資通安全教育訓練：
電子郵件社交工程與機敏資料保護

Joe Hsieh
Chief Operating Officer

By Royal Charter

bsi.

學　歷

- Master Degree in MIS – 加州州立大學

經　歷

- 台灣科技化服務管理協會 (ITSMA) 常務理事
- 行政院主計處政府機關資通安全委員
- 國家資通安全教育訓練講師
- BSI 驗證部協理
- BSI ISO 27001/ ISO 20000產品經理
- BSI 英國標準協會台灣分公司資訊部經理

IT專業領域

- 資訊 & 資安治理、風險管理/ 永續經營與營運持續管理
- IT服務管理、 IT專案管理
- 作業系統管理/ 資料庫管理/ 網路管理/ 應用系統開發

稽核資格及專長

- ISO 9001/ ISO 27001/ ISO 20000/ BS 10012/ CSA STAR 主導稽核員/ ISO 22301 稽核員 (稽核實績 : 超過500家以上之各領域大型企業及重要政府機關)
- IRCA國際註冊ISO 27001/ ISO 20000主導稽核員/ BSI ISO 9001主導稽核員/ IRCA國際註冊資深主任講師/ BSI ISO 27001、ISO 20000、BS 10012、CSA STAR 系列資深主任講師

BSI 英國標準協會
謝君豪 Joe Hsieh
營運長 Chief Operating Officer, COO

By Royal Charter

bsi.

Find out more
www.thebci.org

bci Thought Leadership

BCI Horizon Scan Report 2021

bsi.

bci Leading the way to resilience

風險及威脅評估

風險及威脅評估 —— 過去12個月

非職業性傷病穩居2021年排名榜首，健康與安全緊隨其後

非職業性傷病（如全球疫情）在2020年的預期風險清單上僅居倒數第二，但今年一躍成為大多數組織的主要營運衝擊原因

過去 12 個月的主要衝擊原因（風險指數排名）

- 非職業性傷病 **18.6**
- 健康事故 **18.2**
- 安全事件 **16.1**
- 資通訊中斷 **15.8**
- 網路攻擊和資料外洩 **15.3**

風險及威脅評估 —— 未來 12 個月

在接下來的12個月裡，對大流行疾病的關注繼續佔據主導地位

組織對過往衝擊事件與未來威脅之間的看法仍然存在脫節，往往關注在自覺無法控制的風險，卻忽略通常是由人為或組織失誤所引發的錯敗

未來 12 個月的主要衝擊原因（風險指數排名）

- 非職業性傷病 **9.0**
- 網路攻擊和資料外洩 **6.6**
- 資通訊中斷 **5.2**
- 法規變更 **5.0**
- 極端氣候事件 **4.8**

遭受衝擊的後果

2020年的新冠疫情危機嚴重打擊了員工的士氣與福祉

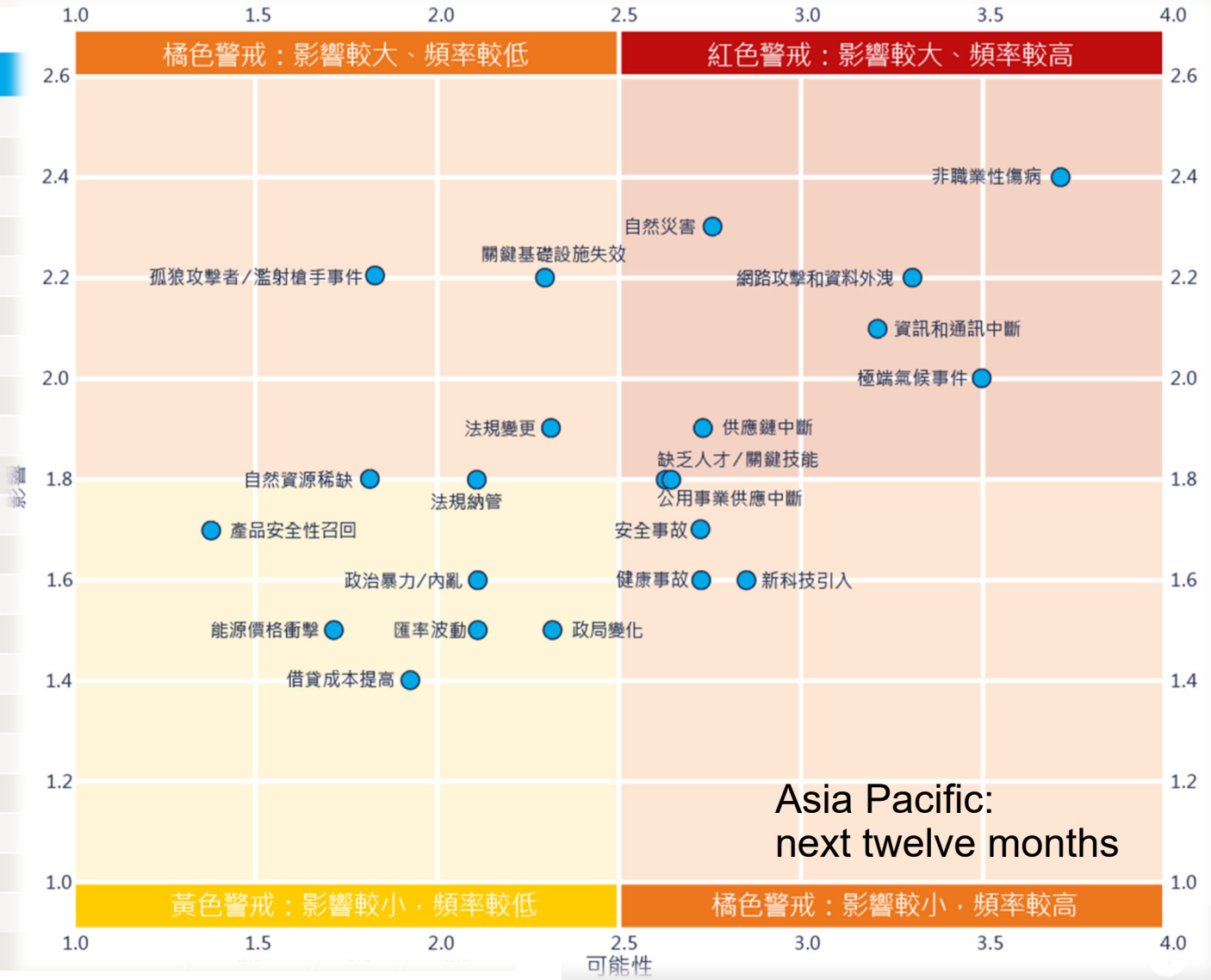
61% 的受訪者認為「員工士氣和福祉」為遭受衝擊所帶來的後果——這個資料比去年上升了 20 個百分點

過去 12 個月裡衝擊所造成的主要影響或後果

- 產能下降 **64.8%**
- 對員工士氣與福祉的負面影響 **61.4%**
- 收益損失 **51.7%**
- 工作成本增加 **43.6%**
- 員工流失或離職 **40.3%**

未來12個月的風險發展趨勢

排名	
1	非職業性傷病（如全球疫情）
2	網路攻擊和資料外洩
3	資訊和通訊中斷
4	法規變更
5	極端天氣事件（如洪水、風暴、冰凍等）
6	關鍵基礎設施故障
7	供應鏈中斷
8	健康事故（職業病、可報告的職業病、壓力/心理健康、因病缺勤增加）
9	人才/關鍵技術短缺
10	自然災害（地震、海嘯等）
11	引入新技術（物聯網、人工智慧、大資料）
12	公用資源供應中斷
13	政局變化
14	法規納管
15	安全事故（人身傷害、死亡、資產損失、危險事件、應報事件）
16	孤狼攻擊者/濫射槍手事件
17	政治暴力/內亂
18	匯率波動
19	借貸成本提高
20	能源價格衝擊
21	自然資源稀缺
22	產品安全性召回



Asia Pacific:
next twelve months

產業目前及未來面臨的關鍵維運風險及治理挑戰 (例)

Bimodal 的服務模式 (傳統服務與新創服務要同時運行)

新創及加值服務面臨之未知風險及相關治理議題

因應快速ICT服務(微服務/DevOps)所衍生的控管挑戰

資訊系統/ 服務開發及維運面臨之品質、效率及安全

因應不同單位所負責之業務特性，需滿足的資安強度

IT所提供之資訊系統/ 服務障礙回應及復原(SRP)能力

對客戶資料保護之管理及控管能力(Cyber attack)

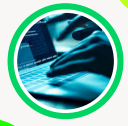
IT面臨越趨複雜化之資訊委外，監督管理機制之適切性

法令法規變化及關注方之要求(如: 資安法/ 主管機關)

2020 產業CSR報告：資訊安全管理已成為重要關注議題之一

強化資安治理的迫切性 – 風險無所不在

駭客攻擊：2021 04 多達10萬個網站並安裝木馬程式，甚至利用PDF檔案滲透



駭客攻擊： 2021 04 趨勢科技軟體舊漏洞遭駭客攻擊

個資及營業祕密外洩：2021 03 中國工程師偷看Line用戶個資

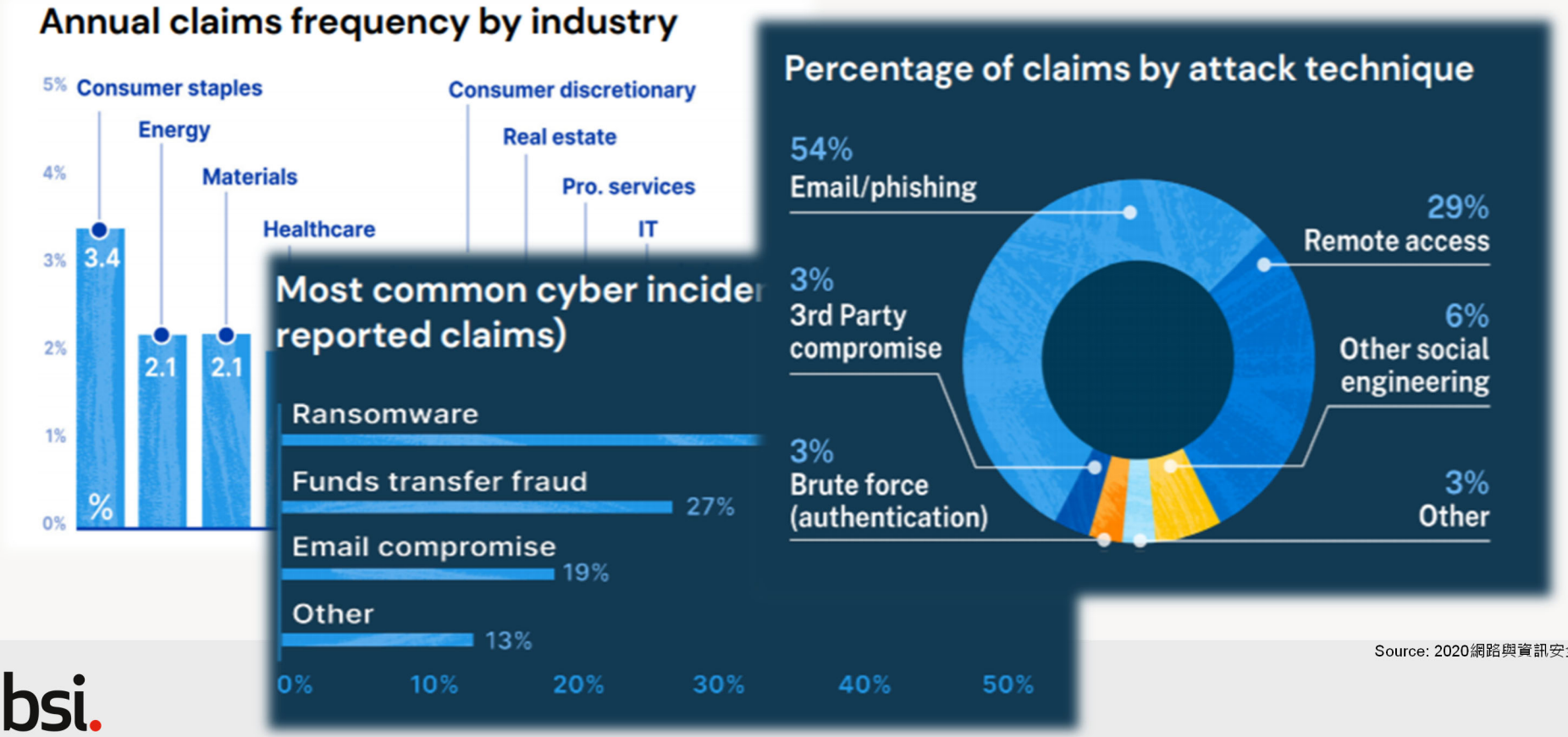
駭客攻擊：2021駭客鎖定製造業發動目標式勒索和DDoS攻擊 (成為新常態)

駭客攻擊：2021 01 電信商手機在供應鏈被惡意軟體滲透，用戶簡訊OTP被攔截導致身分冒用

營運中斷：2020 05 ~ 2021 04 中油、台塑、半導體廠、高科技廠等遭勒索軟體攻擊，造成營運中斷

從資安保險理賠看風險

北美資安險業者Coalition統計該公司內部以及外部數千個保險資料後發現，發現雖然2020年組織因遭勒索軟體攻擊而索賠的案例，比前一年少了18%，但嚴重等級卻增加了，包括駭客要求更高的贖金，恢復正常運作的成本也增加。



攻擊技術

- 郵件釣魚 (54%)
- 遠端存取 (29%)
- 除郵件外社交工程 (6%)
- 第三方工具 (3%)
- 暴力破解 (3%)

Source: 2020網路與資訊安全保險業者Coalition索賠報告

從台灣政府機關資安威脅情勢看組織可關注之面向

社交工程搭配時事議題做為攻擊主軸

APT類型攻擊轉而利用商用工具軟體與服務

供應鏈攻擊活動加劇

物聯網攻擊鎖定監視與網通設備

勒索軟體攻擊風險激增

Source : 行政院國家資通安全會報技術服務中心 109年12月

資安防禦的挑戰 – 攻擊工具易於取得及多樣化
(地下市集 - Underground marketplace price list) - Dark Web

地下市集牌價表
您想要的都有
(匯率: 1 : 30計算)

Cyber attack攻擊手法的多樣化 - 行動式設備/ BYOD攻擊

資料外洩

不安全的
無線網路

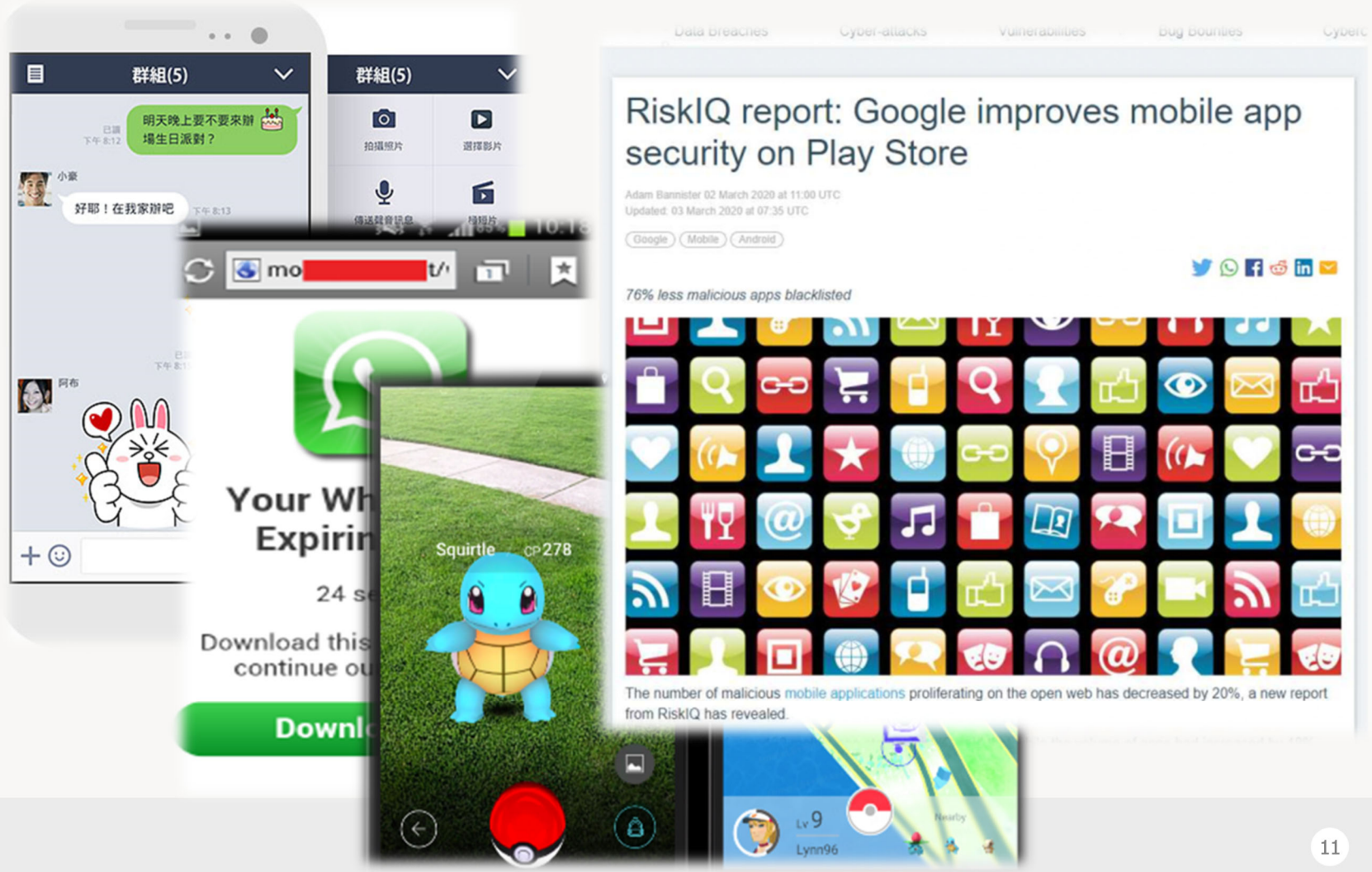
網路釣魚
郵件攻擊

間諜軟體

惡意程式
apps

弱密碼保護

設備作業
系統未更新



Cyber attack 攻擊手法的多樣化 – Ddos (阻斷服務攻擊)

為駭客利用大量偽造且無意義的封包藉以消耗被攻擊者的網路頻寬與系統資源，導致網路癱瘓，無法提供正常的服務

Source : https://horizon.netscout.com/?mapPosition=0.00~0.00~1.00

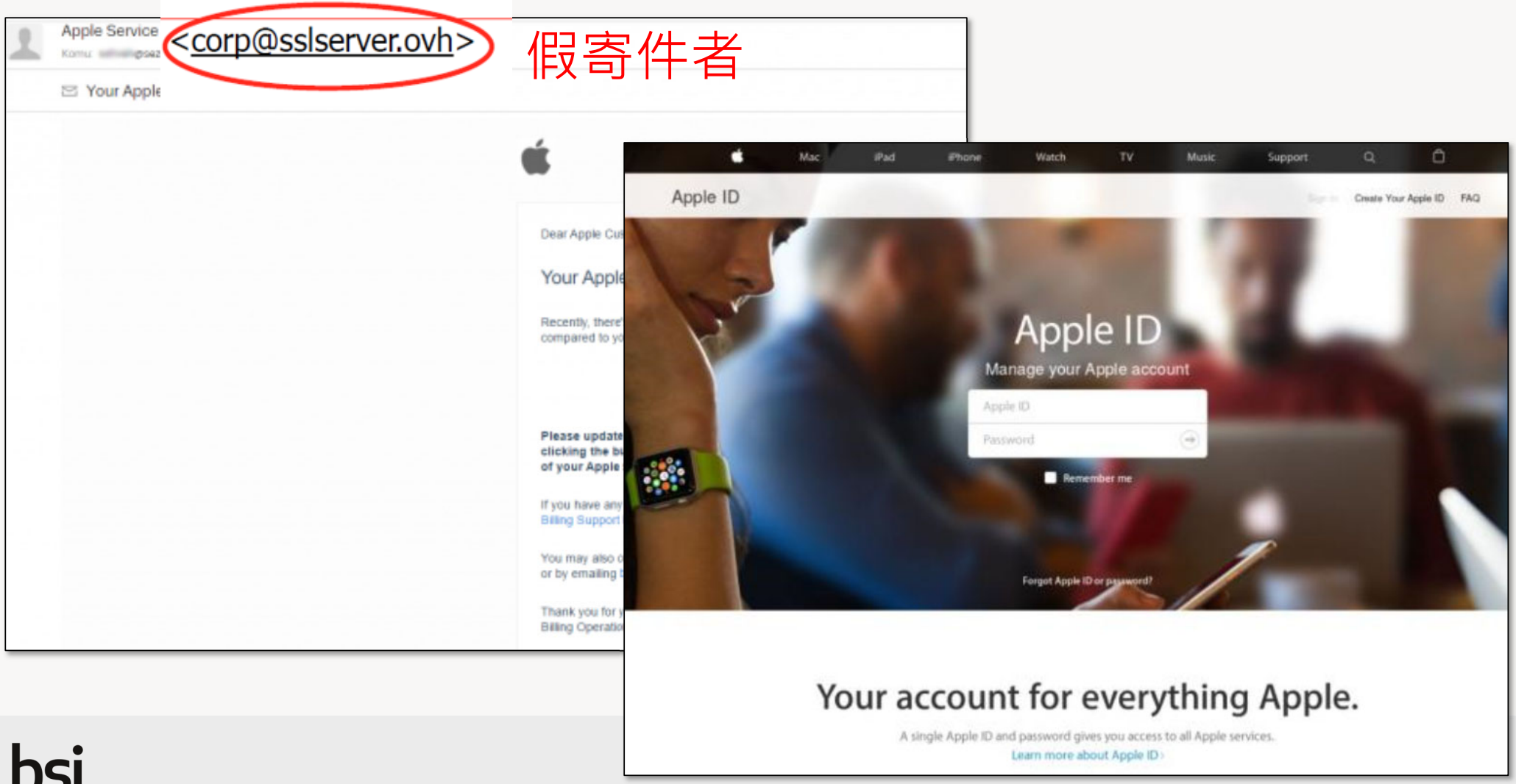
Cyber attack攻擊成功的主因 – 安全意識之缺乏

常用攻擊企業的主旨類別還包含：政治、會議、採購、健康養生、購物、金融、遊戲、八卦、旅遊...等。

社交工程：下列主旨的郵件您是否會開啟?

信件類別	寄件者	信件標題
時事類	1Thome<1theme@yahoo.com.tw>	駭客攻擊8 家券商 金管會：恐還有下波
知識類	黃泰豐<larry1217@gmail.com>	「食色性也」不是孔子說的
健康類	綠色地球<xm4nk499@yahoo.com>	別再用寶特瓶裝水了！各項研究告訴你它可怕的真相！
美容類	Hellen<hellen520@gmail.com>	染唇妝過時啦！2018跟著李聖經擦上微醺MLBB唇才最潮
生活類	韓流最前線<girlpretty@hotmail.com>	變更嬌小，惹人疼！「胖胖單品」逆轉勝
新奇類	李蓉芬<melody8056@msa.hinet.net>	小二生超狂造句 讓網友驚呼：他超懂人性
美女類	杜肯<kentdo5717@outlook.com>	正妹車服員神到了 曾是黑澀會美眉
科技類	新北資訊通<newtaipeinews@yahoo.com>	新北打造智慧城 力推手機無線充電服務
旅遊類	LIME news<limemews@hotmail.com>	領務局LINE 新功能 出國旅遊添保障
財經類	巨富網<richnessnet@outlook.com>	貨幣戰開打？中國單月狂拋660億美元美債！創5年新高

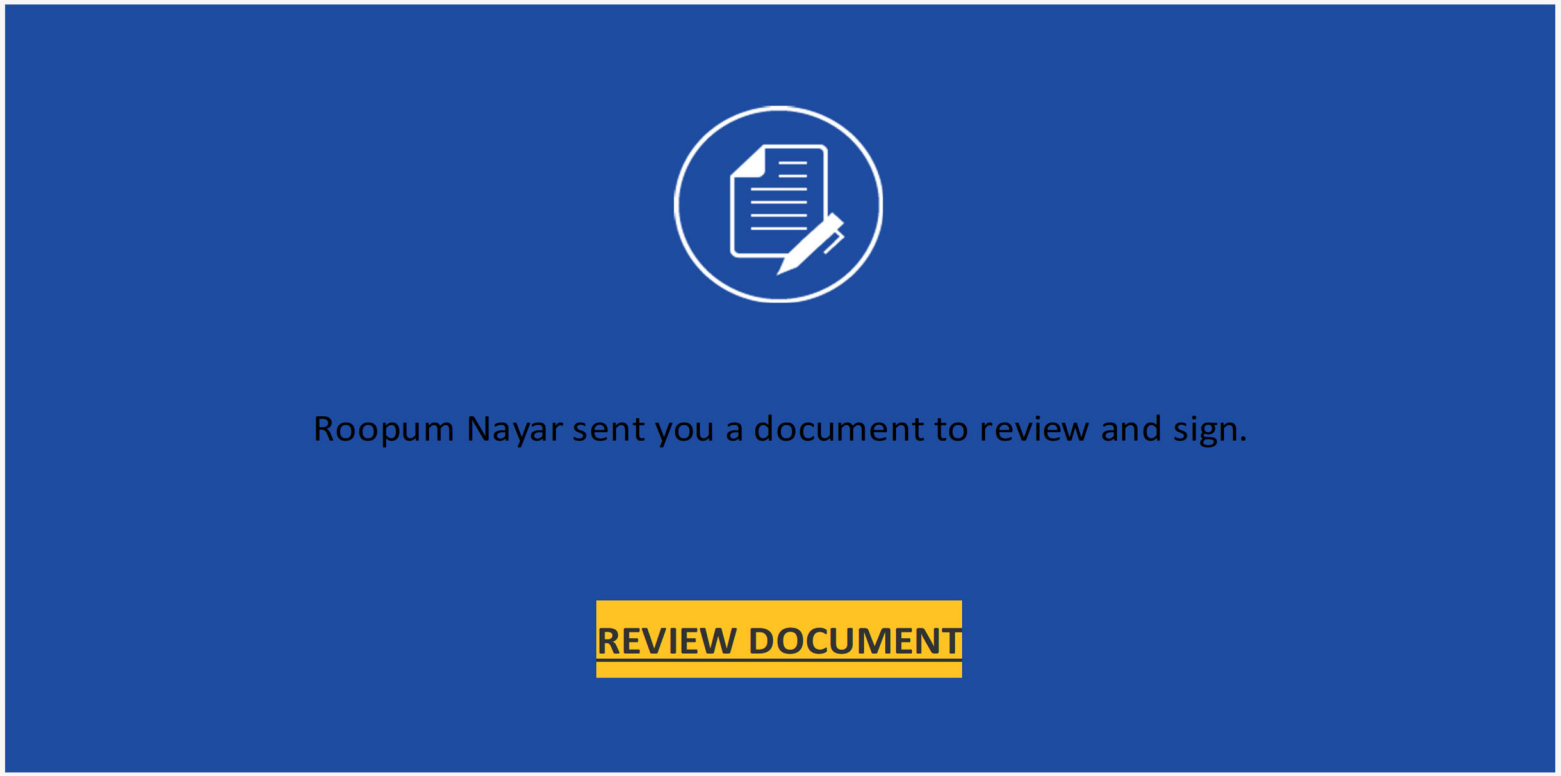
What Phishing looks like -假冒 Apple 名義發送的網路釣魚郵件



社交工程：哪一個網頁是正確的? (偷竊個人敏感資訊)

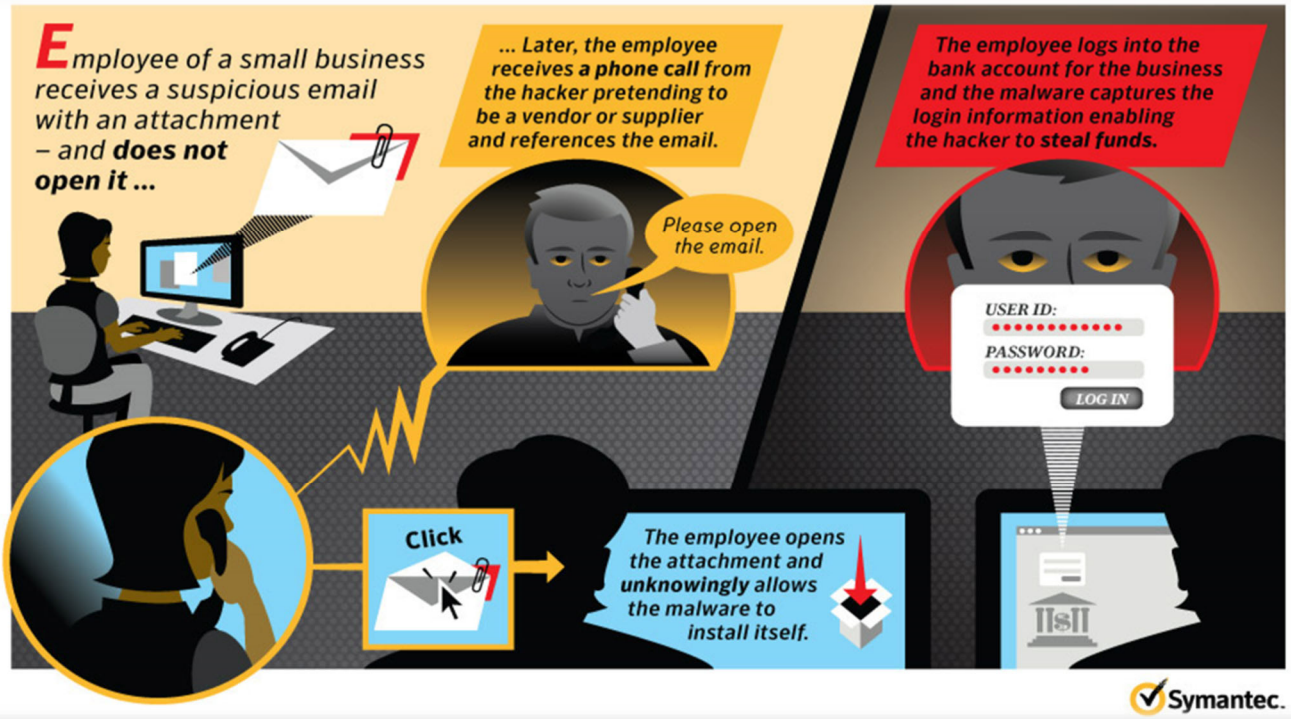
社交工程 (融入到企業的日常作業：竊取企業敏感資訊或是勒索)

DocuSign



社交工程：FBI 警告：「Vishing」攻擊，竊取企業帳號登入資訊

所謂「vishing」就是「voice phishing」（語音釣魚攻擊），是一種社交工程攻擊技術；攻擊者會假冒為受害者信任的個人或單位，利用語音通話與各種話術，試圖從受害者取得各種機敏資訊，例如金融帳戶或企業各種系統的登入資訊。



攻擊者先利用傳統釣魚攻擊方式，取得企業內部網路的權限，之後再透過 vishing 語音釣魚攻擊，和內部僱員的**通話中**，取得**更高權限**的帳號登入資訊。

誘導受害企業的僱員，利用假的 VPN 服務連線到攻擊者設立的**假網頁**，以騙取登入帳號。

大量美國企業，因疫情關係改為**遠距工作**員工在外大量使用 VPN，給攻擊者利用 vishing 攻擊手法**取得VPN的登入資訊**，混入企業內部網路後，發動進一步的攻擊。

Source：資安人/ Symantec

Your network has been infected!

Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **General-Decryptor**

Follow the instructions below. But remember that you do not have much time

General-Decryptor price

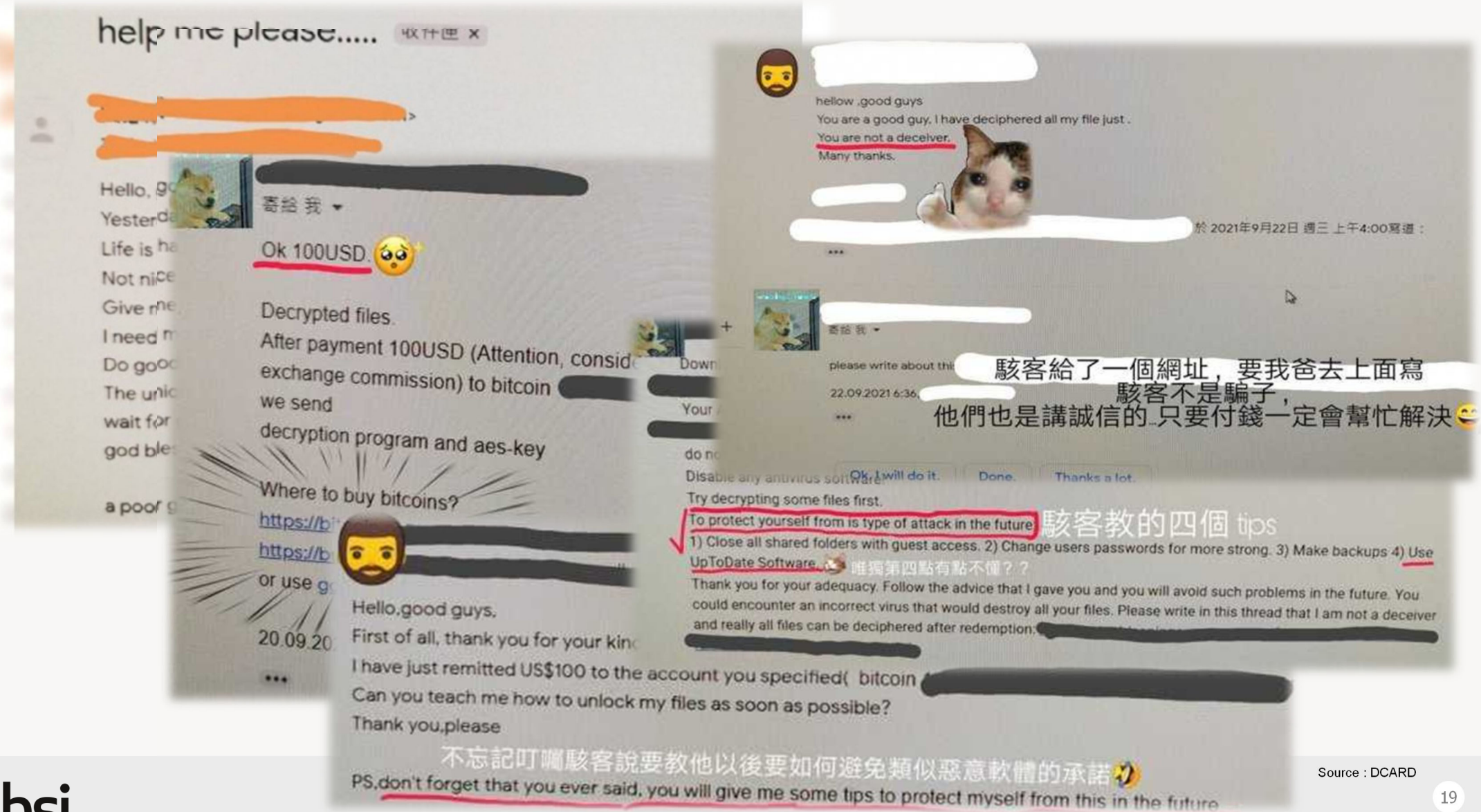
the price is for all PCs of your infected network

You have 8 days, 19:07:29

* If you do not pay on time, the price will be doubled
* Time ends on **Mar 28, 16:30:11**

Current price: 214151 XMR ≈ 50,000,000 USD

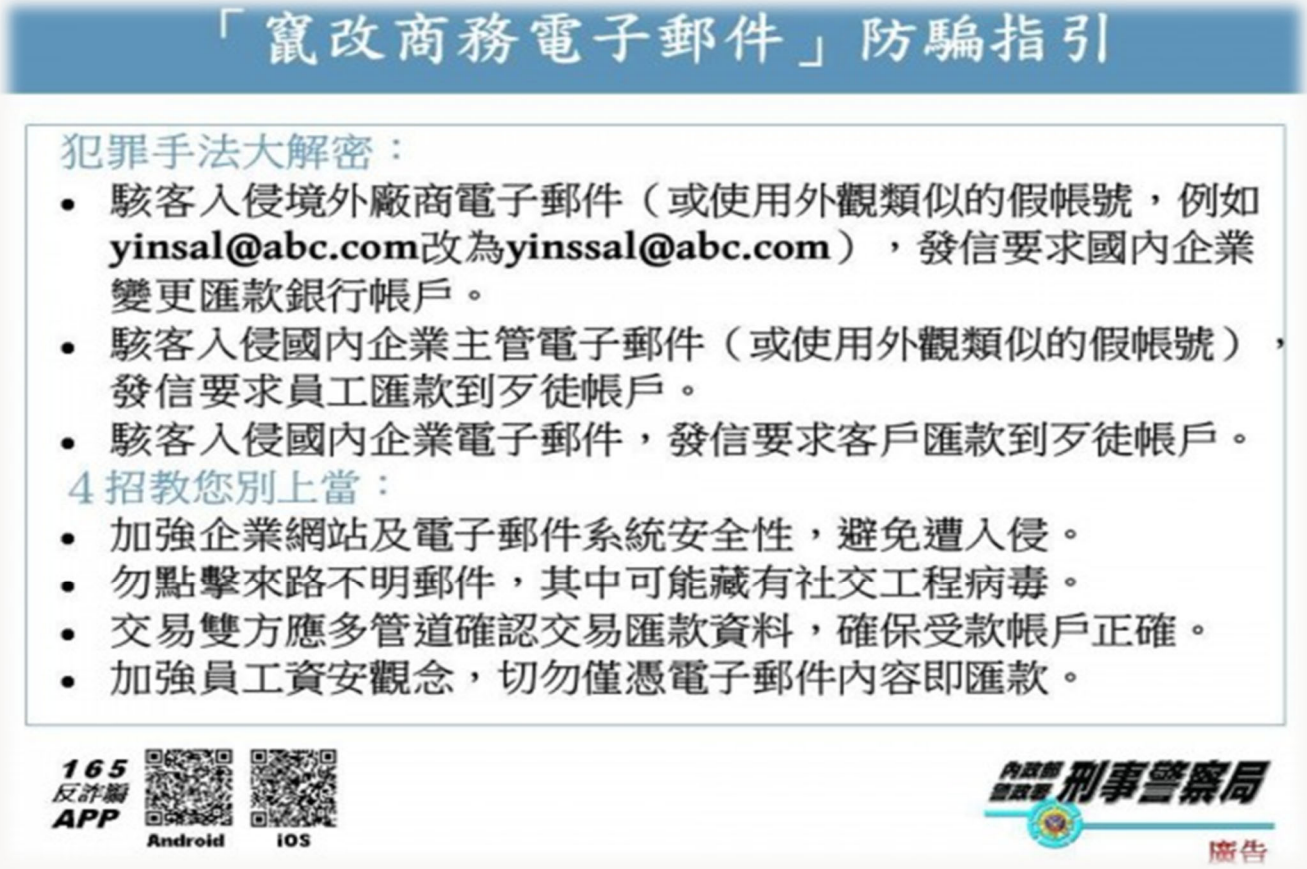
After time ends: 428302 XMR ≈ 100,000,000 USD



Source : DCARD

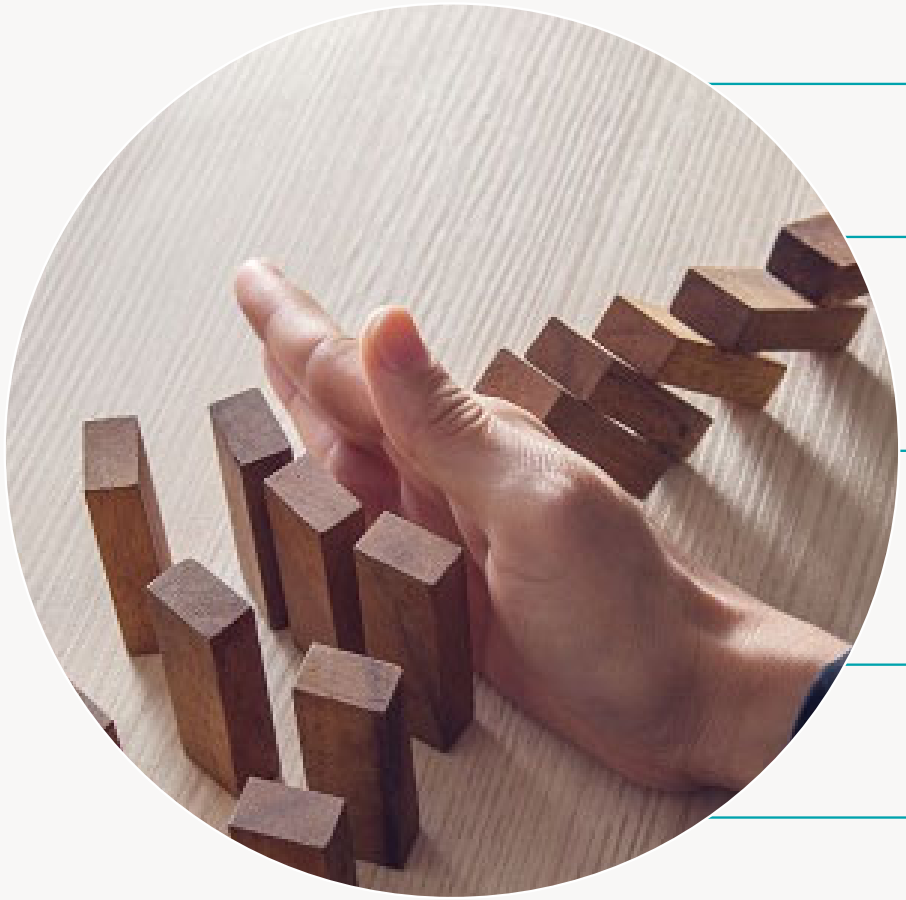
另一種可能的攻擊型式：
企業電子郵件詐騙 BEC (BUSINESS EMAIL COMPROMISE)

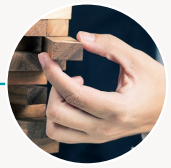
- 藉由入侵端點檢視郵件
- 等待機會並檢視郵件往來
- 利用垃圾信機制
- 要求廠商匯款到指定帳號
- 得手不法利益



Source : 刑事局

企業員工因應勒索軟體攻擊應注意的事項





使用隨身碟、外接硬碟或者雲端空間，備份重要資料。

關閉 Windows 系統的 445 等危險通訊埠，關閉網路共用資料夾。

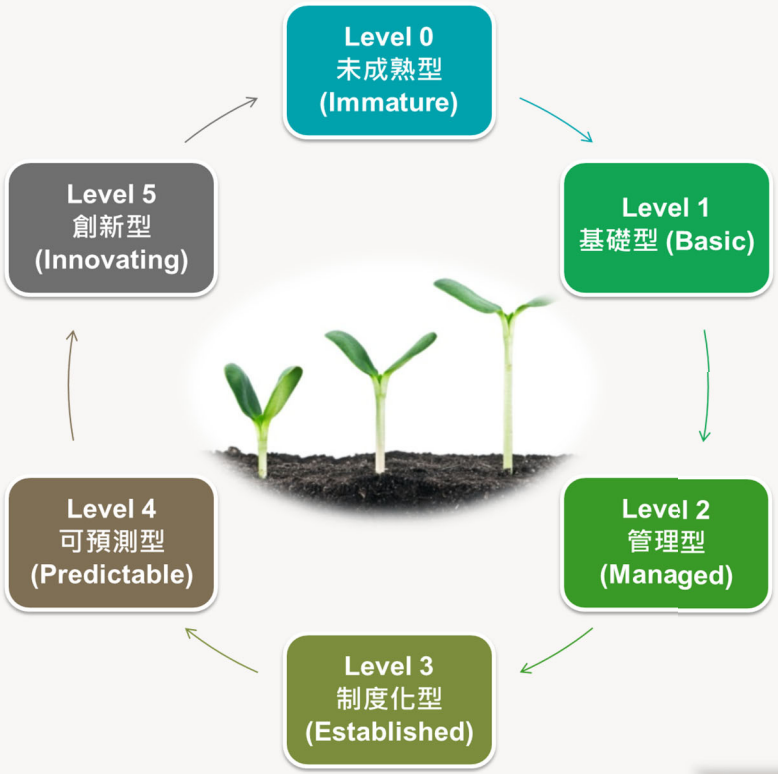
不要點擊來路不明的網站和檔案等。

如果使用者的電腦已遭攻擊，請記住千萬不要乖乖繳納贖金，這是無用之舉。

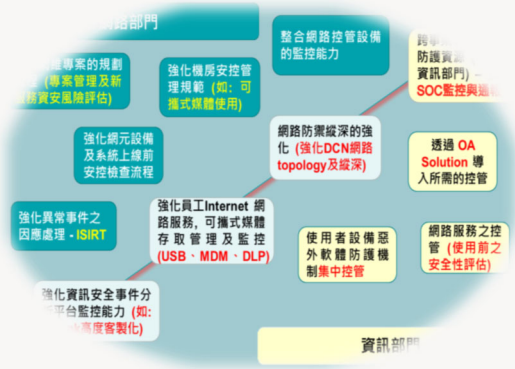
開啟電腦作業系統的 Windows Update，隨時升級系統與修補漏洞。

提升企業在資安之遵循及成熟度

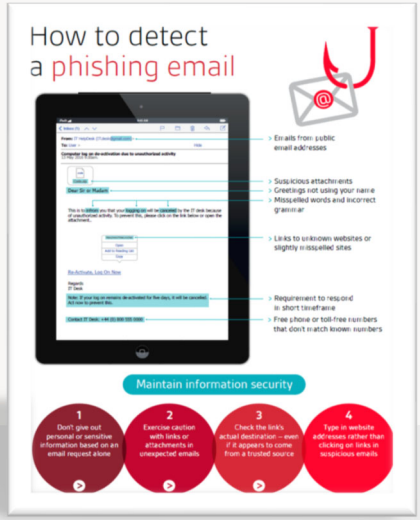
優化既有制度及文化、降低便宜行事及提升落實度



技術面

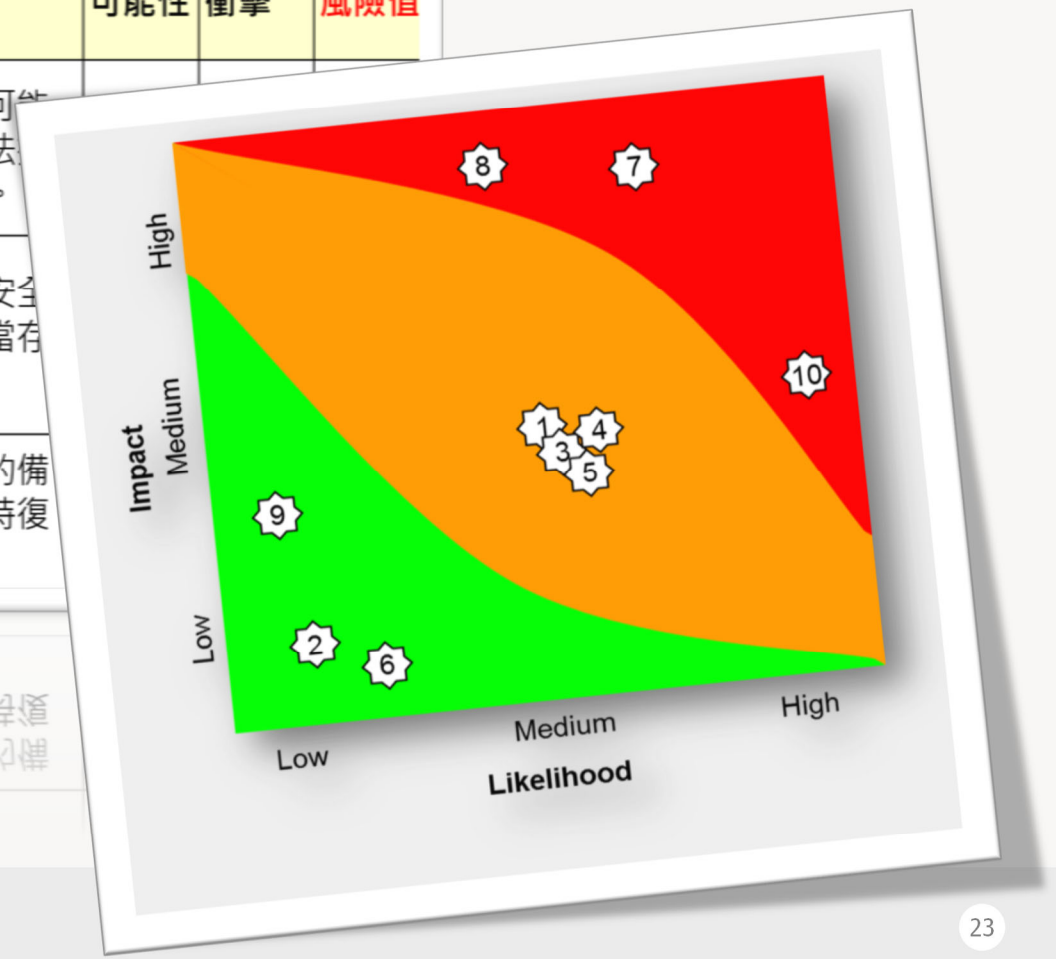


認知面



鑑別集團所面臨的關鍵風險，並勾勒出集團的風險地圖

風險編號	風險來源	風險	風險描述	可能性	衝擊	風險值
3D1	日常作業流程控管	勞工安全及健康議題－沒有明確陳述於工作職掌內	沒有提供足夠等級的支持或是對所有可[illegible]議題提供足夠的調查及研究。因此無法[illegible]供明確的指引供管理階層參考及決策。			
3D2	商業法律關係	未能監控到資訊系統之線上環境資料被未經授權的修改或查詢	針對客戶提供的研發資料未有充足的安全[illegible]防護措施，客戶敏感資料有潛在的不當存取風險。			
3D3	商業法律關係	關鍵設備維護委外廠商未能及時提供所需的服務或支援	因為合約限制無法要求廠商提供足夠的備品及維護時效，導致關鍵服務無法及時復原。			



相關的管理規範必須能否有效的因應企業業務的變化 (數位化時代創新的挑戰) - 避免便宜行事

企業所訂定的管理規範是基於 **“符合性”**而訂? 還是基於 **“有效性”**？

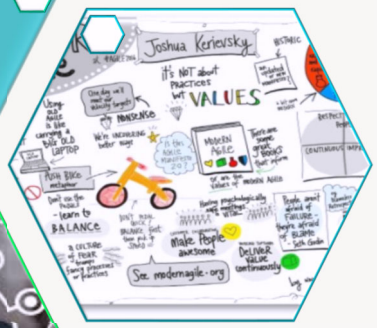
IoT

Fintech

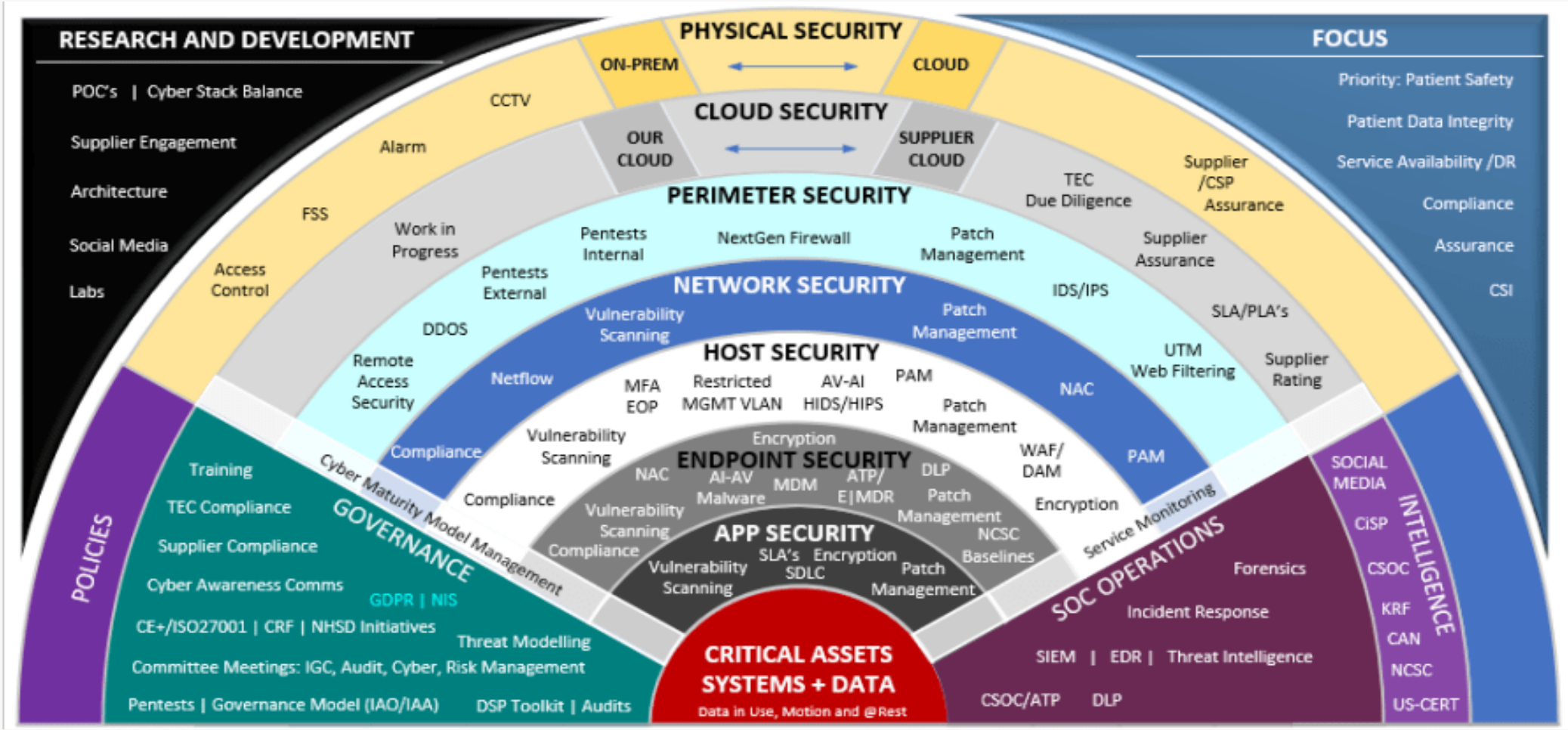
Innovation

AI

Bimodal

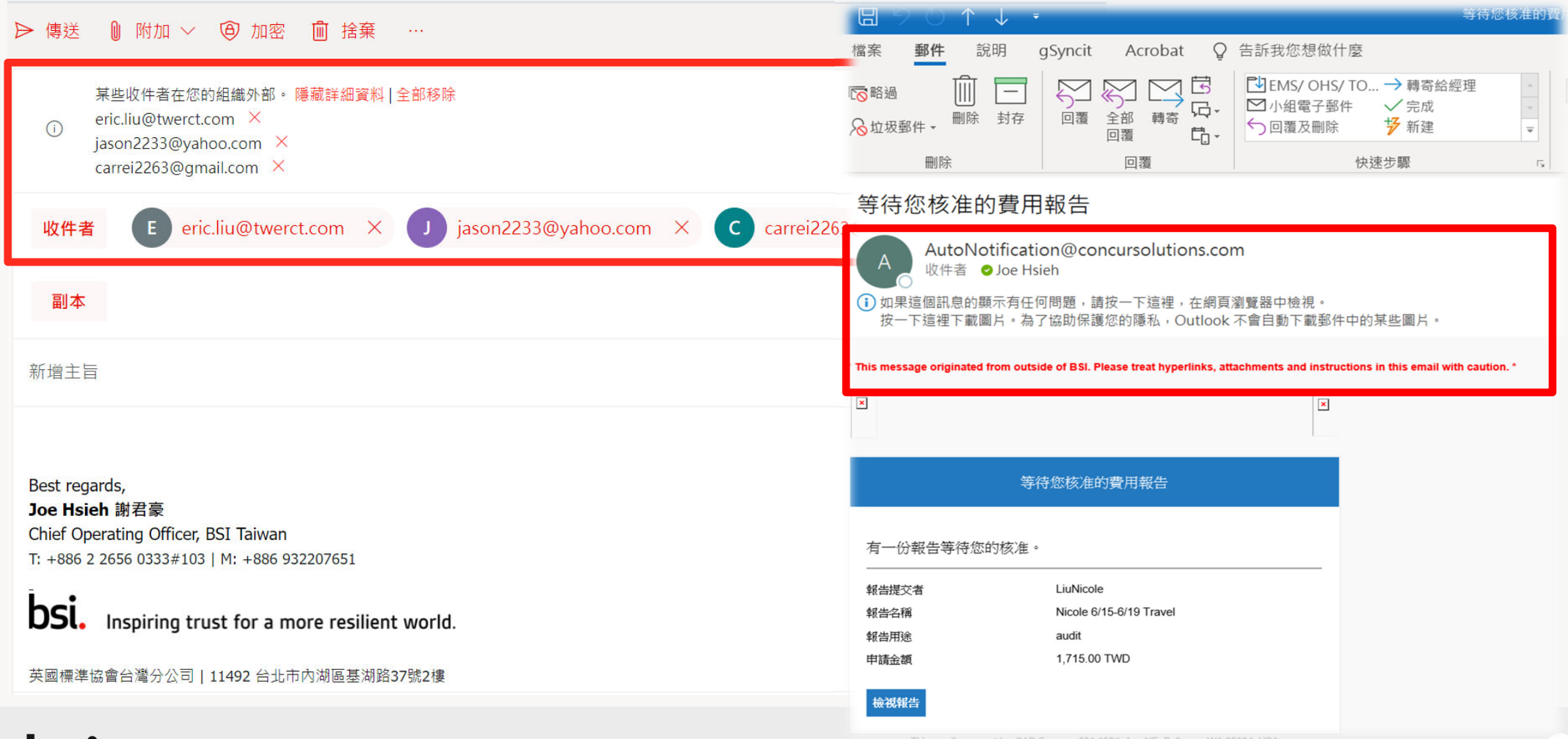


導入必要的安控工具及自動化 – 提昇管理有效性



Source : https://www.peerlyst.com/posts/nhs-healthcare-defense-in-depth-shaun-van-niekerk

透過技術面作為降低被攻擊的機會 (例)

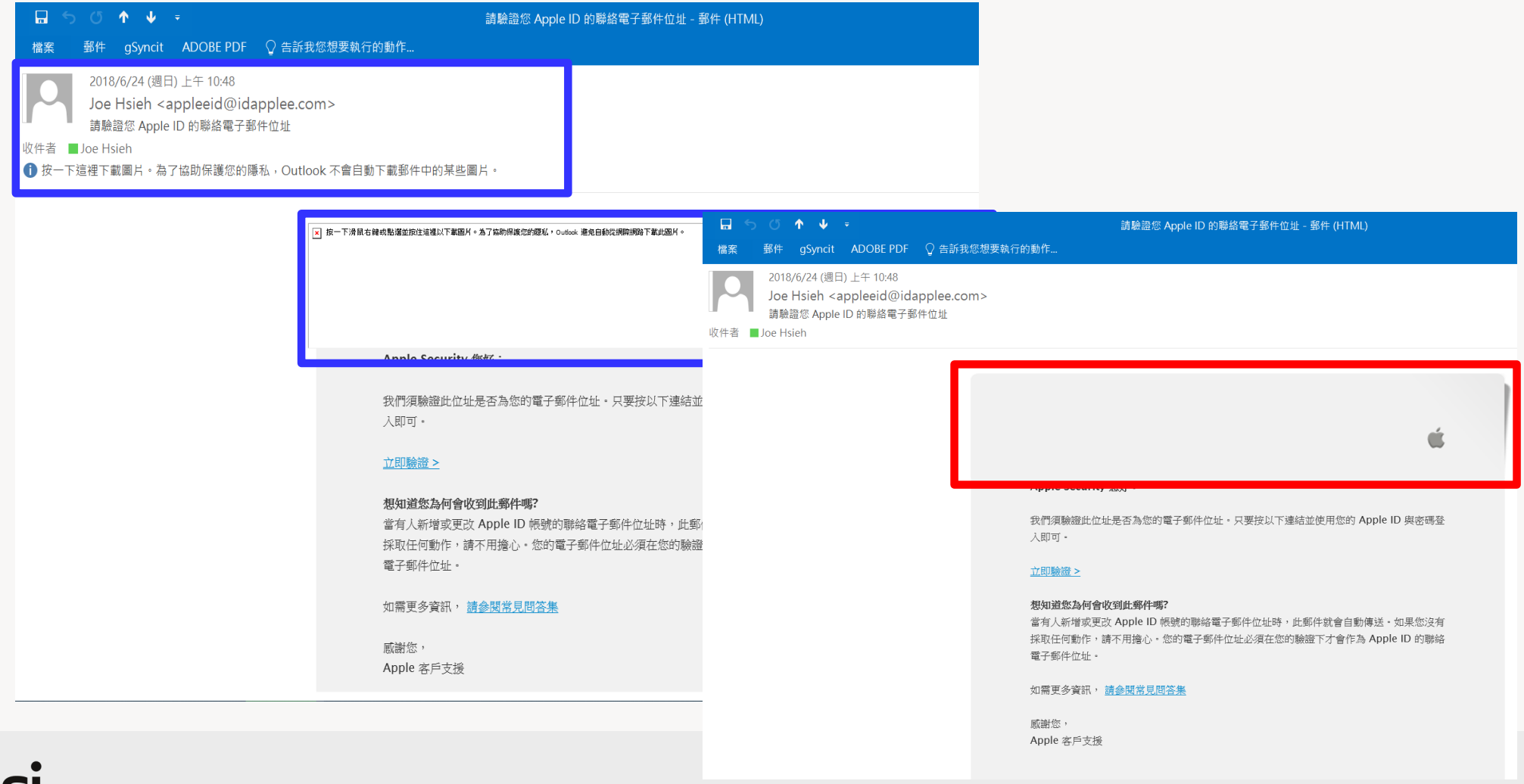


企業的主管及同仁必須了解應肩負的責任

降低落實度及認知不足所造成的風險

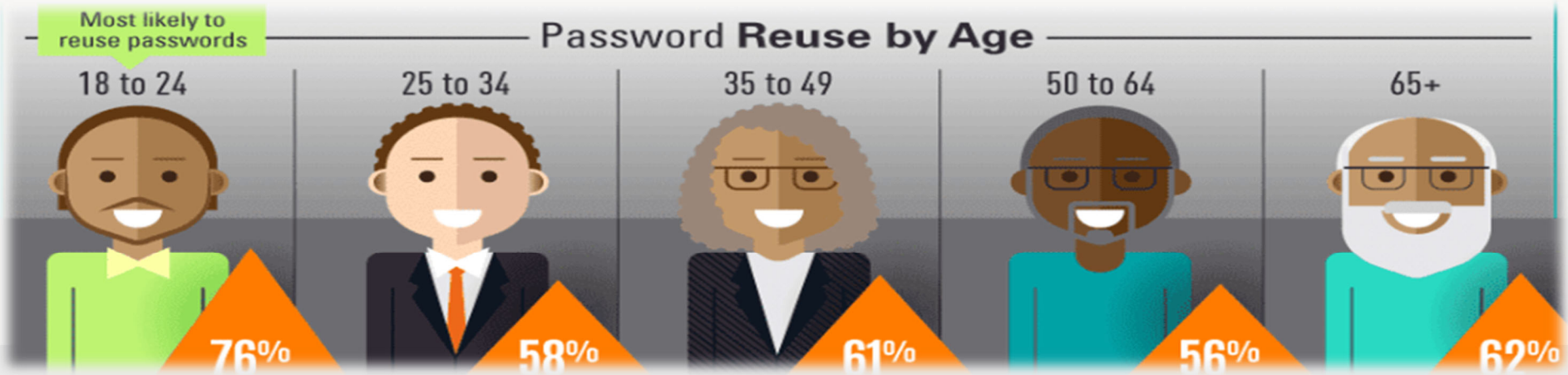
- 同仁認為資安及個資保護是IT或是主辦單位的責任
- 不熟悉日常作業的資安管控要求
- 不願意配合資安相關規定(如: 自行委外.....)
- 輕忽數位化後可能遭遇到的資安及個資保護風險
- 單位內部推動的權責不夠明確

提升認知：降低社交工程攻擊的風險



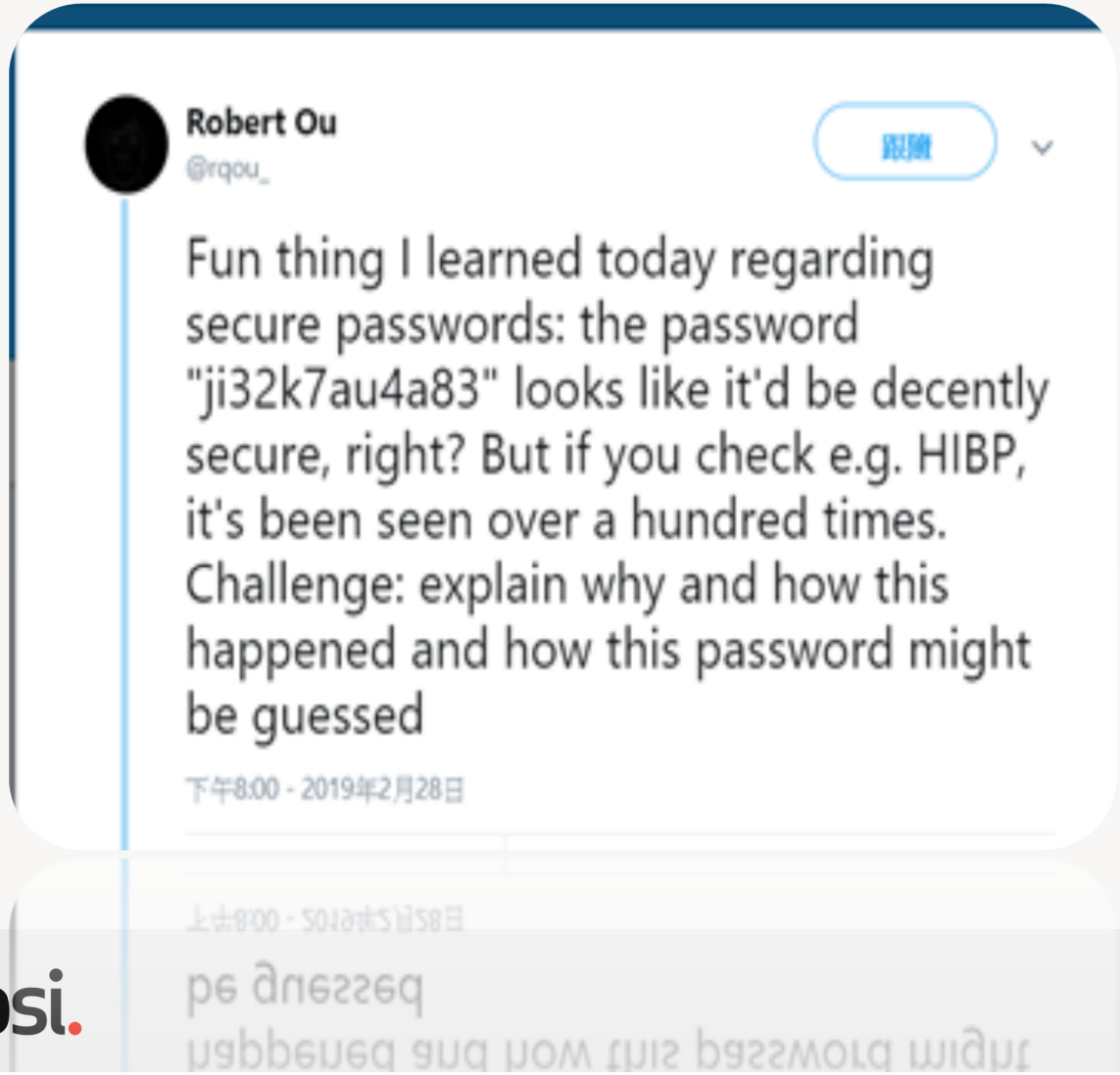
提升認知：使用者所使用的密碼 (Password) 品質及強度之提升

2020最常使用之密碼		
1 - 123456	8 - 12345	15 - 000000
2 - 123456789	9 - 1234567890	16 - 1234
3 - picture1	10 - senha	17 - iloveyou
4 - password	11 - 1234567	18 - aaron431
5 - 12345678	12 - qwerty	19 - password1
6 - 111111	13 - abc123	20 - qqww1122
7 - 123123	14 - Million2	21 - 123

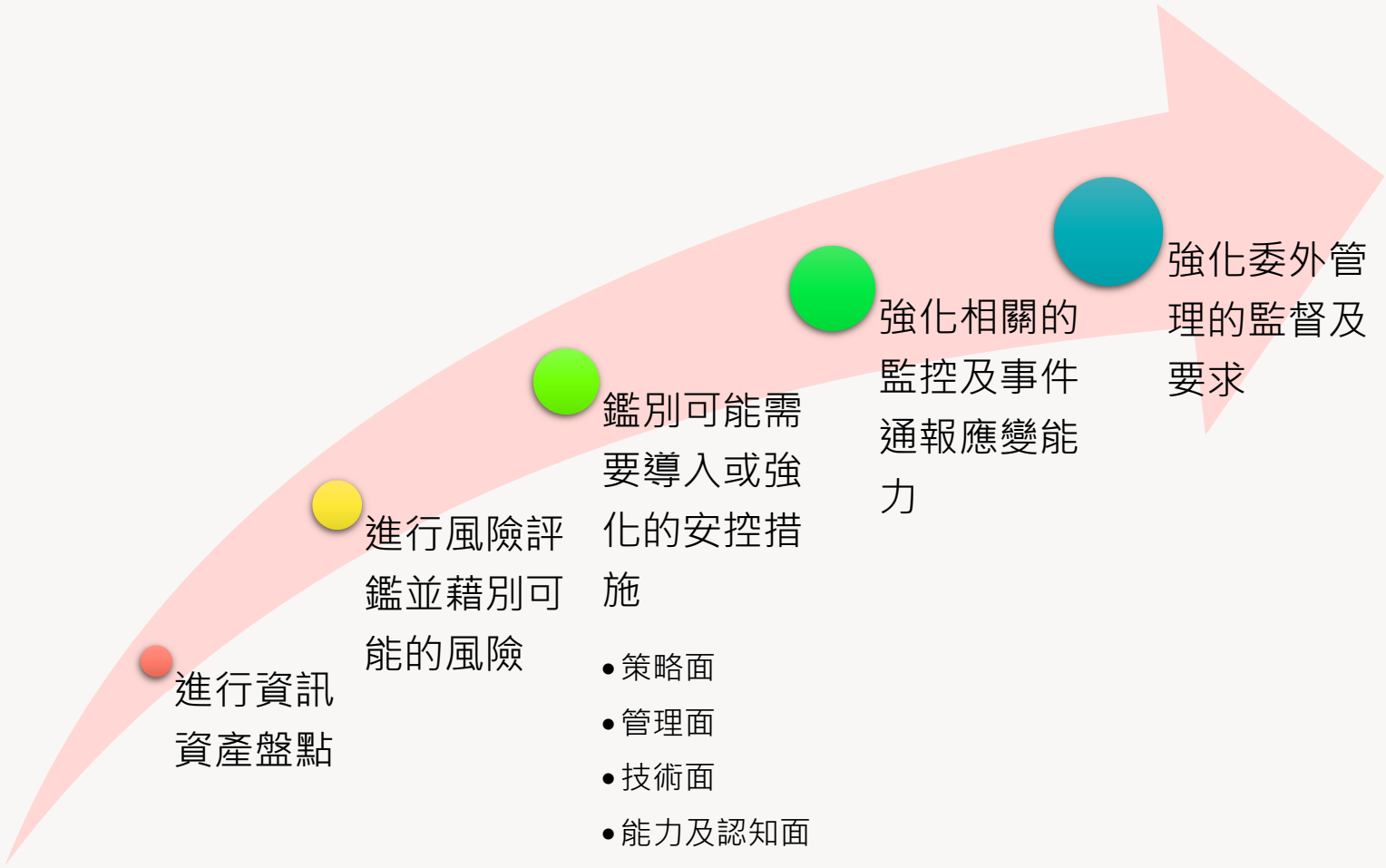


Source : NordPass 2020 & Rock IT

提升認知 - 案例：為什麼「ji32k7au4a83」這組密碼超級熱門？

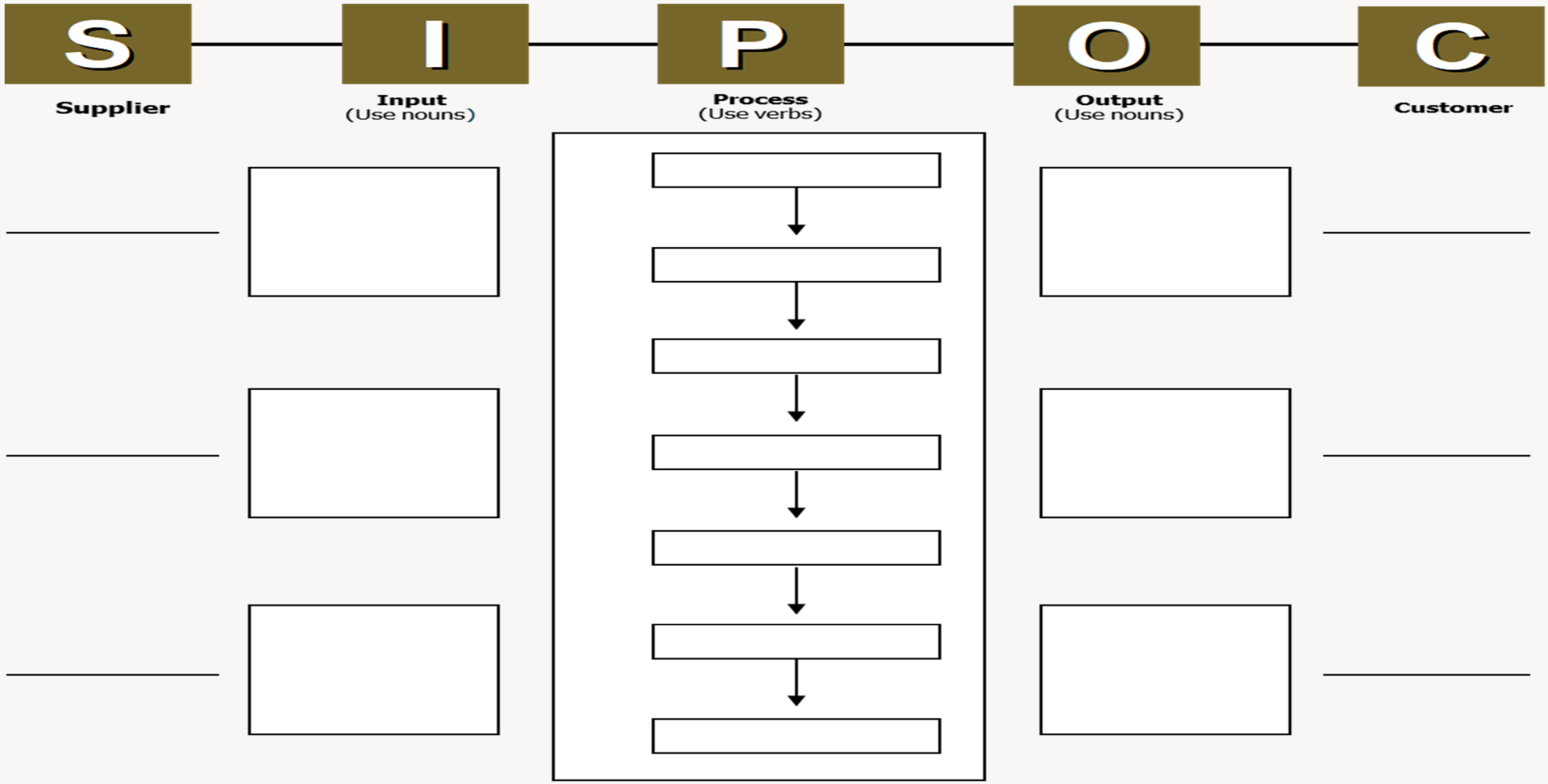


企業如何保護機敏感資料 (例)

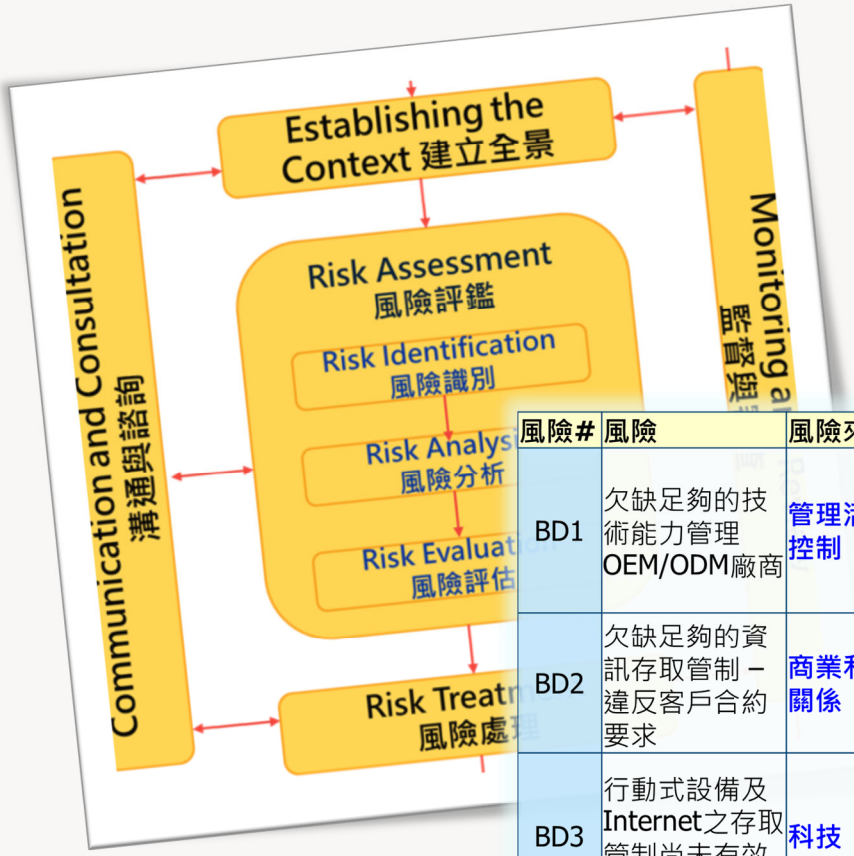


企業如何保護機敏感資料 - 補充資料

鑑別關鍵業務流程 - 從機密性、完整性、可用性及法規遵循角度

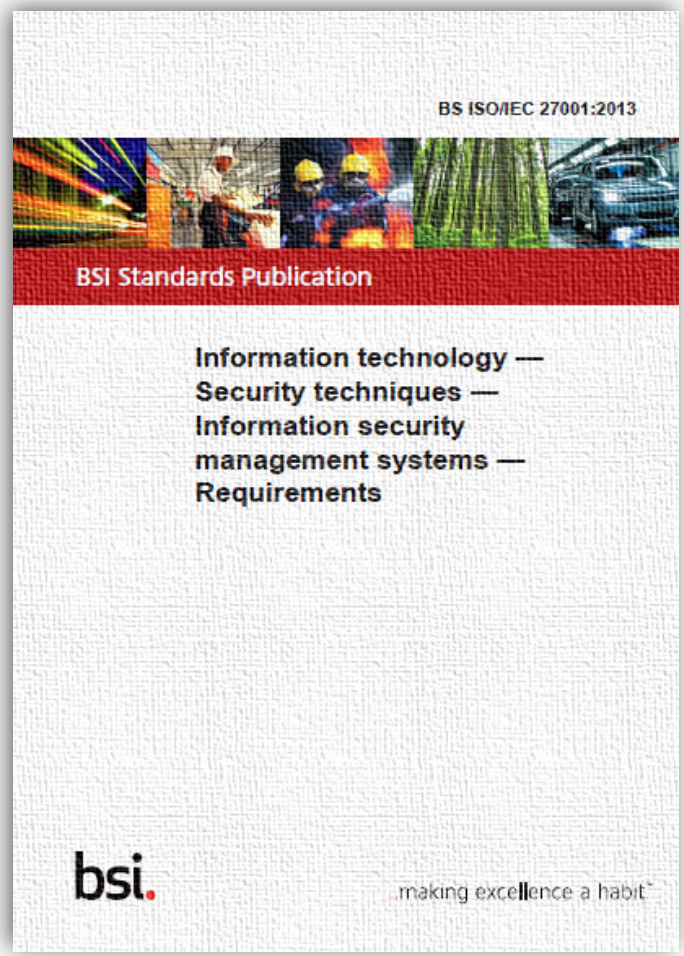


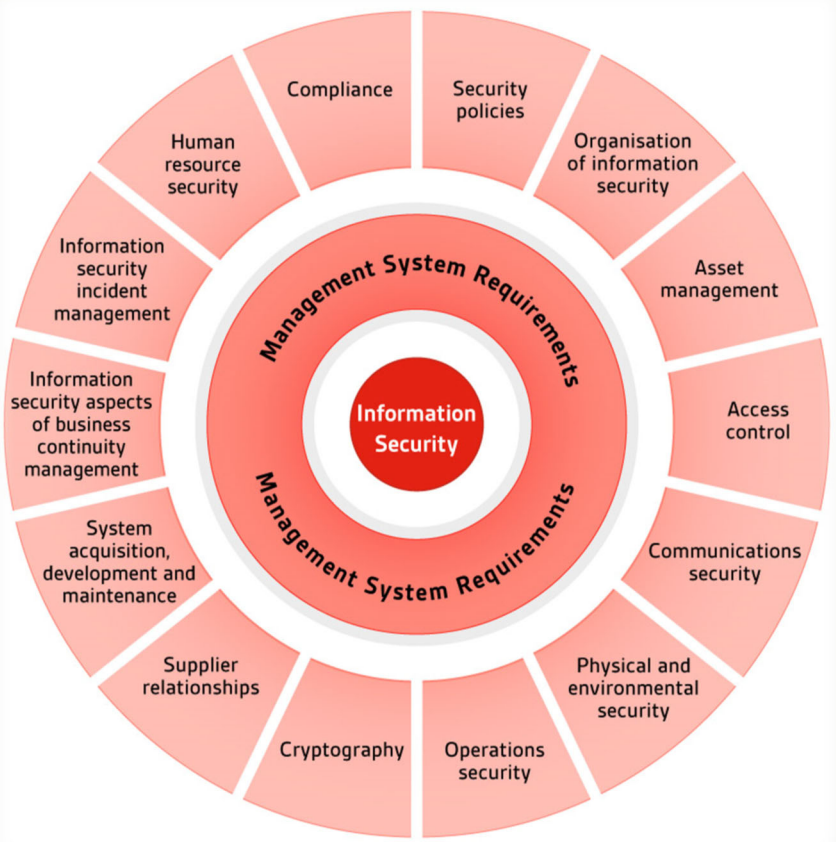
進行風險評鑑並藉別可能的風險 (ISO 31000)



風險#	風險	風險來源	風險描述	可能性	衝擊	風險值
BD1	欠缺足夠的技術能力管理OEM/ODM廠商	管理活動及控制	由於公司須提供敏感研發資料給予代工廠，目前相關之安全管控要求尚未明確規範	3	3	**9**
BD2	欠缺足夠的資訊存取管制－違反客戶合約要求	商業和法律關係	針對客戶提供的研發資料未有充足的安全防護措施.....	3	4	**12**
BD3	行動式設備及Internet之存取管制尚未有效控管	科技	目前公司僅針對行動式設備及Internet之存取制定管理規範，欠缺技術面管制	4	4	**16**

鑑別可能需要導入或強化的安控措施：參考國際標準要求





鑑別可能需要導入或強化的安控措施：策略面/ 管理面/ 技術面/ 能力及認知面

A.5.1 管理階層資訊安全方向	A.6.1 內部組織	A.6.2 行動設備與遠距工作	A.7.1 聘僱之前	A.7.2 聘僱期間	A.7.3 聘僱終止及變更	A.8.1 資產責任
A.8.2 資訊分類	A.8.3 媒體處置	A.9.1 存取控制的營運要求	A.9.2 使用者存取管理	A.9.3 使用者責任	A.9.4 應用系統存取控制	A.10.1 密碼控制措施
A.11.1 安全區域	A.11.2 設備安全	A.12.1 作業程序與責任	A.12.2 防範惡意軟體	A.12.3 備份	A.12.4 存錄與監視	A.12.5 作業軟體的控制
A.12.6 技術脆弱性管理	A.12.7 資訊系統稽核考量	A.13.1 網路安全管理	A.13.2 資訊傳輸	A.14.1 資訊系統的安全要求	A.14.2 開發與支援過程的安全	A.14.3 測試資料
A.15.1 供應商關係之資訊安全	A.15.2 供應商服務交付管理	A.16.1 資訊安全事故管理改進	A.17.1 資訊安全持續	A.17.2 備援	A.18.1 適法性之遵循性	A.18.2 資訊安全審查

鑑別可能需要導入或強化的安控措施：
策略面/ 管理面/ 技術面/ 能力及認知面 (例) - 行動設備與遠距工作

Mobile device and teleworking policy 行動設備及遠距工作政策

行動設備: 政策及支援之安控措施應被採用，以管理使用行動設備所導致之風險。

遠距工作: 政策及支援之安控措施應被實施，以保護存取、處理或儲存於遠距工作場所之資訊。

行動設備政策 (例)

- 行動設備之註冊；
- 實體保護之要求；
- 軟體安裝之限制；
- 連接資訊服務之限制；
- 存取控制；
- 遠端關閉、抹除及鎖定之機制...

允許使用私人之行動設備之管理 (例)

- 私有與營運使用裝置之區隔及在私有裝置上之營運資料之保護；
- 僅在使用者已簽署終端使用者同意認知其責任、放棄營運資料之所有權、允許組織在該裝置遺失時由遠端抹除資料等之後，才提供營運資料存取..

遠距工作政策 (例)

- 通信安全的要求，考量存取資訊之敏感性；
- 預防在私有設備的資訊處理與儲存之機制；
- 使用住家設備的其他人未經授權存取資訊或資源的威脅；
- 家中網路和無線網路組態設定的要求...

遠距工作的實作指引 (例)

- 遠距工作設備和儲存設備之提供；。
- 界定許可的工作、擁有的資訊分級、權限；
- 提供通信設備，包括保護遠端存取的方法；
- 有關家人使用設備和存取資訊的規則；
- 稽核與安全監控...

鑑別可能需要導入或強化的安控措施：
策略面/ 管理面/ 技術面/ 能力及認知面 (例) - 人力資源安全

Prior to employment 聘僱之前

- Screening 篩選
- Terms and conditions of employment
  聘僱條款與條件

During employment 聘僱期間

- Management responsibilities
  管理階層責任
- Information security awareness, education and training
  資訊安全認知教育與訓練
- Disciplinary process
  懲處過程

Termination and change of employment 聘僱終止及變更

- Termination or change of employment responsibilities
  聘僱終止或變更責任

鑑別可能需要導入或強化的安控措施：策略面/ 管理面/ 技術面/ 能力及認知面 (例) - 資訊分類、標示及處置

Classification of information
資訊分類

- **資訊應依法律要求、價值、重要性及對未經授權揭露或修改之敏感性分類。**
  - 分類方案應在**整個企業**內保持一致以便每人均會以相同方式將資訊分級、對保護要求有共同瞭解。

等級	機密性
4	極機密：涉及組織營業活動之極機密相關資料
3	機密：涉及組織營業活動之機密相關資料
2	一般：組織內部使用，需經授權許可流程方得使用
1	公開：組織對外部提供之資料

Labeling of information
資訊標示

- **應依組織所採用之資訊分類方案，發展及實作一套適切的資訊標示程序。**
  - 資訊標示的程序需要涵蓋實體與電子格式的資訊與其相關資產；
  - 標籤應易於識別。程序應對何處及如何附加標籤予以指引。

Handling of assets
資訊處置

- **應依組織所採用之資訊分類方案，發展及實作處置資產之程序。**
  - 對每一分類等級， 應界定包括保全作業、儲存、傳輸、解除機密等級與銷毀等處置程。

鑑別可能需要導入或強化的安控措施：
策略面/ 管理面/ 技術面/ 能力及認知面 (例) - 存取控制

鑑別可能需要導入或強化的安控措施：
策略面/ 管理面/ 技術面/ 能力及認知面 (例) - 實體與設備安全

Secure areas
安全區域

- Physical entry controls
  實體進入控制措施
- Securing offices, rooms and facilities
  保全辦公室、房間及設施
- Working in secure areas
  安全區域內工作

Equipment
設備安全

- Removal of assets
  資產的攜出
- Security of equipment and assets off-premises
  場所外設備及資產的安全
- Secure disposal or reuse of equipment
  設備的安全汰除或再使用
- Unattended user equipment
  無人看管的使用者設備

鑑別可能需要導入或強化的安控措施：策略面/ 管理面/ 技術面/ 能力及認知面 (例) - 系統存錄與監視

Event logging
事件存錄

- 事件日誌應記錄使用者活動、異常及資訊安全事件，應加以產生、保留及定期審查。
  - 事件日誌可包括；
    - 使用者ID；
    - 關鍵事件的日期、時間及細節，如登人與登出；
    - 設備身分或位置；
    - 存取系統的成功與被拒絕；
    - 特權的使用；
    - 存取的檔案與存取的種類；
    - 使用者在應用系統內執行之交易紀錄

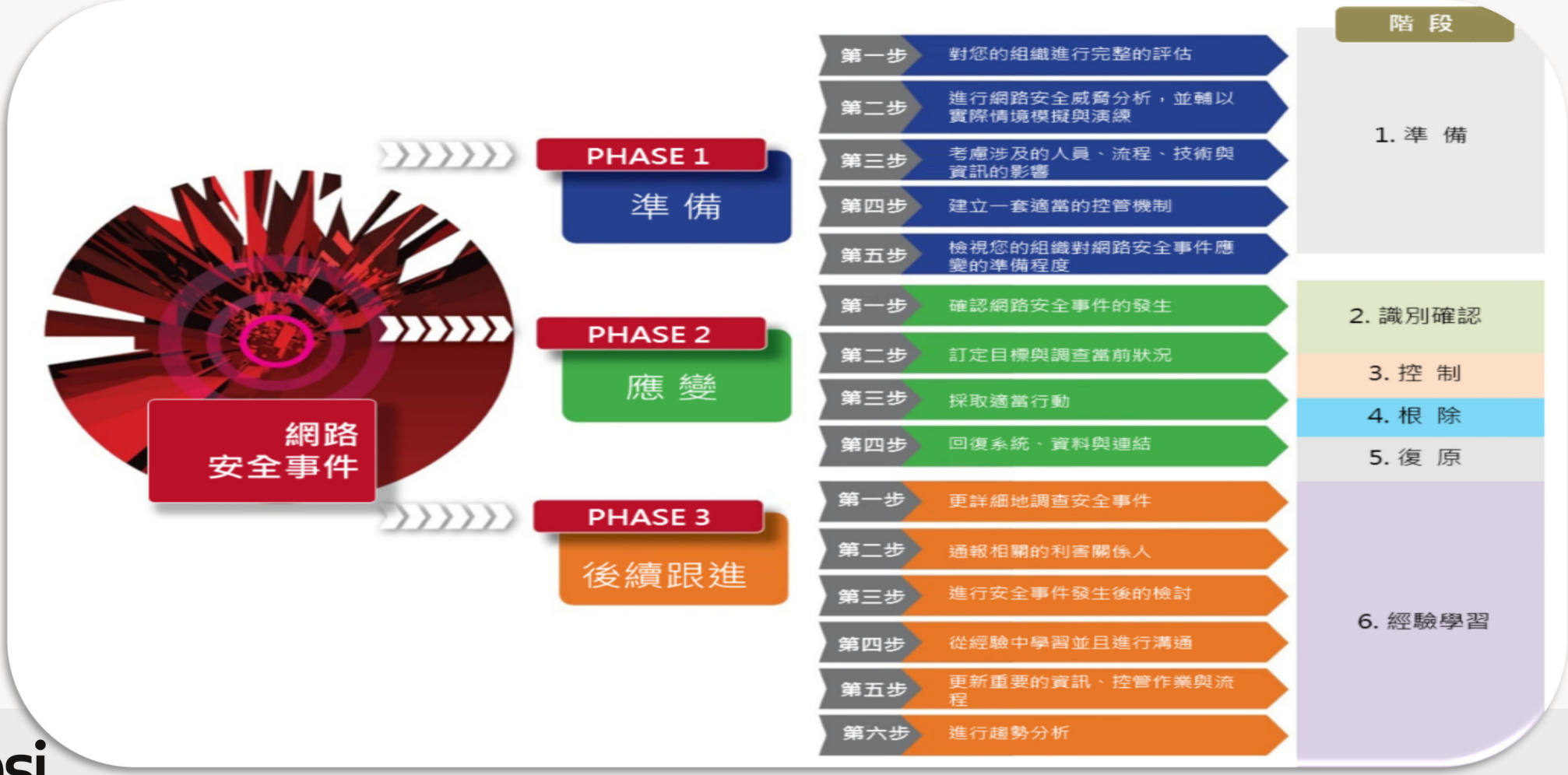
Protection of log information
日誌資訊的保護

- 應防範存錄設施及日誌資訊遭竄改及未經授權存取。
  - 系統日誌通常包含大量的資訊，為了資訊安全監視的目的而有助於識別重要的事件，應考慮將訊息自動複製到第二個日誌中，或使用適當的系統公用程式或稽核工具；
  - 即時複製日誌至系統管理者或操作者控制之外的系統可用以保全日誌。

Administrator and operator logs
管理者與操作員日誌

- 應存錄系統管理者及操作者之活動，且應保護及定期審查該日誌。
  - 授權使用者帳號持有者可能能夠操縱在其直接控制下之資訊處理設施的日誌，因此有必要保護及審查日誌以維護特權使用者之可歸責性。

鑑別可能需要導入或強化的安控措施：
策略面/ 管理面/ 技術面/ 能力及認知面 (例) – Incident Response



Thank you