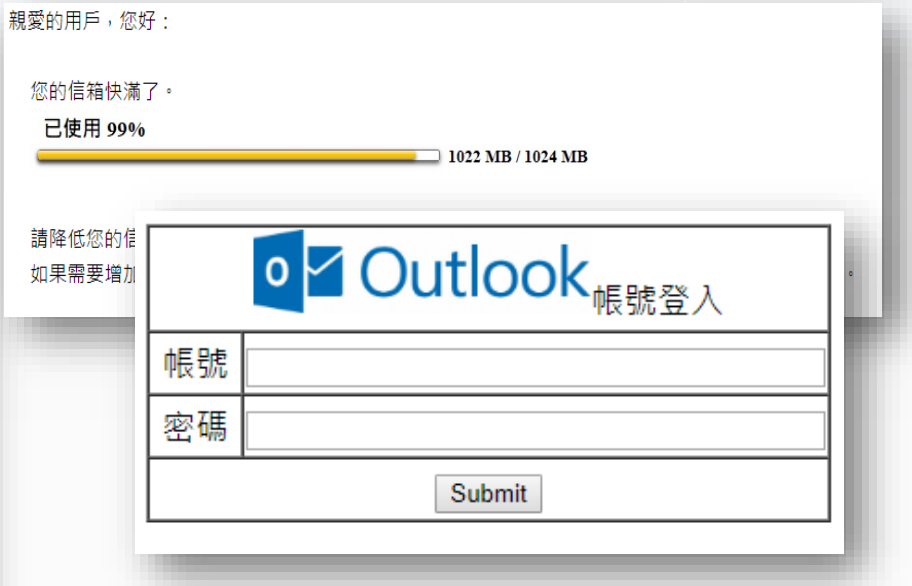




你說企業不會中獎嗎?

- 有沒有聽過社交工程?!
  - –簡單來說就是，利用人性弱點，應用簡單的溝通和 欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破資通安全防護，遂行其非法的存取、破壞行為。



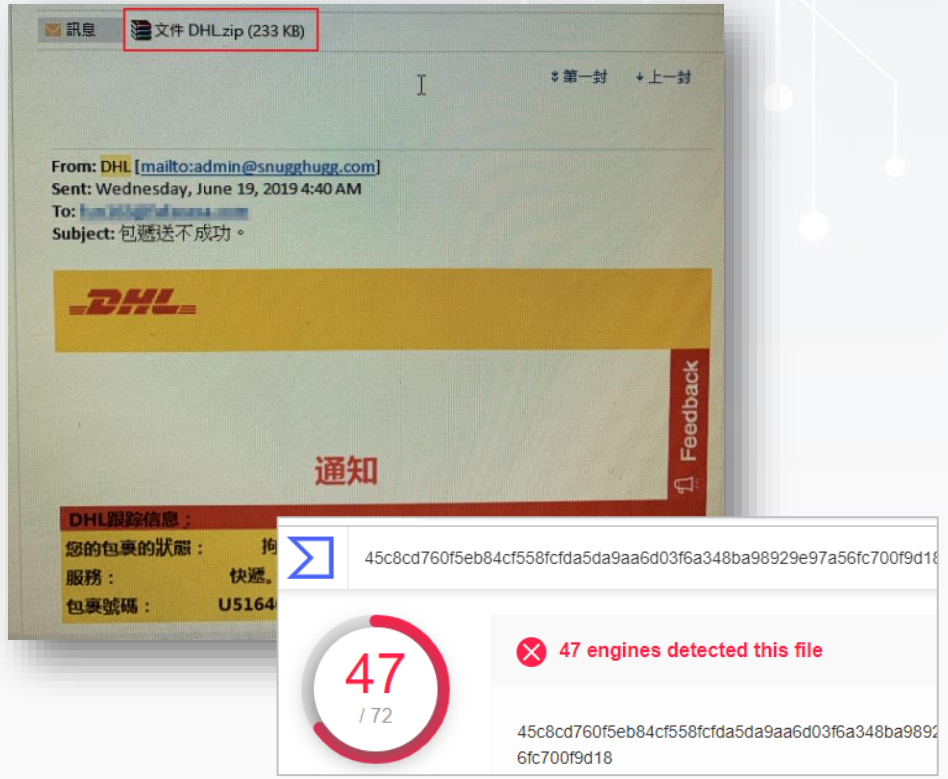


實際案例1-勒索軟體

- 檔案陸續加密， 但不知為什麼?
- 發現加密後，網路隔離
  (第一步絕對是止血)
- 諮詢：可疑下載?可疑信件?可以執行?
  (一般感染會有兩個步驟：取得＆執行)
- 同仁：無特殊程式安裝，也沒什麼可疑信件。

實際案例1-勒索軟體(續)

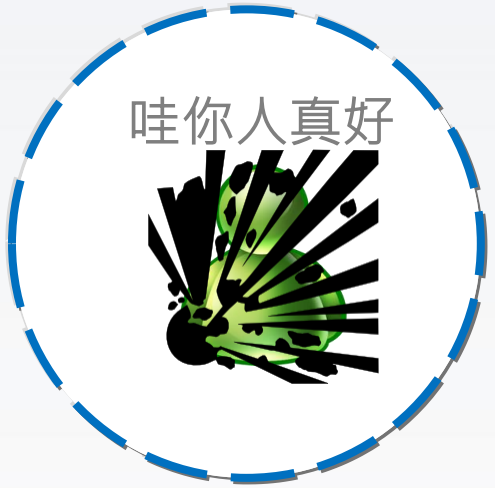
- 附件檔案DHL.zip
- 諮詢：是否開啟過物件？
- 找事件軌跡及可能路徑
  - 重現確認
  - 多軟體檢視執行序…
  - 加密時間、檔案還原
  - 開啟紀錄
- 確認事件路徑
- 經典型，將惡意程式封裝在壓縮檔，逃避防毒軟體偵測
- 啟示：小心可疑信件，預覽也是一種開啟



為什麼要透過社交?

禮物送你

經過適當的偽裝



防火牆、入侵防禦系統

(心理層面)
想要什麼？
需要什麼？

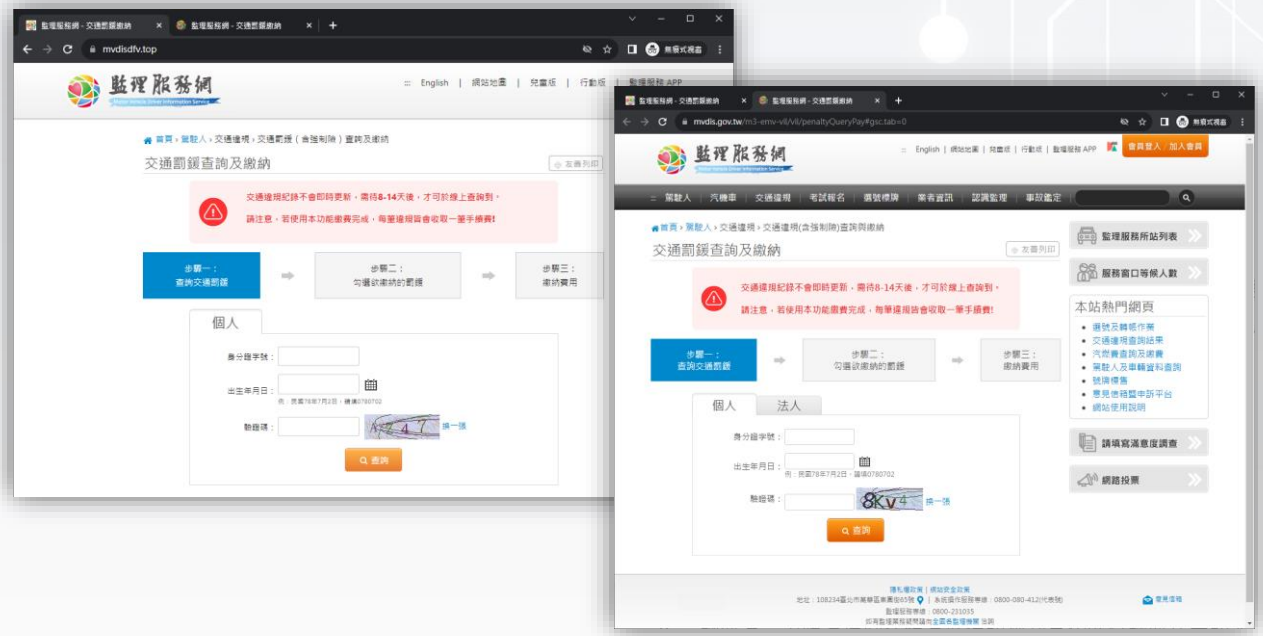
+

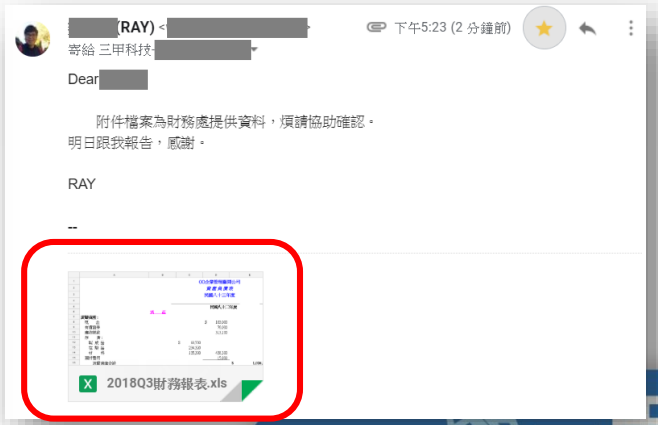
(攻擊層面)
想要做什麼？
攻擊手法？

串聯手法包裝

信中的千百種可能?!

- 依攻擊者喜好！
  - 夾帶惡意連結
    - 釣魚網站
    - 偷你資料
    - 偷你權限
    - 偷你錢
    - 偷你…
  - 夾帶惡意檔案
    - 勒索軟體
    - 惡意程式
    - 入侵企業
    - 埋下後門程式
    - …





實際案例2-勒索軟體

遇見勒索

```
total 36940
drwx------  2 mysql mysql     4096 Dec 26  2018 eCard
drwx------  2 mysql mysql     4096 Oct 23 23:27 eCardSql
-rw-rw----. 1 mysql mysql 27262976 Nov  4 18:23 ibdata1
-rw-rw----. 1 mysql mysql  5242880 Nov  4 18:23 ib_logfile0
-rw-rw----. 1 mysql mysql  5242880 No
drwx------. 2 mysql mysql     4096 No
-rw-rw----  1 mysql mysql    42338 Nov 26  2018 MySQL.log
srwxrwxrwx  1 mysql mysql        0 Nov  4 14:05 mysql.sock
-rw-r--r--  1 root  root         6 Nov  4 11:59 mysql_upgra  info
drwx------  2 mysql mysql     4096 Nov  4 11:59 performance_schema
drwx------  2 mysql mysql     4096 Oct 23 23:27 PLEASE_READ_ME_XMG
drwx------  2 mysql mysql     4096 Nov  4 11:21 test
```

PLEASE_READ_ME_XMG

```
6.0) Gecko/20100101 Firefox/66.0"
193.169.252.34 - - [redacted] "POST /phpMyAdmin/import.php HTTP/1.1" 200 3011 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko
/20100101 Firefox/[redacted]"
193.169.252.34 - - [redacted] "POST /phpMyAdmin/export.php?db=[redacted] TTP/1.1" 200 814 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0
) Gecko/20100101 F[redacted]"
193.169.252.34 - - [redacted] "POST /phpMyAdmin/import.php HTTP/1.1" 200 1994 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko
/20100101 Firefox/[redacted]"
193.169.252.34 - - [redacted] "POST /phpMyAdmin/import.php HTTP/1.1" 200 2886 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko
/20100101 Firefox/[redacted]"
193.169.252.34 - - [redacted] "POST /phpMyAdmin/import.php HTTP/1.1" 200 3018 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko
/20100101 Firefox/[redacted]"
193.169.252.34 - - [redacted] "POST /phpMyAdmin/export.php?db=[redacted] TTP/1.1" 200 826 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:
79.0) Gecko/20100[redacted]"
193.169.252.34 - - [redacted] "POST /phpMyAdmin/import.php HTTP/1.1" 200 1998 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko
/20100101 Firefox/[redacted]"
193.169.252.34 - - [redacted] "POST /phpMyAdmin/import.php HTTP/1.1" 200 2891 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko
/20100101 Firefox/[redacted]"
193.169.252.34 - - [redacted] "POST /phpMyAdmin/import.php HTTP/1.1" 200 3016 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko
/20100101 Firefox/[redacted]"
193.169.252.34 - - [redacted] "POST /phpMyAdmin/export.php?db=[redacted] TTP/1.1" 200 7392180 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv
:79.0) Gecko/20100[redacted]"
193.169.252.34 - - [redacted] "POST /phpMyAdmin/import.php HTTP/1.1" 200 1996 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko
/20100101 Firefox/[redacted]"
193.169.252.34 - - [redacted]
/20100101 Firefox/[redacted]"
193.169.252.34 - - [redacted]
/20100101 Firefox/[redacted]"
```

Post /phpMyAdmin/export.php?=db=XXXXX

密碼破解

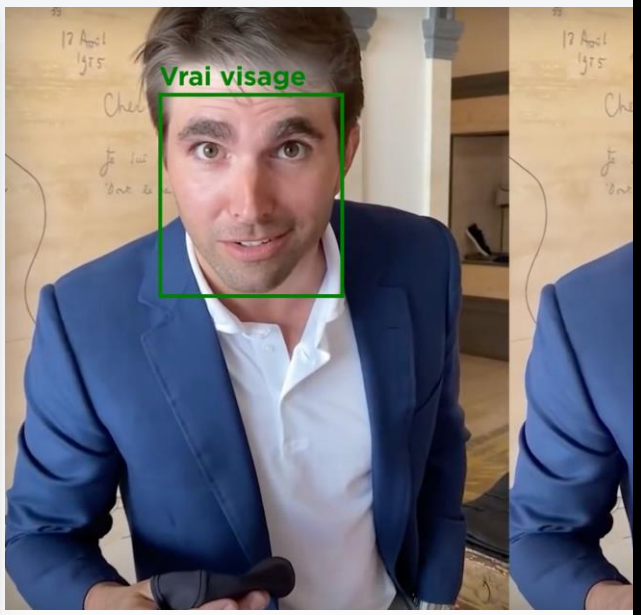
→傳出資料

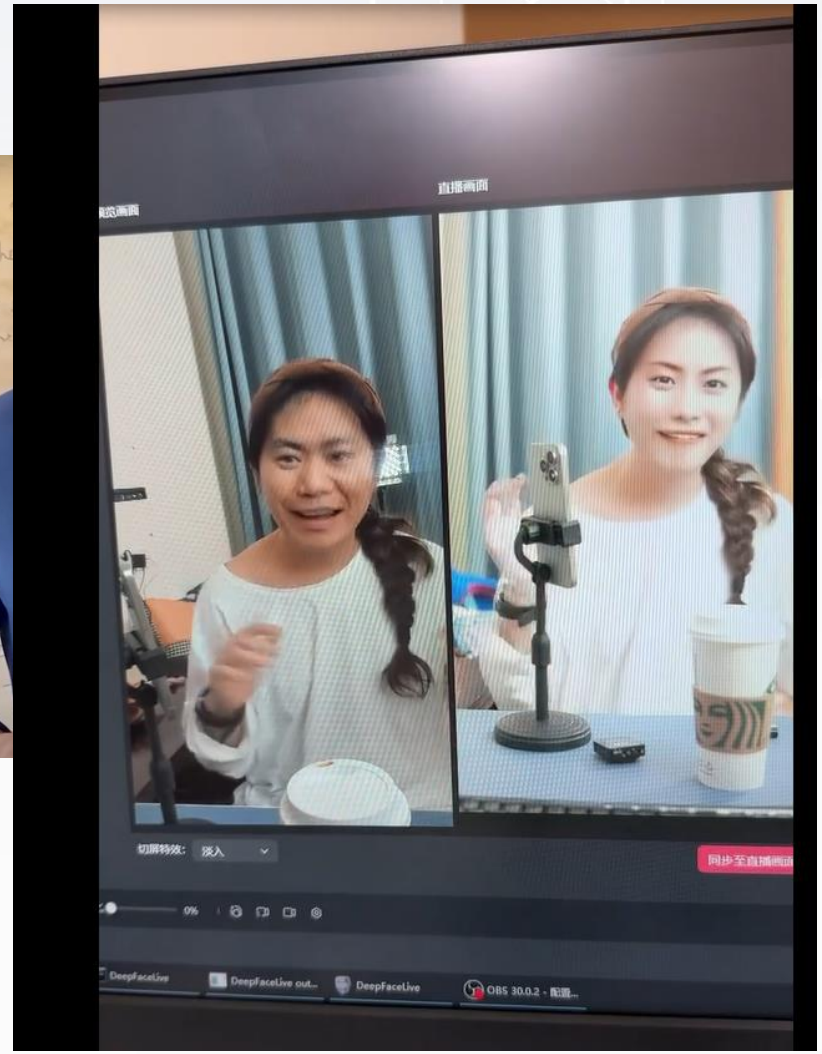
→加密/刪除

→勒索贖金

詐騙手法結合現代技術

- DeepVoice、DeepFake

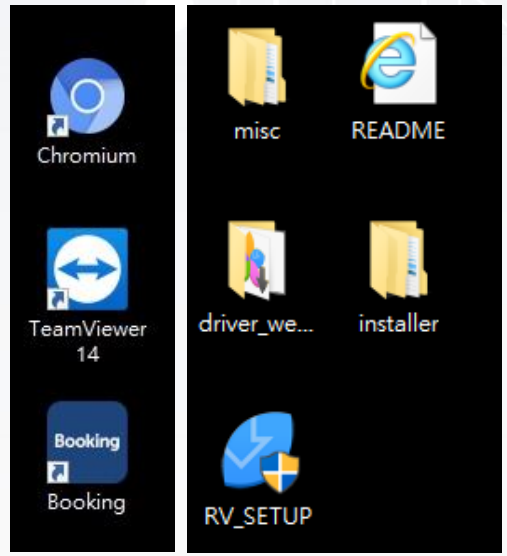


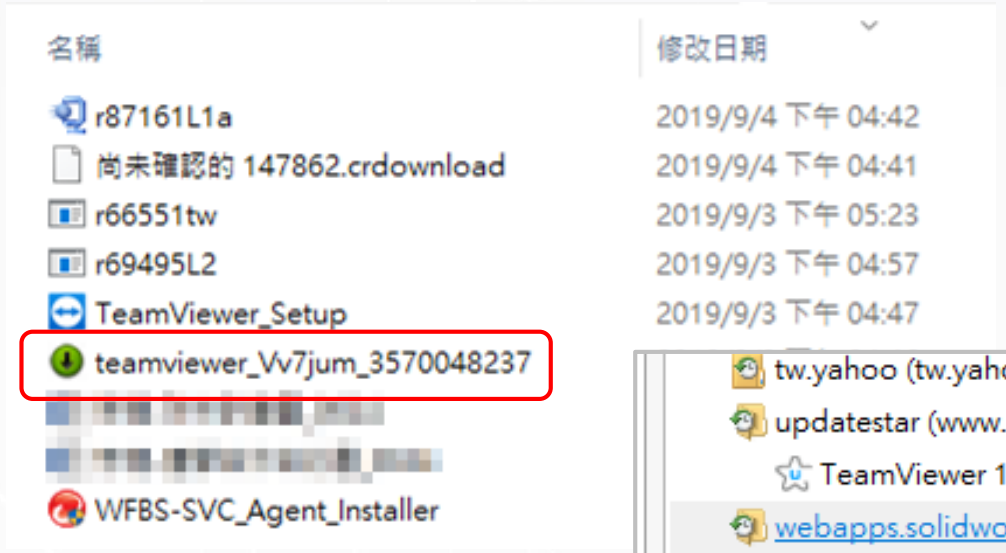


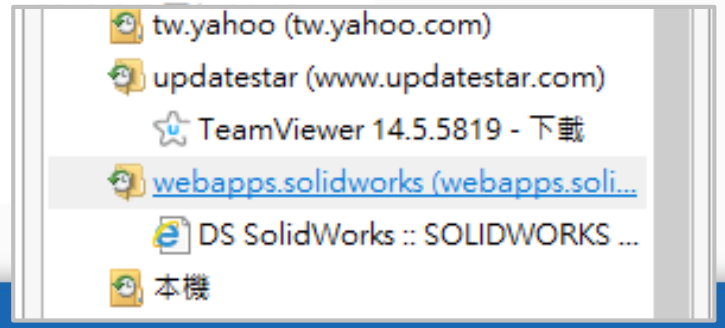
https://news.tvbs.com.tw/focus/2064534

不會有人來騙我們小公司吧?!

- 發現時間
- 檢視近期安裝程式(TeamViewer)
- 確認安裝軟體的取得(官網)
- 檢視下載紀錄與瀏覽紀錄







你說企業不會中獎嗎?

- 有沒有可能企業還存在很多弱密碼、預設密碼?!

1	123456
2	123456789
3	Picture1(新進榜)
4	password
5	12345678
6	111111
7	123123
8	12345
9	1234567890
10	Senha(葡語,密码)

11	1234567
12	qwerty
13	abc123
14	Million2
15	000000
16	1234
17	iloveyou
18	aaron431
19	password1
20	qqww1122

不進榜、但也...

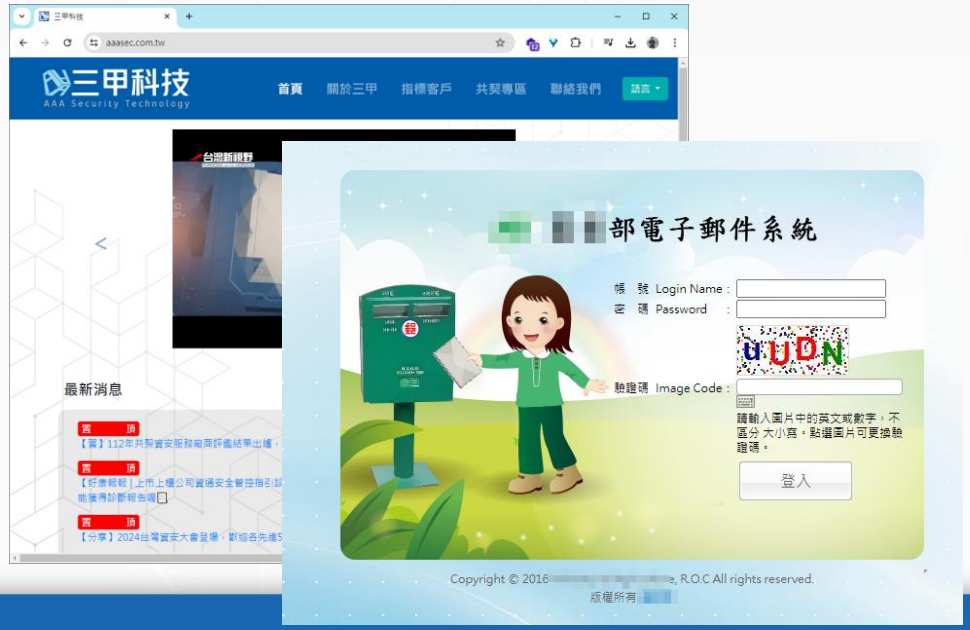
- P@55W0RD
- zaq12wsx
- ZAQ!2wsx
- 統編/電話
- 分機
- Ji32k7au4a83

Google

- admin/admin
- admin/password
- root/root
- monitor/!monitor (HP)
- root/calvin (Dell iDARC)
- admin/dh123456 (監視器)

那...

- 對外服務系統?
  - 官方網站
  - 供應鏈系統
  - 郵件伺服器
  - …



- 容易被遺忘卻有能力的資產?
  - 網路攝影機
  - 網路印表機
  - 掃地機器人
  - 機聯網設備
  - 碳排測試設備
  - …

都安全嗎?

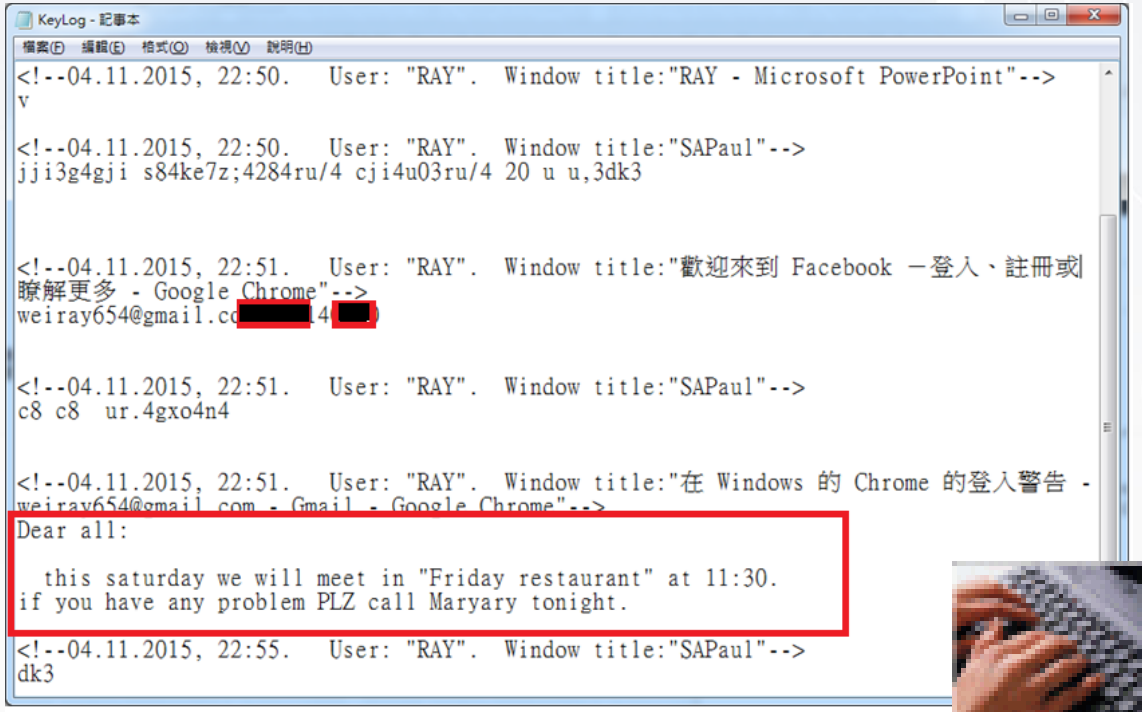
沒事都沒事，一有事就...

- 沒認知到漏洞被惡意使用?!

WinRAR

- WinRAR 嚴重漏洞，開啟壓縮檔可讓駭侵者遠端執行任意程式碼
- CVE 編號：CVE-2023-40477
- 影響產品：WinRAR 6.23 先前版本。
- 解決方案：立即更新 WinRAR 至 6.23 與後續版本。

在外面辦公的安全?


KeyLog - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
<!--04.11.2015, 22:50. User: "RAY". Window title:"RAY - Microsoft PowerPoint"-->
v
<!--04.11.2015, 22:50. User: "RAY". Window title:"SAPaul"-->
jji3g4gji s84ke7z;4284ru/4 cji4u03ru/4 20 u u,3dk3
<!--04.11.2015, 22:51. User: "RAY". Window title:"歡迎來到 Facebook 一登入、註冊或瞭解更多 - Google Chrome"-->
weiray654@gmail.co
<!--04.11.2015, 22:51. User: "RAY". Window title:"SAPaul"-->
c8 c8 ur.4gxo4n4
<!--04.11.2015, 22:51. User: "RAY". Window title:"在 Windows 的 Chrome 的登入警告 - weiray654@gmail.com - Gmail - Google Chrome"-->
Dear all:
this saturday we will meet in "Friday restaurant" at 11:30.
if you have any problem PLZ call Maryary tonight.
<!--04.11.2015, 22:55. User: "RAY". Window title:"SAPaul"-->
dk3

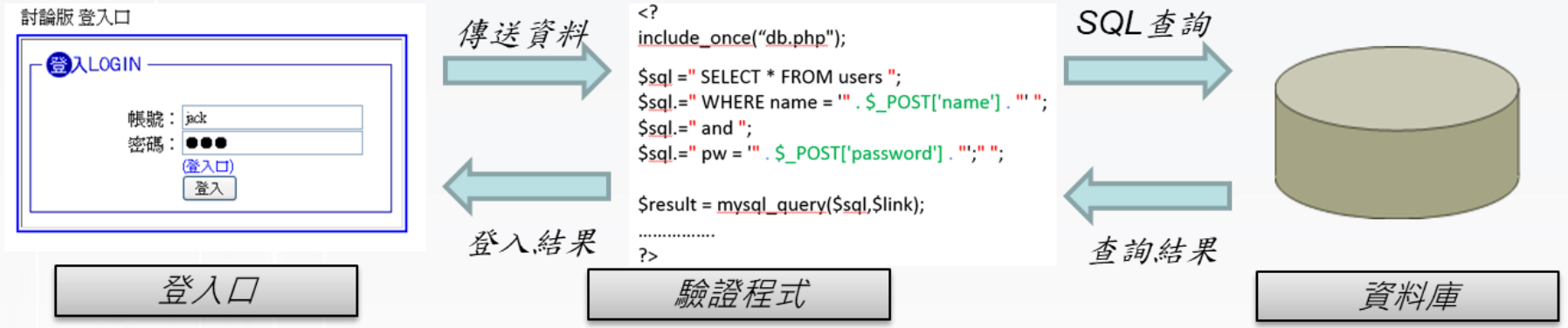

沒設密碼


竊聽


資源回收筒

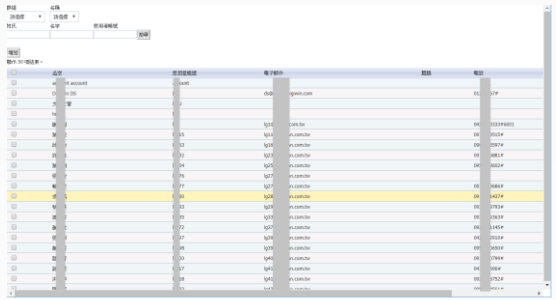
常見的技術弱點-SQL Injection

- SQL 是資料庫的查詢語言
- SQL Injection 常出現於語法以 拼接 做查詢



SELECT * FROM users
WHERE name = ' Ray '
and
pw = ' 666'

SELECT * FROM users
WHERE name = ' Ray '
and
pw = ' '
or
'A' = 'A '



▲ 透過SQL injection通訊資料範例

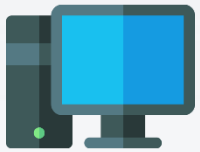
常見的技術弱點-XSS

- Cross-Site Scripting (XSS)
- 網頁跨站攻擊，利用程式碼將惡意網站嵌入至正常網頁中，欺騙使用者進行存取，以擷取使用者私密內容。
- 反射型、儲存型

演練案例

1. 掃描取得資訊

9. 發現伺服器
主機弱點



10. 成功使用
Microsoft弱點
控制伺服器

額外目標
取得主機控制權

8. 使用其內員工信箱，
設計偽裝的系統警告信

額外目標
使用員工信箱資
訊進行社交工程

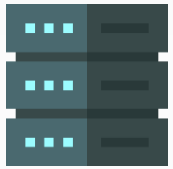
2. 不需密碼
存取之資訊

6. 發現網站

7. **SQL injection**
取得資料庫中資訊

主要目標
取得機敏資料

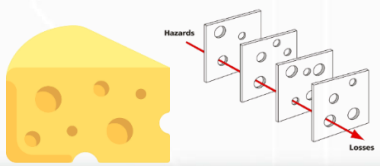
3. **發現敏感**
網段相關資訊



4. 於網段
發現網域控制站

5. 於共享資料夾發現**產品規格書、工作進度報告、敏感往來信件、產品報價單與客戶資訊**

主要目標
取得機敏資料



企業資安管理

三甲科技
AAA Security Technology

大部分落地的資安

* 控管風險

- 確保資訊及資通系統資產免於發生潛在〝不可承受的風險〞，管控組織在可承受風險範圍內。

Confidentiality (機密性)

- 確保只有經授權的人，才能允許存取資訊
- 驚！中華郵政商城傳個資外洩，民眾被詐騙集團盯上

Integrity(完整性)

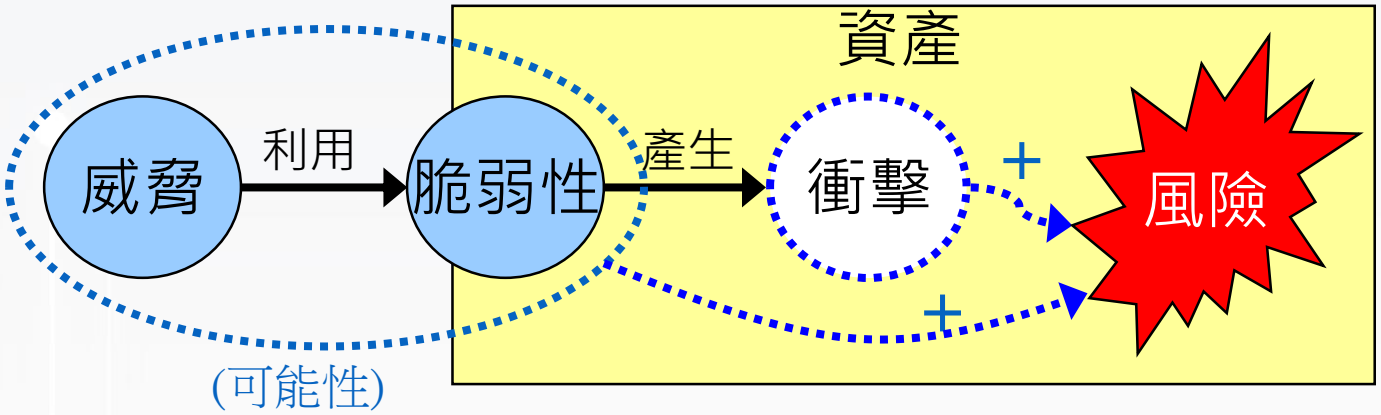
- 確保資訊內容與資訊處理方法正確且完整
- 單車又出包，官網市徽遭竄改為『台北好好拆』

Availability(可用性)

- 確保經授權的使用者需要時，能存取資訊與使用相關資產
- 前天當、昨天當，新北市戶政系統頻出包

風險

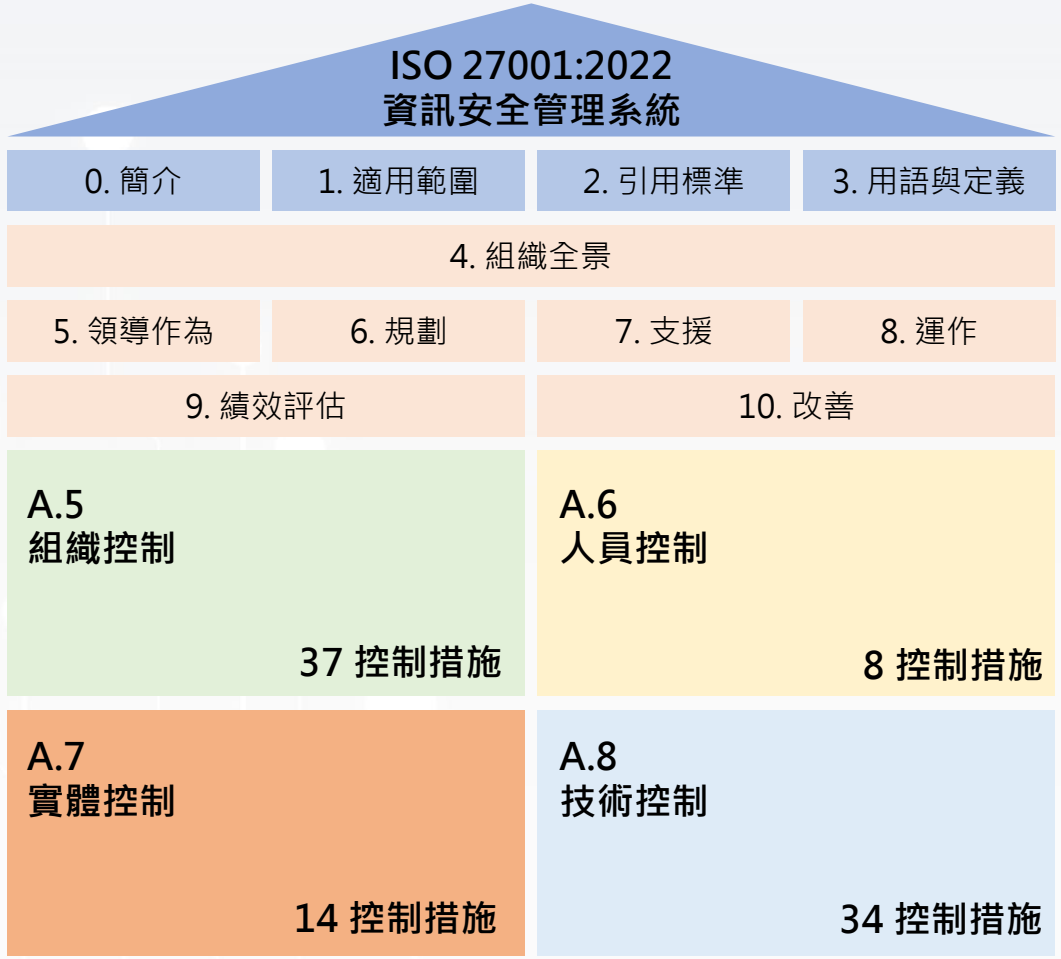
- 「風險」是指「威脅」利用其相對應「脆弱性」造成企業資訊資產受到「衝擊」的「可能性」



- 風險透過「衝擊」與其「可能性」兩個因素的結合來定義其影響程度或損害程度
- 風險管理的目標：~~最低~~**合理**的防護成本投入下獲得最~~優化~~**適當**的安全性

(最優化非最強固，而是最合適)

最熟悉的工具　ISO/IEC 27001



4 Domians ; 93 Controls

營運安全

A5.30 營運持續之資通訊準備

資料安全

A8.10 資訊刪除
A8.11 資料遮罩
A8.12 防範資料外洩

雲安全

A5.23　雲服務之資訊安全

資訊安全

A5.7　威脅情報
A7.4　實體安全監控
A8.9　組態管理
A8.16 活動監控
A8.23 網頁安全防護
A8.28 程式開發安全

ISMS 資訊安全政策

【文件制定及實施】

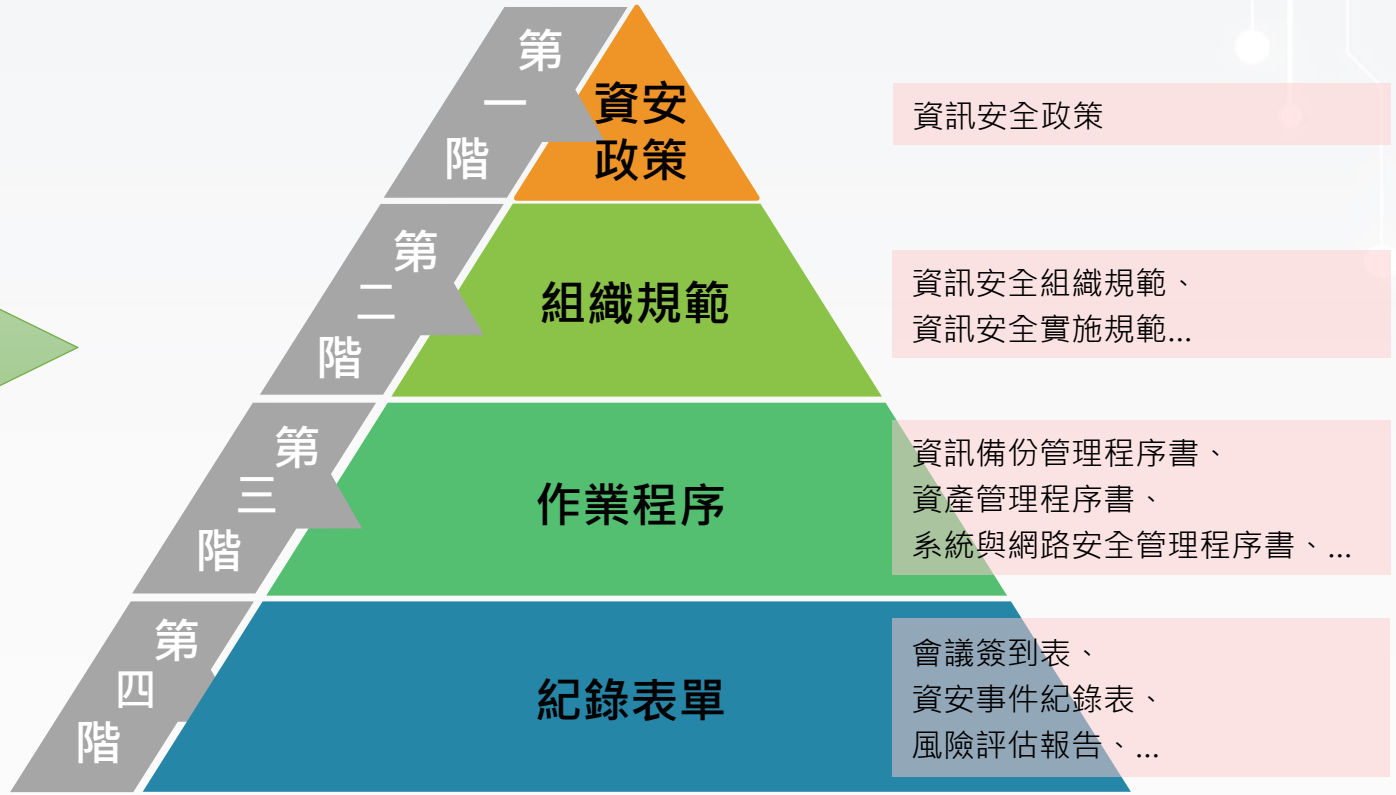
外部需求

- 相關法令及法規
- ISO 27001:2022
- 個人資料保護法
- 供應商要求
- ...

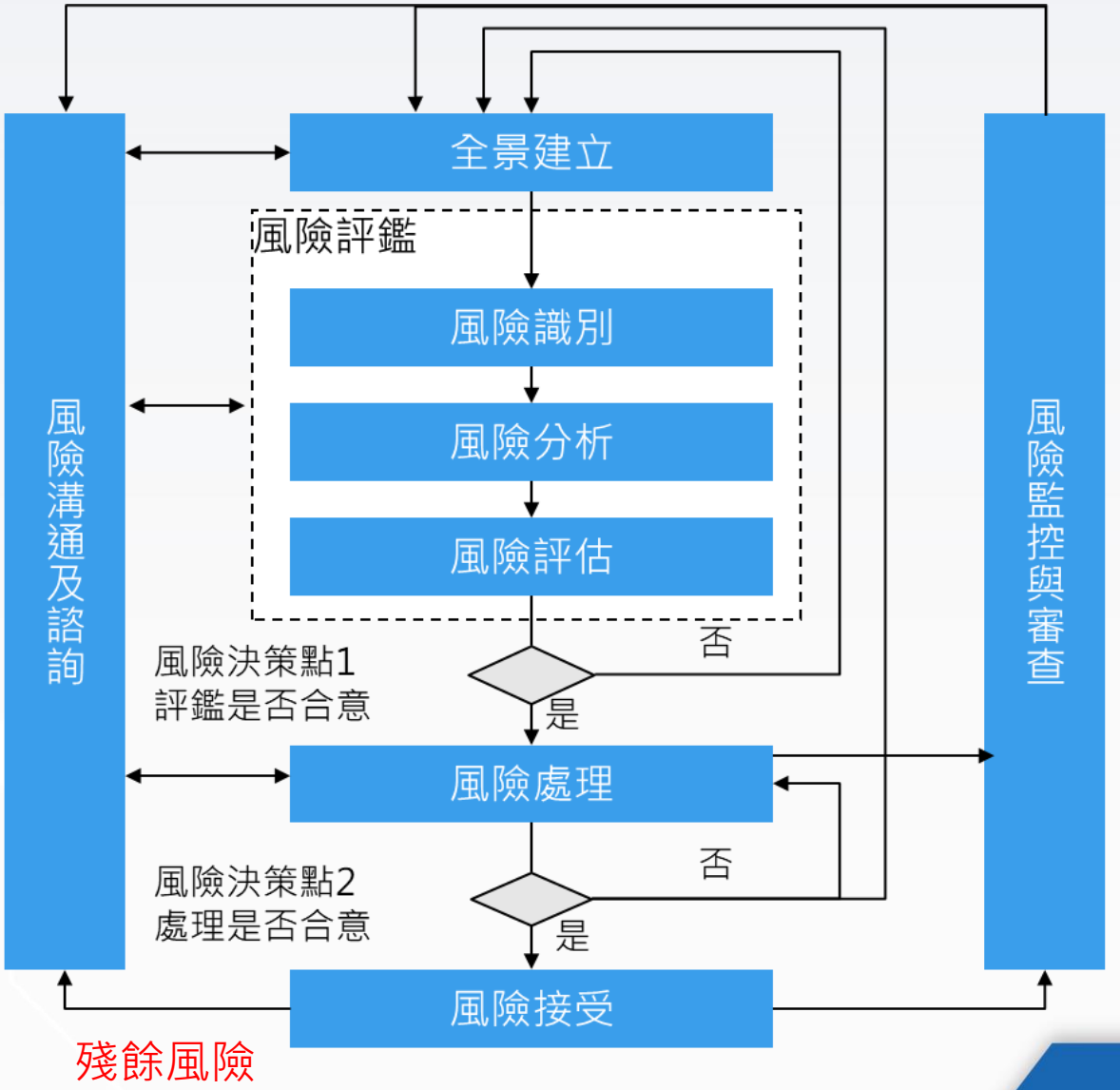
內部文件

- 風險評鑑報告
- 現有文件及表單
- 相關作業流程

整合現行作業模式



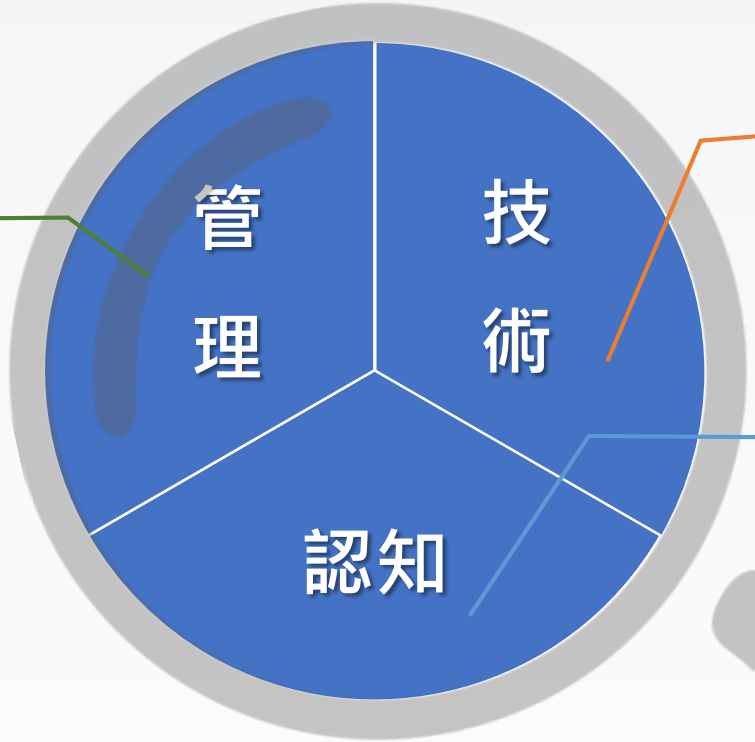
風險管理


全景建立
風險評鑑
風險識別
風險分析
風險評估
風險決策點1
評鑑是否合意
否
是
風險處理
風險決策點2
處理是否合意
否
是
風險接受
殘餘風險
風險溝通及諮詢
風險監控與審查

觀察資安怎麼做?

從「資通安全管理法」看資安

- ISMS輔導
- 持續運作演練
- 內部稽核輔導



- 網站安全弱點檢測
- 系統滲透測試
- 資通安全健診
- …

- 資通安全教育訓練[一般、資訊]
- …

事前防護 | 事中應變 | 事後復原

觀察資安怎麼做?

從「上市上櫃公司資通安全管控指引」看資安

- 資訊資產盤點
- 風險評估
- 資訊安全管理制度

- 郵件社交工程演練
- 資通安全教育訓練
- 加入情資分享組織

- 須具備資安防護措施
- 依需求區隔網段

- 核心系統弱點掃描
- 核心系統滲透測試
- 系統上線前源碼掃描

觀察資安怎麼做?

圖片來源：CIO Taiwan

- 從「Secure Controls Framework」看資安

SECURE CONTROLS FRAMEWORK

#	SCF Domain	SCF Identifie	Cybersecurity & Data Privacy by Design (C|P) Principles	Pr
1	Cybersecurity & Data Privacy Governance	GOV	Execute a documented, risk-based program that supports business objectives while encompassing appropriate cybersecurity & data protection principles that addresses applicable statutory, regulatory and contractual obligations.	Organizations specify the de cybersecurity & data protecti measure success, to ensure risk management.
2	Artificial and Autonomous Technology	AAT	Ensure trustworthy and resilient Artificial Intelligence (AI) and autonomous technologies to achieve a beneficial impact by informing, advising or simplifying tasks, while minimizing emergent properties or unintended consequences.	Organizations ensure Artifici technologies are designed to transparent, explainable and related risks are governed ac considerations to minimize er
3	Asset Management	AST	Manage all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset's location.	Organizations ensure techno throughout the lifecycle of the disposal, ensuring only autho organization's network and to stored, processed or transmi
4	Business Continuity & Disaster Recovery	BCD	Maintain a resilient capability to sustain business-critical functions while successfully responding to and recovering from incidents through well-documented and exercised processes.	Organizations establish proce recover from adverse situatio as well as provide the capabi
5	Capacity & Performance Planning	CAP	Govern the current and future capacities and performance of technology assets.	Organizations prevent avoida capacity and performance limitations by proactively planning for growth and forecasting, as well as requiring both technology and business leadership to maintain situational awareness of current and future performance.

#	SCF領域	#	SCF領域
1	資安與資料隱私治理	18	資訊保證
2	人工智慧與自動化技術	19	維護
3	資產管理	20	行動裝置管理
4	營運持續與災難復原	21	網路安全
5	容量和效能規劃	22	實體與環境安全
6	變更管理	23	資料隱私
7	雲端安全	24	專案與資源管理
8	合規性管理	25	風險管理
9	組態管理	26	安全工程與架構
10	持續監控	27	安全營運
11	密碼保護技術	28	資安意識與訓練
12	資料分類與處理	29	技術開發與取得(應用程式安全)
13	嵌入式技術		
14	終端安全	30	第三方管理
15	人力資源安全	31	威脅管理
16	身分識別與驗證	32	弱點與修補管理
17	事件回應	33	網站安全

資安，我們該怎麼做

- 透過**現況盤點**了解須要做什麼？

  盤點組織資訊資產/威脅，了解組織**資訊命脈**，更有效益規劃

- 配合**企業目標**與期望調整

  挖掘**企業痛點**與期望短中長程**改善目標**

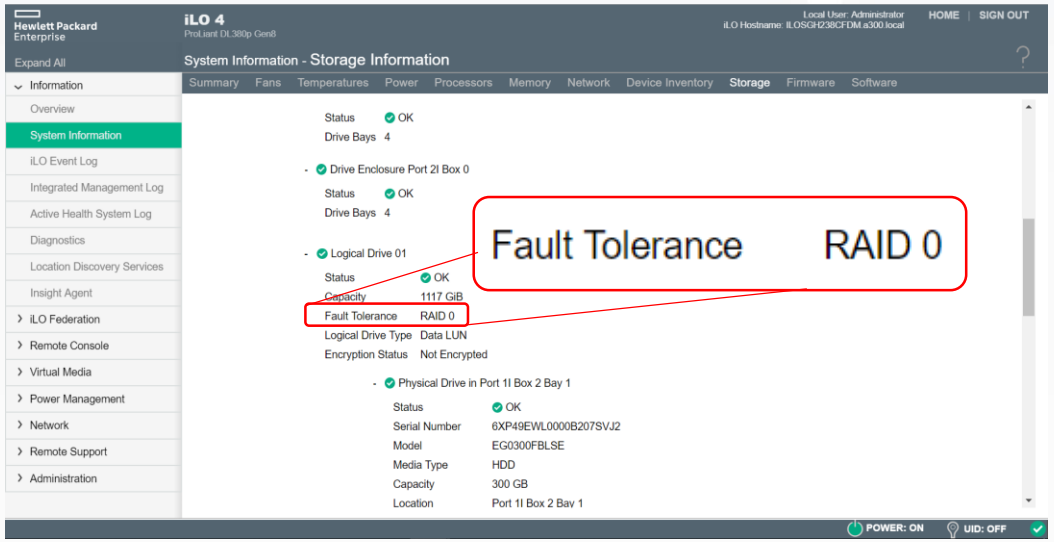
- 因應**防護需求**作好準備

  透過基礎防護、安全存取、管理制度，建立有效控管

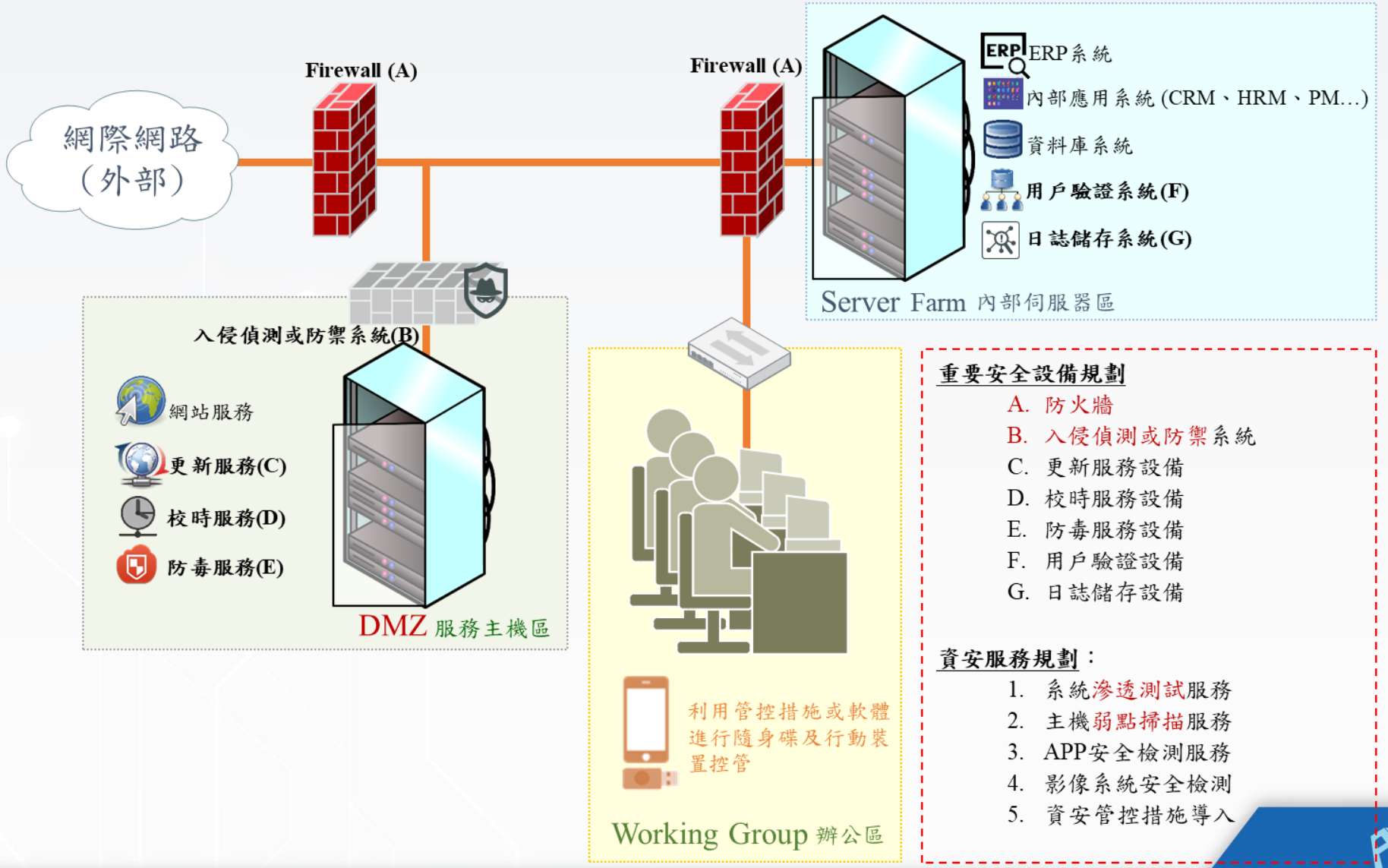
從了解做起

實務案例分享

- 案例背景：企業導入智慧化卓有成效，資訊主責 MIS*1，以需求導向
- 初步盤點了解狀況，逐步改變
  - 內網大通透、訪客區即可全看透
  - 核心伺服器潛在問題未發現
  - 事件即搶救、無備援機制
  - 同仁無資安意識概念
  - 系統管理較無文件化(網路拓樸圖)
  - 設備掌握度低、系統穩定性不佳
  - 高階設備執行低階工(防護設定)



從基礎鞏固



重要安全設備規劃

A. 防火牆
B. 入侵偵測或防禦系統
C. 更新服務設備
D. 校時服務設備
E. 防毒服務設備
F. 用戶驗證設備
G. 日誌儲存設備

資安服務規劃：

1. 系統滲透測試服務
2. 主機弱點掃描服務
3. APP安全檢測服務
4. 影像系統安全檢測
5. 資安管控措施導入

萬一的萬一，反思一下

- 如果被攻擊了，我們能偵測到嗎? → 偵測機制、…
- 如果偵測到了，我們能即時阻擋嗎? → 阻擋機制、…
- 如果阻擋失敗，我們能怎樣快速救援嗎? → 備援機制、…
- 如果資料遺失，我們能怎樣復原回來? →備份機制、還原機制
- 如果有阻擋了，看到相關紀錄軌跡嗎? → 日誌機制、…
- 如果有軌跡了，我們能探查發生經過嗎? → 調查機制、…
- 如果知道過程，我們能找出根因、能解決嗎?
- 如果…

我們不是要最強，而是要能對抗制衡

-常常問題處理成本，遠高於前置防禦-

自我檢視 - 政策規則對應

- 美國國家標準技術研究院(NIST)
- 網路安全框架 v2.0 (Cybersecurity Framework v2.0, CSF v2.0)

功能	治理(GOVEM)	
類別	● 組織全景 ● 風險管理策略 ● 角色、職責與權限	● 政策 ● 監督 ● 網路安全供應鏈風險管理

功能	辨識 (IDENTIFY)	保護 (PROTECT)	偵測 (DETECT)	應變 (RESPOND)	復原 (RECOVER)
類別	● 資產管理 ● 風險評鑑 ● 改善	● **身分管理、驗證及存取控制** ● 認知與訓練 ● 資料安全 ● 平台安全技術架構韌性	● 持續監控 ● 不良事件分析	● 事故管理 ● 事故分析 ● 事故應變報告與溝通 ● 事故減緩	● 事故復原計畫執行 ● 事故復原溝通

協同任務

- 技術防護設備/服務
  - –軟硬體設備
- 技術檢測設備/服務
  - –黑箱檢測
  - –白箱檢測
- 管理工具
  - –專案管理工具
  - –流程控管工具
- 企業資安評級
- 外部資產曝險管理

辨識能力	防護能力	偵測能力	回應能力	復原能力
資產管理	存取控制	稽核和可歸責性	事件通報	系統備份與復原
風險管理	資安意識與訓練	情境意識		
資安評估	配置管理			
	身份驗證			
	資安維護			
	媒體防護			
	人員安全			
	實體保護			
	系統和通訊保護			
	系統和資訊完整性			

Panorays

XCockpit EASM

Security Scorecard

資安眼 HorusEyes

借力評估以利輔導

角色與責任

(可多層化、也可扁平化，僅舉例參考)

角色類型	典型身份	核心責任	常見行為/任務
資安決策者	CEO、資安長、IT主管	負責資安政策方向、資源配置、風險決策	訂立政策、決策資安藍圖、核定資安預算、審閱重大事件與報告、...
資安管理者	資安專責主管、資訊部門主管	落實制度、監督流程、推動訓練與稽核	建立制度、執行訓練、核定風險評鑑、...
資安推動單位	管理部、部門窗口、資安大使	將資安觀念與要求向部門傳達、反映問題	推動訓練、協助政策落實、...
資料守護單位	文管單位、個資/隱私監督單位	管理個資/敏感資料權限、資料保留/刪除策略	資料分類、加密控管、定期審查、...
技術執行單位	資安工程師、IT人員、監控單位	維運資安設備、控管權限、修補弱點、異常偵測	防火牆管理、帳號控管、弱點修補、日誌監控、...
一般使用者	所有員工	正確使用IT資源、遵守規範、發現即通報	完成訓練、不點可疑連結、主動通報異常、...

制定資安管理規範注意要項(1/2)

- 明確性要求(避免模糊、籠統語句)
  - –應遵守公司資訊安全相關規定，並避免資安風險
  - –所有員工在使用公司資訊系統時，應遵循下列規範：
    (1) 禁止將公司帳號密碼洩漏予他人
    (2) 禁止於未經授權設備上登入公司內部系統
- 落地執行性
  - –應採取必要措施保障密碼安全
  - –使用者密碼應符合以下要求：
    (1)至少 8個字元
    (2)包含大小寫英文字母、數字與特殊符號，至少包含三種要素
    (3)每 180天需更新一次，並不得與前三次密碼相同

制定資安管理規範注意要項(2/2)

- 角色分工
  - –發生資安事件時，應依公司流程通報與處理
  - –當資安事件(如資料外洩、病毒感染、非法入侵等)發生時
    (1)發現人員應於 30 分鐘內通報資安小組
    (2)資安小組由技術經理召集，負責事件等級判定與應變啟動
    (3)事件等級達 2級以上，應由 CISO 於 4 小時內向總經理報告並研擬公告草案
- 符合內、外部要求
  - –依據《個人資料保護法》第 12 條之規定，對個人資料必須採取下列保護措施…
- 實際風險對應
  - –員工於遠距工作期間，應遵守以下資訊安全規範…
  - –員工使用生成式AI協處工作時，必須確保…

舉例生成式AI

【AI應用】

- 會議記錄、語音錄音自動紀錄
- 解決問題、程式解題協助開發
- 資料彙整、自動寫信
- 行政院及所屬機關(構)使用生成式AI參考指引(來源)

優 與 憂

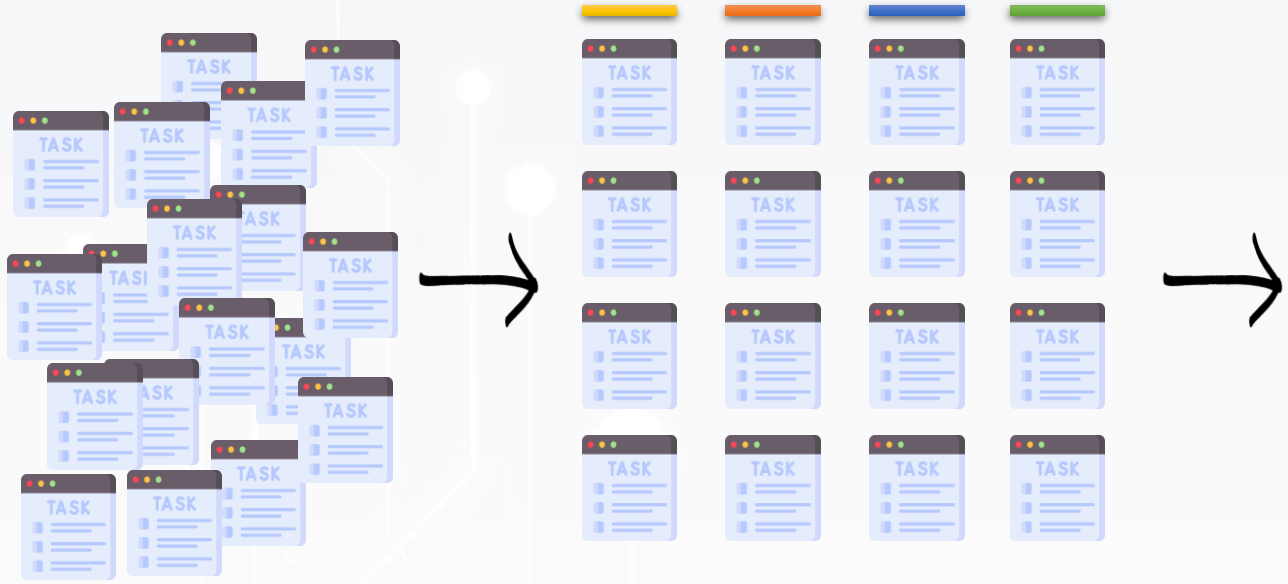
安全。機敏。信任。法規。...

常見管理失效問題(1/2)

- 條文空泛、不具可操作性
  - 例如，規範中僅提到「應加強密碼管理」，但未規範密碼複雜度或更換頻率
- 技術與管理脫節
  - 例如，部署防毒與防護系統，但對工具使用沒進行人員訓練或相關控管流程
- 政策與實務流程不一致
  - 例如，禁止使用隨身碟，但內部資料傳遞仍有多數員工使用
- 缺乏內部宣導與教育訓練，員工不清楚政策內容或理由
  - 例如，不熟悉變更管理流程(評估、授權、執行、查核等)或表單使用流程
- 政策制定後未檢討
  - 要求持續精進，PDCA循環

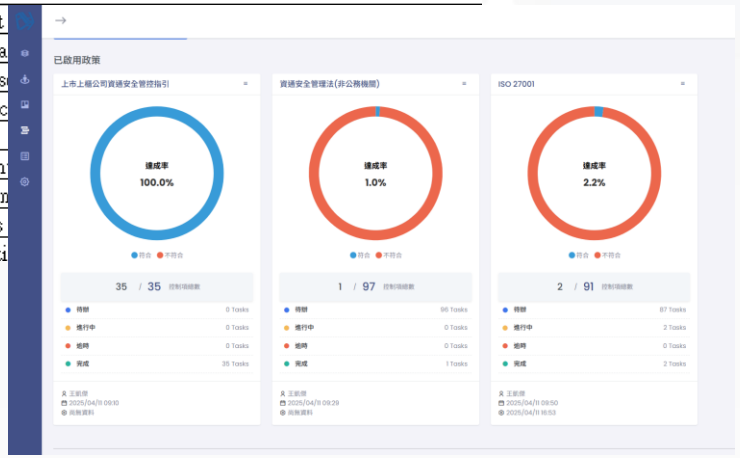
常見管理失效問題(2/2)

- 知識/工作紀錄於個人腦袋當中
- 任務工作交接不順利遺漏重要事項



任務整理

Standard	Section
A.5.1	Management direction for information security
A.6.1	Internal Organisation
A.6.2	Mobile devices and teleworking
A.7.1	Prior to employment
A.7.2	During employment
A.7.3	Termination and cha
A.8.1	Responibility for ass
A.8.2	Information classific
A.8.3	Media handling
A.9.1	Business requiremen
A.9.2	User access managen
A.9.3	User responsibilities
A.9.4	System and applicati



追蹤表單或工具平台

思考一下?

企業組織希望透過郵件社交工程演練，評估同仁的資訊安全意識水準，並藉由實際演練的過程，提醒全體人員應對可疑郵件提高警覺，避免點擊不明連結或下載附件。身為資安長的您，若需制定執行頻率與演練策略，請問以下哪一項方案最為妥當？

(1)要求每個月執行一封信郵件社交工程演練
(2)要求每半年執行一回合郵件社交工程演練
(3)要求每一年執行兩回合郵件社交工程演練

沒有所謂標準答案

總結

- ✓沒有一套制度適合所有組織，
  但可以從模仿和學習開始
- ✓沒有一套制度一輩子適用，
  有行動、有改善，才有效益 (PDCA)
- ✓資訊安全不是單一部門責任，
  而是所有同仁的承諾與守護

感謝聆聽

三甲科技
AAA Security Technology