簡報技巧
(基礎概念及實例分享_內部威脅)

109年7月24日

疾病管制署檢驗及疫苗研製中心

TAIWAN CDC

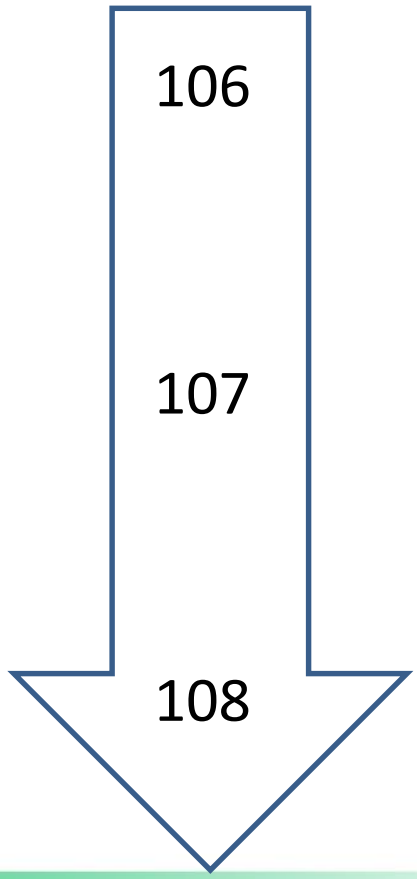
簡報大綱

- 基本概念
- 實例分享
- 結論

簡報技巧基本概念

- 使用簡單一致的設計版面(字型、顏色、背景)
- 每一版面使用含基本資訊的有限的字數
- 不要讀稿
- 不要面對簡報檔，面對觀眾，並常與觀眾互動
- 在演講期間，不要道歉；若有疑慮或容易誤解的內容，則不放入簡報
- 應使用影片或實例分享

內部威脅



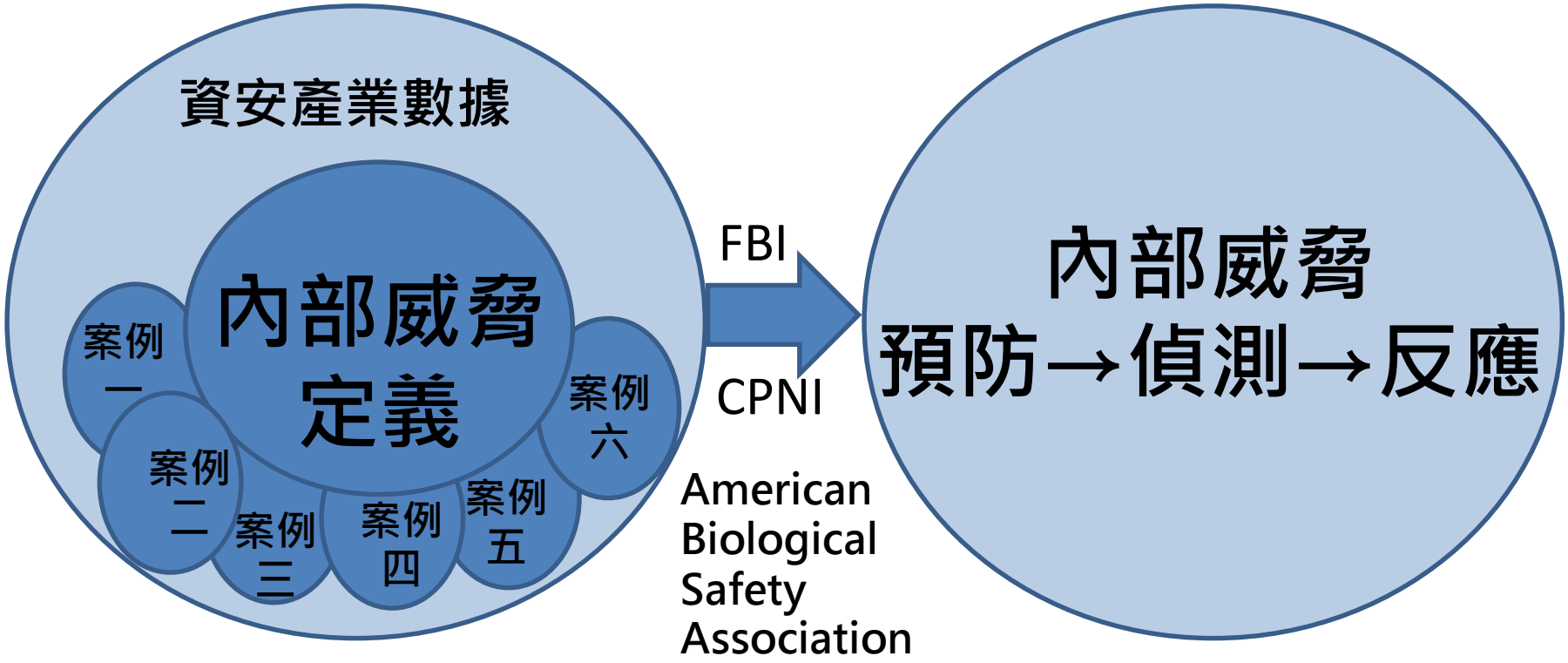
實例分享一(他山之石)

實例分享二(內部文化)

實例分享三

內部威脅談高等級實驗室規劃管理
(預醫所高治華副所長)

實例分享一　106/3/29



內部威脅案例一

腕龍、圓頂龍、翼手龍、霸王龍

Dennis Nedry was a computer programmer at Jurassic Park. Due to his financial problems and low salary, he accepted an offer from Biosyn to smuggle dinosaur embryos off the island.

內部威脅定義

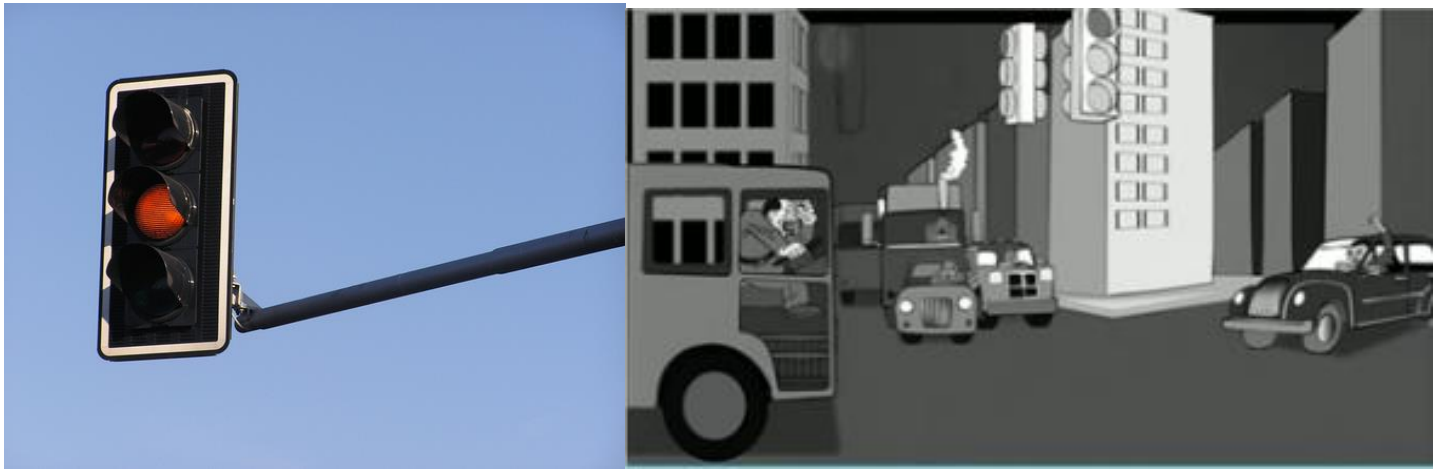
內部威脅就是由具有授權之現職或離職員工、合約廠商或業務合作夥伴惡意威脅組織安全的行為

內部威脅(包括破壞、偷竊、詐欺、間諜活動、競爭優勢)常透過濫用授權、偷竊材料及不正當操作物理設備。

An insider threat is generally defined as a current or former employee, contractor, or other business partner who has or had authorized access to an organization ‘s network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization’ s information or information systems. Insider threats, to include sabotage, theft, espionage, fraud, and competitive advantage are often carried out through abusing access rights, theft of materials, and mishandling physical devices.

Insider Threats, Definitions, Video 1 and 2

內部威脅案例二　美國城市一個案例



美國某城市-員工聯盟進行**勞工協商**

雖然預防而解除兩個僱員的系統權限，但因**督導者曾分享帳號**
進入系統後解除四個十字路口的紅綠燈號誌控制箱，並禁止任何人進行修理
四天內紅綠燈信號閃爍，自動由紅轉綠轉黃

內部威脅案例三　美國電腦網路公司一個案例

電腦網路公司的職員得到兩家主要客戶之一提供新工作
此職員下載未來公司的競爭者80份文件

內部威脅案例四　　花旗銀行一個案例

員工因績效不佳遭解雇，離職前上傳惡意程式，導致導致了花旗銀行在北美地區約90%的網絡癱瘓，
由於未授權入侵企業計算機，他被判處了21個月監禁及支付77,200美元的賠償。

內部威脅案例五　　政府機構一個案例

一個外國政府機關的職員，利用職權在妻子出國時將其放入國家恐怖分子的名單。
她上訴了三年，無人理會，直至她丈夫高升，他的上級進行背景檢查發現他的太太是恐怖分子，這時才發現他太太的申訴。

內部威脅案例六

廖姓工程師對公司極為不滿，以惡意程式破壞停車柱控制器致全台YouBike大當機，中檢今天以涉嫌妨害電腦使用罪將他起訴。記者白錫鏗 / 攝影

廖男（27歲）是微程式公司工服部的系統工程師，因不願於夜間輪班，對公司不滿，遂利用台中市及彰化縣You Bike車柱控制器韌體「正式更新」的機會，植入他撰寫的惡意自動排程程式及他變更的不正確檔案至主機。

致使台北市、新北市、桃園市、新竹市、台中市、彰化縣全部的YouBike車主控制器均當機，造成微笑單車公司1612萬8338元的財產損失以及630萬4413元的商譽損失。

廖姓工程師否認妨害電腦使用的犯行，**檢察官依據**

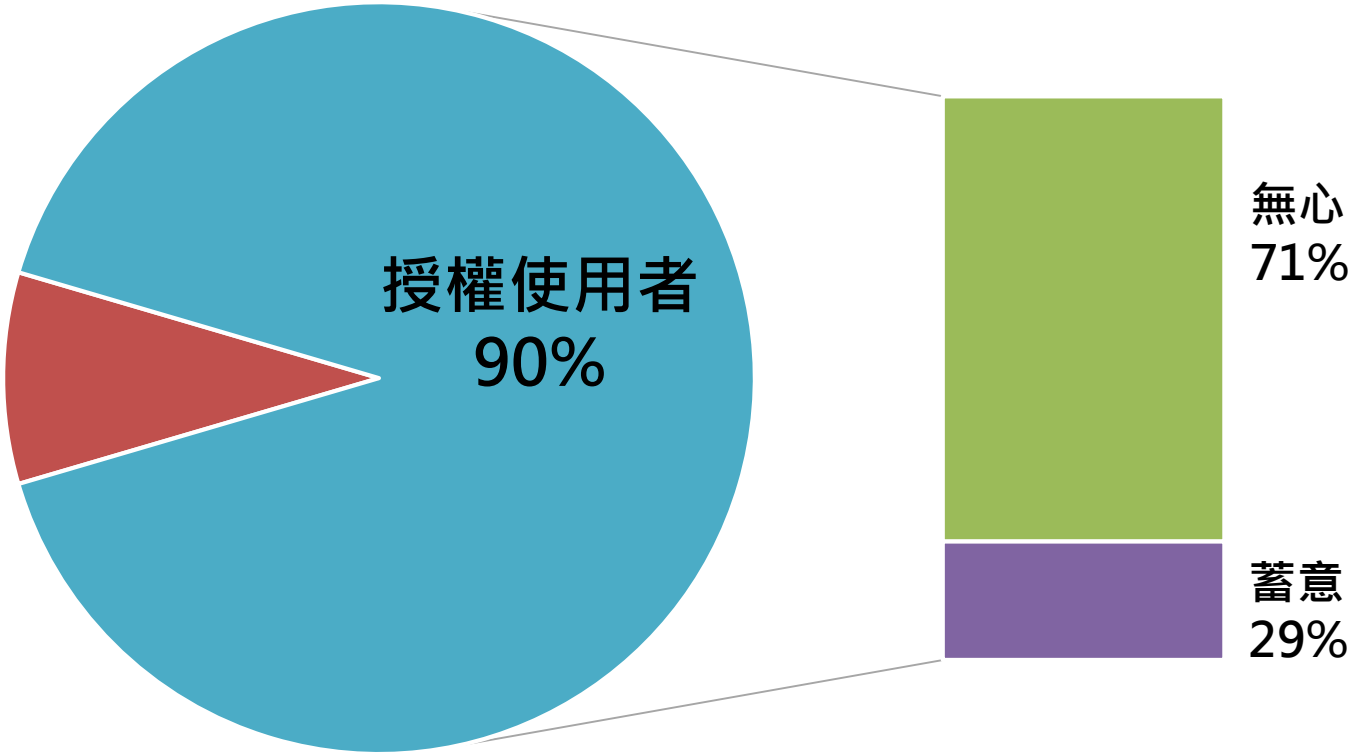
- 廖與同事的通訊軟體對話曾表示「我每天被老闆幹，還是繼續做下去」、「害我上次的加班費都被砍」、「我希望出包，上面的才有警覺」，顯示他對公司極為不滿。
- 廖嫌於去年9月6日，因陳姓證人發現有人惡意刪除「Linux跳板主機」之Log紀錄前，竟上網查詢「如何從bash history中刪除一筆指令」、「完全刪除bash history」、「如何知曉誰刪除檔案」等。
- 甚至9月7日，警方至微程式公司欲調取所有的主機Log紀錄「後」，又上網查詢「如何使用foremost復原資料」、「復原虛擬主機」、「是否可刪除或覆寫shell script」等，足證廖男是本件妨害電腦使用的人。

內部威脅已成為資安產業的重要議題

- 內部威脅已被定位為5大資安專業領域與常見案例
- 每3個資安事件，就有2個是被授權接觸內部資料之行為所造成的

Gartner「2015年使用者與企業單位行為分析市場指南 (UEBA；User and Entity Behavior Analytics)」

• Verizon 2015資料外洩調查報告

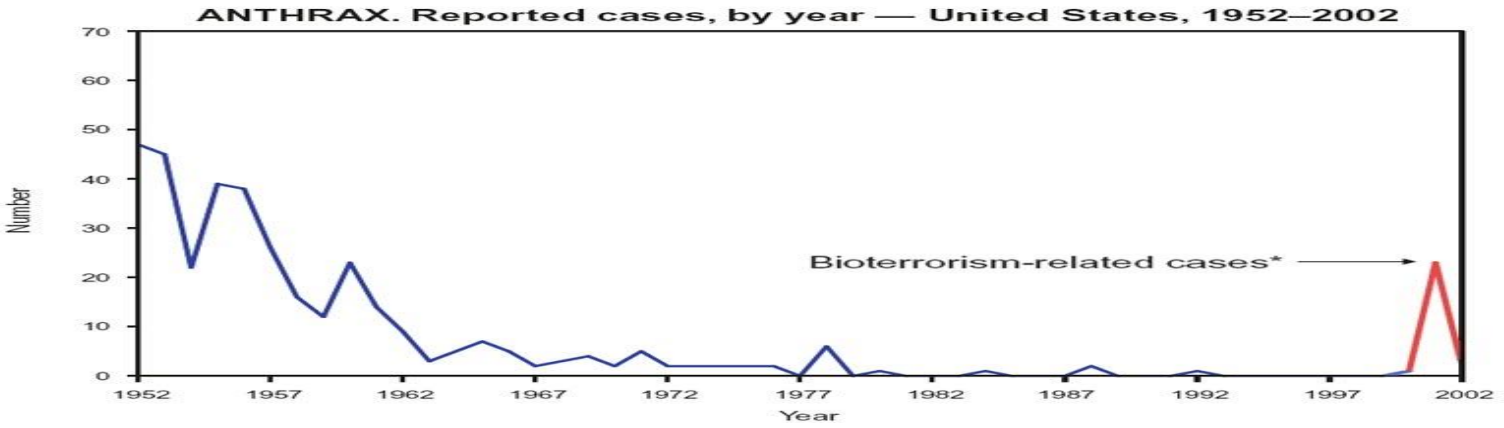


日常工作中應用程式的使用及使用者不經意的操作行為，已成為全球資安團隊嚴苛的資安潛在風險與挑戰

CERT Insider Threat Report
75%的內部威脅是無法預警的，而且一旦造成資安事件，所造成的財損與破壞程度是外部威脅的2倍。

實驗室內部威脅是真的嗎？

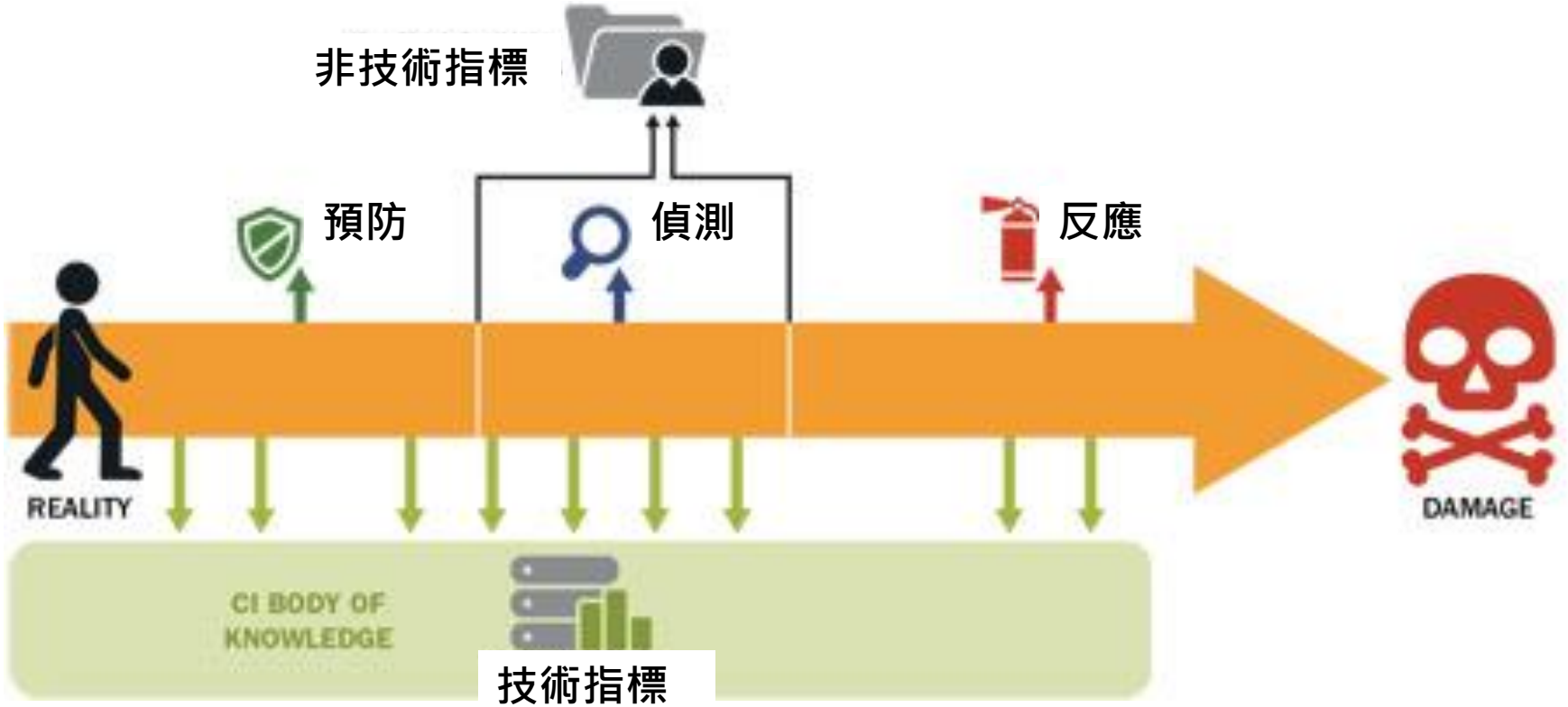
- 我們實驗室從來沒有生物材料相關案例發生
- 我不做管制性病原與毒素，所以有人偷竊或濫用生物材料/技術的可能性極低
- 每個在這裡工作的人都經過審查，因此適合在這裡工作
- 我們的實驗室在招聘員工時，有一個優良的適合性過程，所以每個人永遠是一個好人
- 如果有人要做壞事，我們會知道，有人會報告



* One epizootic-associated cutaneous case was reported in 2001 from Texas.

Two cases of cutaneous anthrax were reported to CDC in 2002. One case occurred in a laboratorian who had been processing environmental samples for *Bacillus anthracis* in support of investigations of the bioterrorist attacks in the United States during fall 2001. The other was a naturally occurring case in a veterinarian who was performing a necropsy of a cow.

CDC



技術指標

內部威脅人員的風險特徵

個性內向	盡量降低自己的錯誤
貪婪/財務需要	無法承擔責任
勒索妥協性高	無法接受批評
強迫和破壞行為	自我感知價值超過表現
叛逆/被動攻擊	缺乏同理心
倫理彈性高	執法傾向
忠誠度不高	容易挫敗/失望
坐享其成 - 自戀	管理危機無效的經驗

具有這些特徵的個人可能達到對組織進行惡意活動的點。 最好的預防措施之一是培訓員工識別和報告同行或業務合作夥伴展示的行為指標。

人員保全

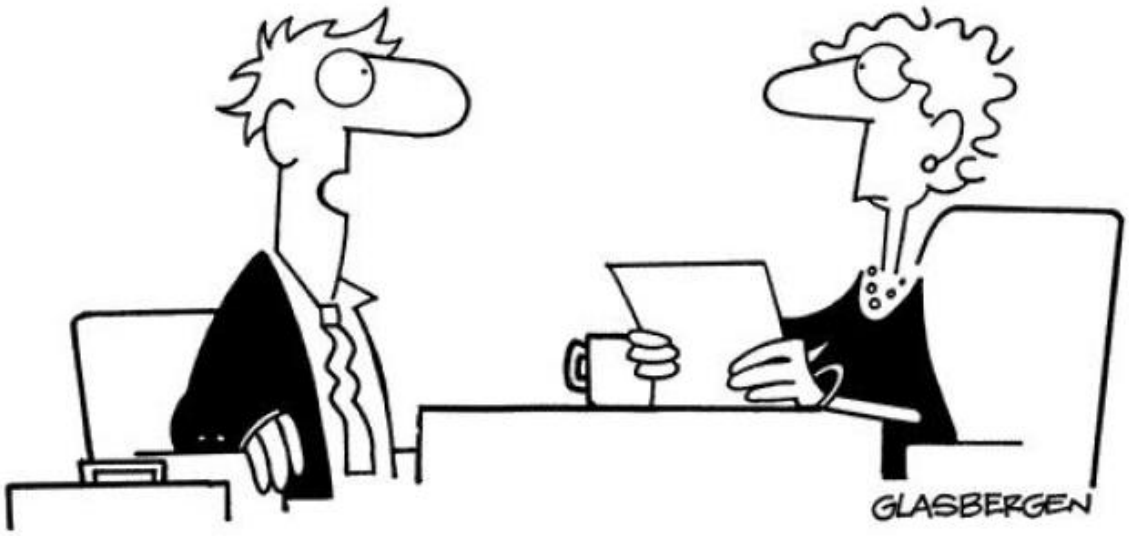
個人保全計劃授權員工保護自己承擔責任，了解他們可能遇到的潛在威脅性質

- 職前適合性 - 建立行為基線
- 員工可靠性 - 持續評估以確定個人是否偏離其行為基線
- 培訓 - 知是遵守的先決條件
- 個人保全 - 通過業務安全、資訊安全和威脅意識等領域進行教育訓練，保護個人免於在不知不覺成為內部威脅的從犯

Collectively works to identify, monitor, and counter inside threats

職前適用性

- **FBI安全風險評估**
  - 不是“背景調查”
  - 不確定員工是否適合接觸管制性病原及毒素
- **申請人/員工資訊**
  - 犯罪史
  - Home address history
  - 工作經歷
  - 聯繫方式(專業/同儕)
  - 簽證
- **記錄文件**
  - 犯罪記錄
  - 民事命令
  - 開車記錄
  - 教育記錄
  - 專業許可/認證
- **訪談**
  - 申請人/僱員
  - 專業和同行參考（尋求次要聯繫）
  - 採用戰術面試程序（例如結構化，開放式問題）
  - 居留身份



“What do you mean, it’s not a good résumé?
It’s the most expensive one they had on eBay!”

員工可靠性法規

- 42CFR73.11(f)(3)

保全計畫必須敘述評估接觸管制性病原及毒素員工的可靠性步驟：

✓ 自我或同儕失竊、損失或釋出意外事件通報

✓ 員工教育訓練

✓ 員工適合性持續監控

可疑行為案例

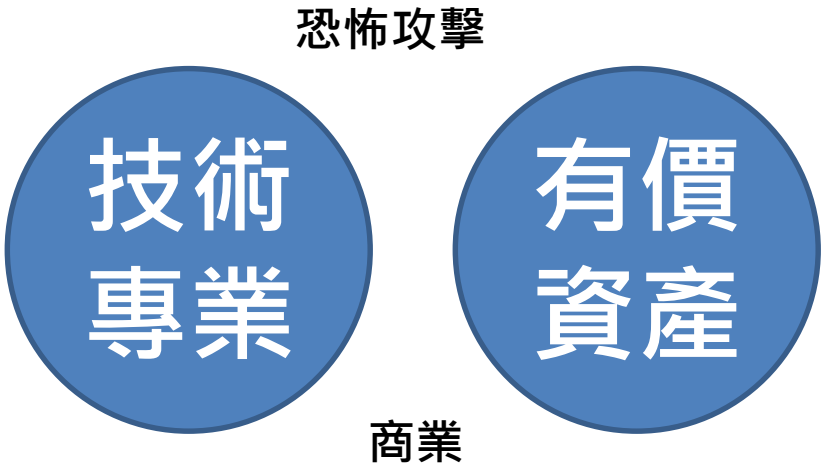
- 發送不適當的電子郵件、郵件或書面/口頭文字
- 不公正的憤怒/侵略
- 對同事的不當行為/破壞同事的研究
- 身體暴力（對物或人）
- 不明原因缺席
- 欺騙
- 實驗室工作不合乎規範
- 沒有正當理由加班
- 不必要地影印資料，特別是有專屬及機密文件
- 對非業務相關事項感興趣
- 瀏覽電子郵件密碼，竊取實驗室筆記本或試劑
- 暴力或有自殺傾向
- 造假報告
- 非法攜帶武器
- 殘酷對動物
- 盯梢，強迫關係
- 外觀上的顯著變化
- 重大工作/生活改變(例如獲得意外財富，異常的外國旅行)
- 吸毒/酒精/藥物濫用/賭博
- 過分專注於申訴

通報失敗

- 訓練不足 - 不知道哪些行為嚴重需報告; 不明白通報價值。
- 糟糕的領導 - 害怕報復或缺乏對組織和政策的信心。
- 擴散的責任 – 期望他人報告。
- 對可疑行為變得不敏感

內部威脅風險評估
Insider Risk Assessment

- 可能面臨的威脅及其發生機率



風險評估原則

- 鑑別實驗室重要資產
- 鑑別威脅 (based on the intent and capability of those who could carry out the threat)
- 評估威脅發生機率
- 評估威脅發生衝擊層面及範圍
- 審查現有防制措施
- 預防保全風險計畫

降低內部風險

- 降低招募有威脅風險存在的員工
- 限縮現有員工的保全風險
- 降低保護資產內部活動的風險
- 依據風險實施保全預防措施

職前篩選
Pre-Employment Screening

- ✓阻止雇用可能希望損害組織的申請人
- ✓偵測有意在招聘/申請階段傷害組織的個人
- ✓拒絕雇用打算損害組織的個人或不適合的申請人

員工持續保全
Ongoing Personnel Security

- CPNI的內部數據
  - ✓ 超過75%的員工忠誠度在就職後發生了變化
- 風險行為
  - ✓ 洩漏資訊
  - ✓ 破壞流程 process corruption
  - ✓ 竊取資訊
  - ✓ 偷竊
- 動機
  - ✓ 錢 financial gain
  - ✓ 報復 revenge
  - ✓ 惡名 notoriety
  - ✓ 政治或宗教理想 political or religious ideology
  - ✓ 恐懼或壓迫 fear or coercion

管理指導方針

- ✓保全文化 security culture
- ✓直接管理 line management
- ✓接觸管制 access controls
- ✓安全合約 secure contracting
- ✓社會工程 social engineering
- ✓社交網及網路篩選 social networks and the use of the internet screening for the insider threat
- ✓可疑行為通報 reporting concerns
- ✓保護監控 protective monitoring
- ✓調查 investigations
- ✓退出程序 exit procedures

保全文化和行為改變
Security Culture and Behaviour Change

- 組織中良好的保全文化是保全制度的重要部分
- 保全文化是一組價值觀，由組織成員共享
- 有效的保全文化的好處包括：
  - ✓員工參與並承擔保全問題的責任
  - ✓遵守保全措施的意願增加
  - ✓通過鼓勵員工以保全模式思考和行動，降低保全事件發生風險
  - ✓員工通報保全相關行為/活動意願增加

FBI如何抵禦內部安全威脅

- FBI內部人員Robert Hansen於1979到2001年之間為蘇聯竊取內部情報事件，引發的保全問題
- 前FBI情報分析師Leandro Aragoncillo亦於2007年被指揮犯有間諜罪，其被懷疑曾向菲律賓方面傳遞敏感信息

✓FBI CISO Arlette Hart：流程、文化與員工信任正是抵禦內部威脅的最有效手段

FBI解決內部威脅的幾種可行手段

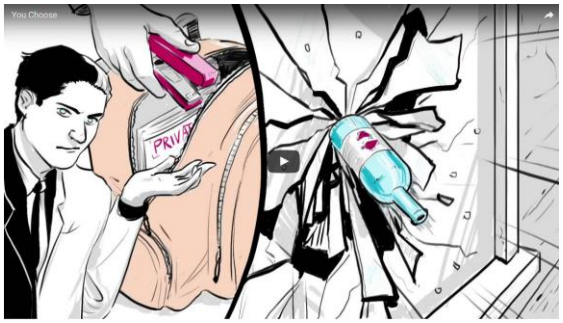
- ✓ **採取眾包方案**：允許員工以實名通報各類疑似內部威脅的事件
- ✓ **內部調查重點放在資訊保護層面**：是一項關鍵而強大的能力，必須謹慎處理
- ✓ **控制整體環境**： 不允許員工自帶設備辦公，而且在員工許可的情況下，進行監測與嚴格控制。
- ✓ 阻止內部威脅的關鍵在於搶在事件發生之前迅速採取行動。舉例來說，我們有權針對已經決定離職的員工查看其訪問活動以及數據移動流程。

1. Your company needs you

2. People, people, people

3. Fly in the ointment

4. You Choose



5. Risky business

6. One small step

結論

- **威脅是人**
  - ✓保全的焦點是人 – 員工的保全
- **暴力是一個過程**
  - ✓威脅呈現在行為指標，可當作威脅評估的數據
- **聰明的內部監護人 – 最寶貴的工具、同儕和自我通報**
  - ✓無法通報
  - ✓虛報
  - ✓報復

  } 必須受到保護
- **員工保全 - 是一個很複雜的監測平台**，進行行為監測、指標偵測及威脅案例轉交給威脅評估小組

實例分享二

內部威脅
(Insider threat)

107年12月12日下午15:00-15:15

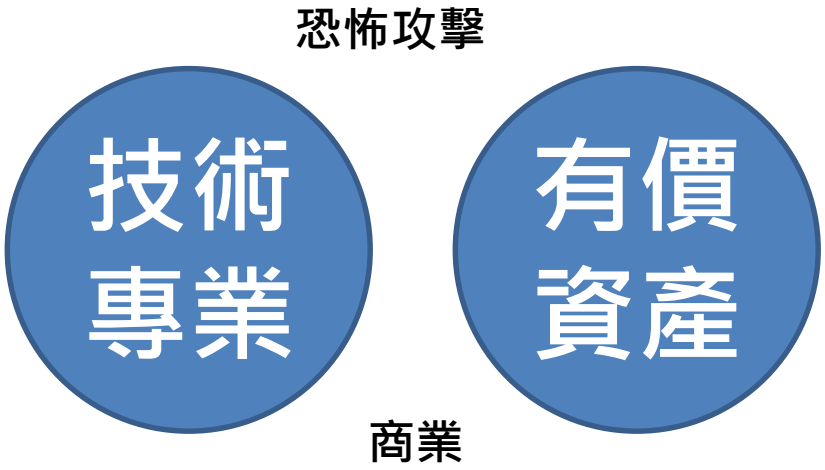
內部威脅定義

內部威脅就是由具有授權之現職或離職員工、合約廠商或業務合作夥伴惡意威脅組織安全的行為

行為包括破壞、偷竊、詐欺、間諜活動或競爭優勢，例如透過濫用授權、偷竊有價材料(特別是管制性病原及毒素)及不正當操作物理設備

內部威脅風險評估
Insider Risk Assessment

- 可能面臨的威脅及其發生機率



適任性評估

透過**觀察、自我通報及同儕通報**，監視個人行為，確保個人適合繼續具有資格。

- 書面
- 口試
- 筆試
- 現場觀察
- 訪談

附件 7.6

管制性病原取得人員評估紀錄表

員工姓名：_____ （員工代碼：_____）

操作管制性病原：_____（自　年　月起擔任此職務共　年　月）

評估日期：　年　月　日

評估時機：□就職前適合性評估* □持續性評估**

評估方式：□書面 □口試 □筆試 □現場觀察 □訪談相關人員

結果紀錄：

評估方式簡述	評估結果（得分**和評語）
書面：(相關書面文件如附) □學歷 □工作經驗 □警察刑事紀錄證明 □違反管制性病原管理法規犯罪紀錄 □其他 **口試：** □生活起居□心理狀況了解 □人員知能評核 **筆試**(□人員知能評核)：（試卷如附） **現場觀察：** **訪談相關人員：**	

*就職前適合性評估，需至 e 等公務園學習網通過所需訓練時數及 LIMS 系統人員知能評核考試，並檢附警察刑事紀錄證明(俗稱良民證)。請上警政 e 網通申請或親至當地警察局外事科申請，需檢附申請書、國民身分證正本及影本各 1 份。每份 100 元，2.5 個工作天。

**持續性評估需含人員知能評核(口試或筆試)。

***得分以 100 分為滿分；80 以上及格；70-79 再評估；70 以下不適合該職務。

其它紀錄：

□管制性病原 15 主題 18 小時訓練。

總評：□適任現職：預定下次評估日期：　年　月　日（三年一次）

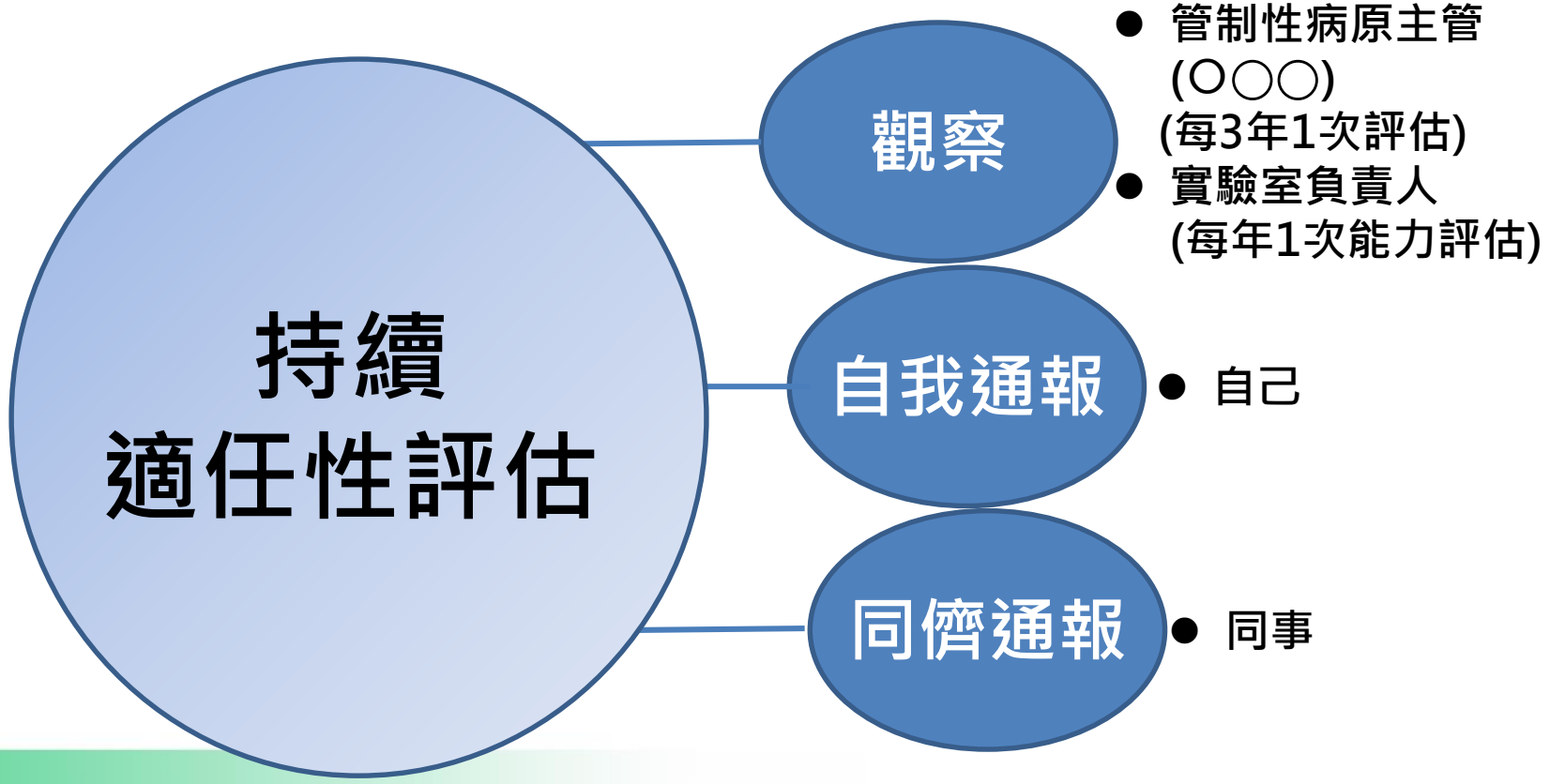
□再評估：預定下次評估日期　：　年　月　日

□不適任現職

管制性病原主管：　　實驗室主管：

RDC-QR-1501-05

內部威脅 人人有責



- 發送不適當的電子郵件、郵件或書面/口頭文字
- 不明原因缺席
- 實驗室工作不合乎規範
- 沒有正當理由加班
- 不必要地影印資料，特別是有專屬及機密文件
- 對非業務相關事項感興趣

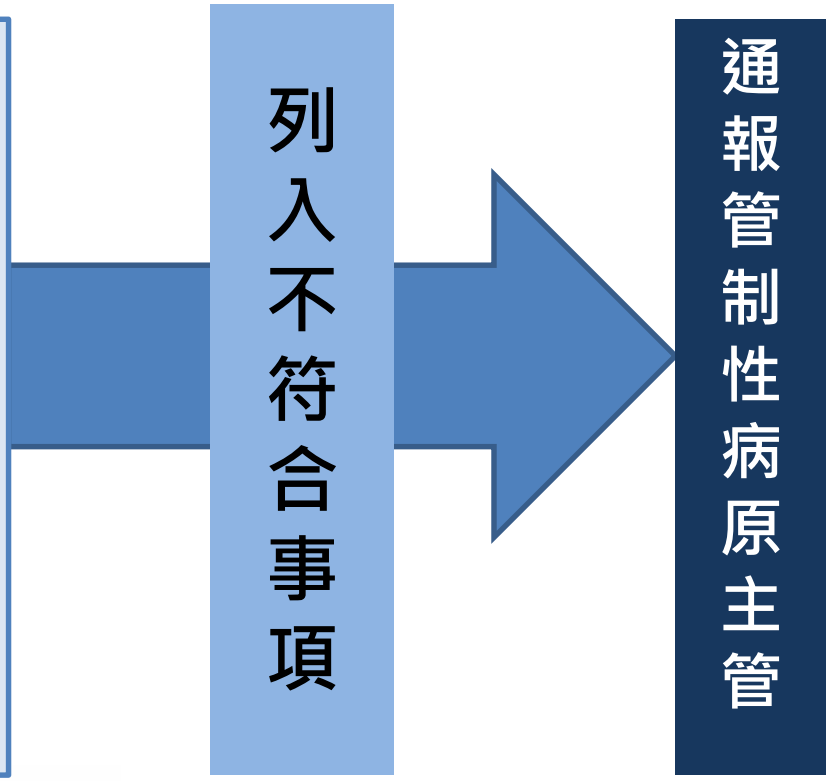
- 不公正的憤怒/侵略
- 對同事的不當行為/破壞同事的研究
- 身體暴力（對物或人）
- 欺騙

- 暴力或有自殺傾向
- 造假報告
- 非法攜帶武器
- 吸毒/酒精/藥物濫用/賭博
- 殘酷對動物

- 瀏覽電子郵件密碼，竊取實驗室筆記本或試劑
- 盯梢，強迫關係
- 外觀上的顯著變化
- 重大工作/生活改變(獲得意外財富，異常的外國旅行)
- 過分專注於申訴

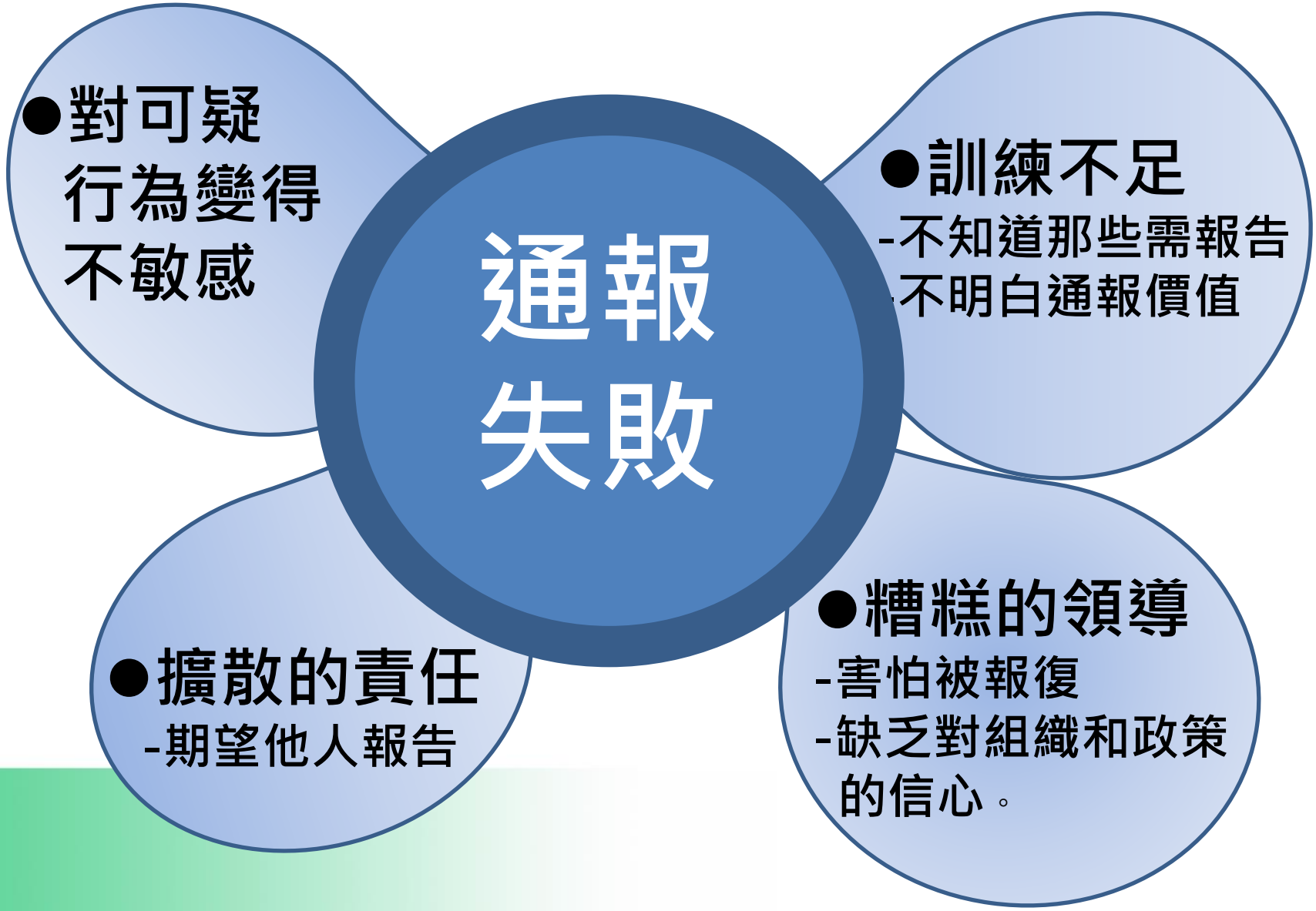
管制性病原異常事件通報

- 鑰匙、密碼、門禁卡等之遺失或損害
- 可疑人物或活動
- 管制性病原之遺失或遭竊
- 管制性病原之釋出
- 管制性病原之庫存或使用紀錄遭竄改或損毀



管制性病原異常事件通報前提

- 依規定配戴職員證
- 不隨便幫人開門
- 進門不隨便夾帶他人
- 管制性病原確實記錄
- 管制性病原相關保密


通報失敗
●對可疑行為變得不敏感
●訓練不足
-不知道那些需報告
-不明白通報價值
●擴散的責任
-期望他人報告
●糟糕的領導
-害怕被報復
-缺乏對組織和政策的信心。

結論

- 內部威脅是人
- 建立內部保全文化
- 建立預防及偵測機制

謝謝大家的聆聽
歡迎討論