CYBERSEC 2024 臺灣資安大會 | 5/14 Tue – 5/16 Thu 臺北南港展覽二館

Generative Future

FINSEC Forum

金融資安事件應變的資安長心態權衡：韌性治理或鑑識證據

高大宇 博士

永豐銀行 副總經理

Dayu Kao Dr.

Vice President

產官學
理論與實務

大綱

1.當前資安挑戰和事件應變的應用場景

2.如何增強資安事件的韌性治理

3.如何實踐資安事件應變的鑑識證據要求

4.企業實踐資安事件應變的機遇、案例分享及因應策略

5.結語

1.當前資安挑戰和事件應變的應用場景(趨勢)

擴充邊界：快速聯防降損

2023/10/7 以哈衝突(一連串的近程火箭彈突襲)
2024/05/05 黎巴嫩向以色列發射近程火箭彈

現況	彈海突襲濫殺	天堂淪為地獄	事前保密到家
問題	萬箭齊發/鐵束(穹)難擋	邊境失守/橫向移動	憂患意識/死於安逸
攻擊	走私材料自製 火箭飽和攻擊	發揮絕佳創意 如入無人之境	嚴重情報失靈 自我感覺良好
資安防禦	供應鏈管理 縮短決策時間 DDOS演練防禦	分析調查異常 修補弱點破口 ZTA零信任架構	持續檢測監控 暗網情資蒐集 OSINT整合分析

Iron Dome/Beam
Anti-missile System

After Airstrike

來源： https://udn.com/news/story/123777/7944177
https://abcnews.go.com/International/timeline-surprise-rocket-attack-hamas-israel/story?id=103816006

韌性治理的網路安全框架(CSF)與網路防禦矩陣(CDM)

Generative Future

金融資安事件應變以法遵為本，紀錄是滿足法律要求所必需的

Devices

App

Net

Data

Users

識別 (Identify)

- 資產管理
- 營運環境
- 治理策略
- 風險評估
- 風險管理
- 供應鏈管理

防禦 (Protect)

- 存取控制
- 資安意識教育訓練
- 資料安全
- 保護程序
- 維運管理
- 防護技術

偵測 (Detect)

- 異常事件
- 持續監控
- 偵測流程

應變 (Respond)

- 應變計畫
- 紀錄保存
- 事件分析
- 事件釐清
- 緩解風險

復原 (Recover)

- 復原計畫
- 溝通改善
- 經驗回饋

Tech ML+AI

People KSA

ISMS + PIMS Process BCM + Resilience Management

2.如何增強資安事件的韌性治理(現況)

公司治理與資安維運覆核

Generative Future

公司治理
Cooperate Governance

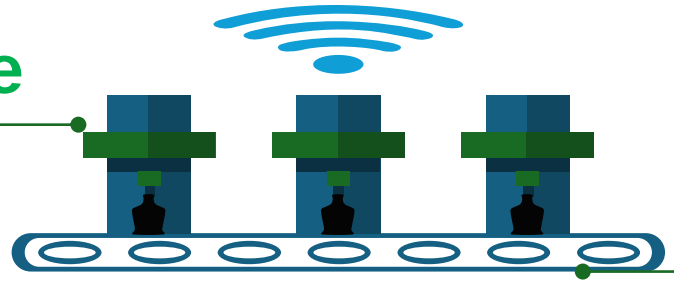
Diversity, Equity and Inclusion (DEI)
Corporate Sustainability Report (CSR)
Sustainable Development Goals (SDGs)
Environmental, Social and Governance (ESG)

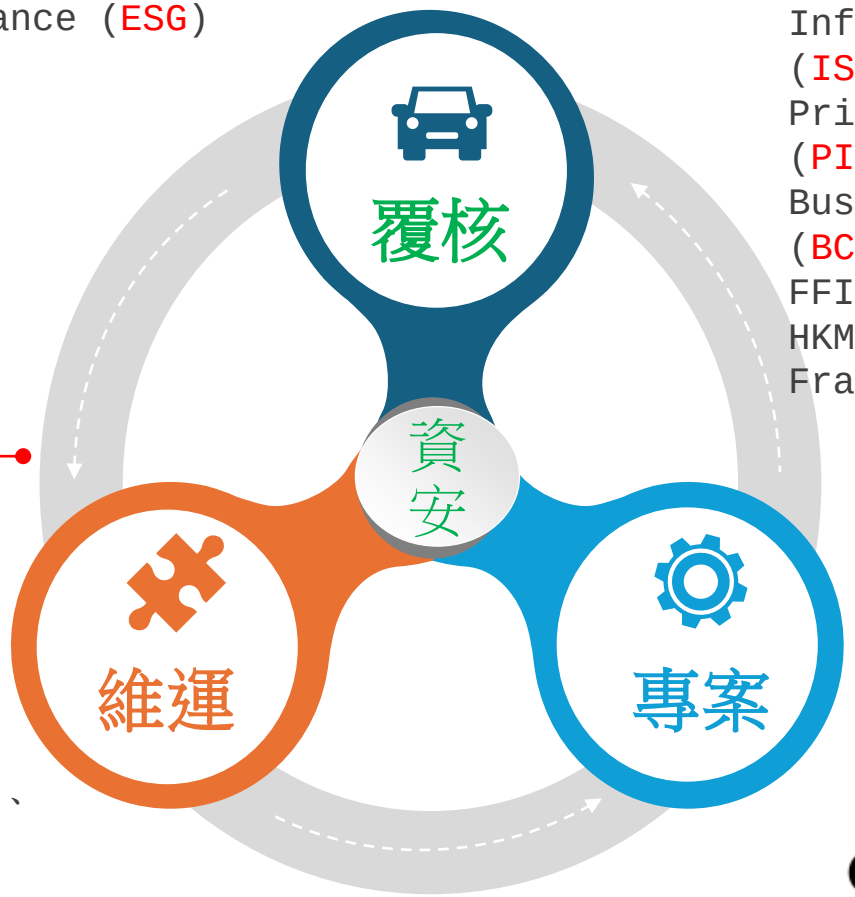
指導

監督

IT Operation

FW、WAF、IPS、Antivirus、Proxy、Security Operations Center (SOC)、Security Incident and Event Management (SIEM)
Vulnerability Assessment/Penetration Testing (VA/PT) 、Red Team (RT)、Breach and Attack Simulation (BAS)、External Attack Surface Management (EASM)





IT Governance

Information Security Management System (ISMS)
Privacy Information Management System (PIMS)
Business Continuity Management System (BCMS)
FFIEC Cybersecurity Assessment Tool (CAT)
HKMA Cyber Resilience Assessment Framework (C-RAF)

IT Project

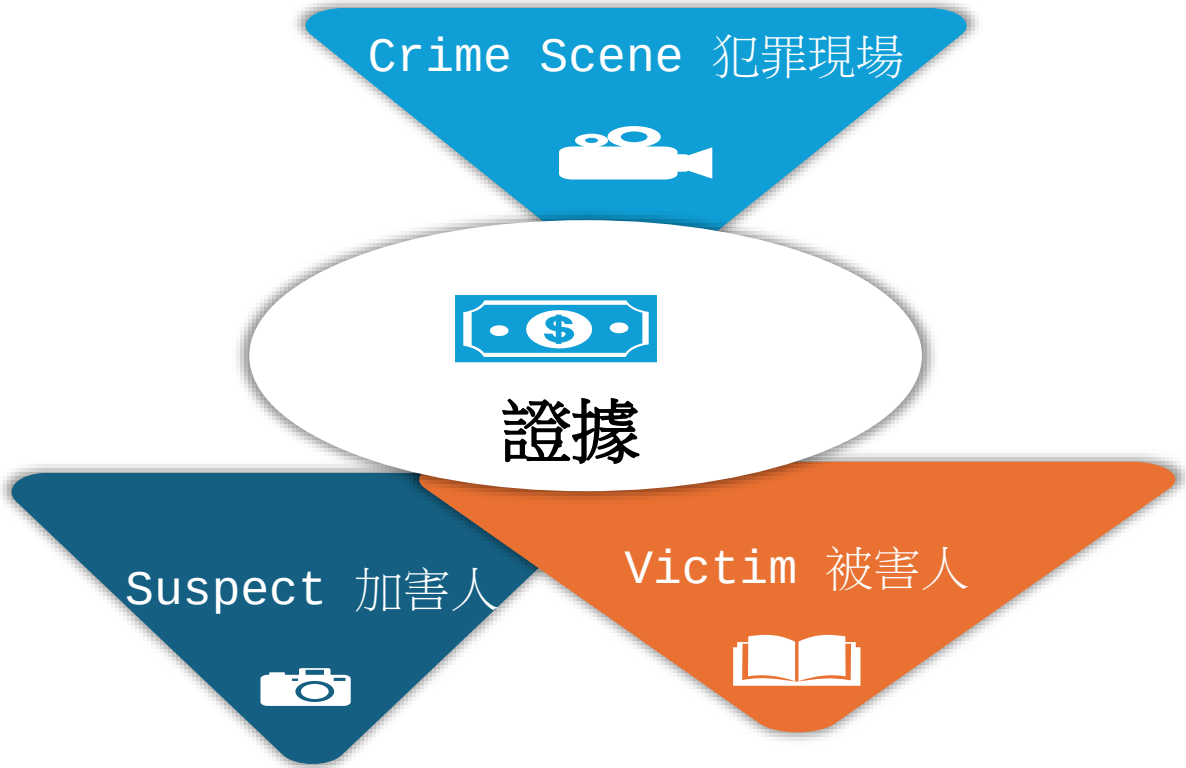
Artificial Intelligence (AI)、AR/VR、 Block Chain 、Cloud computing、Cybersecurity、big Data、IOE/IOT、FinTech、5G/6G

3.如何實踐資安事件應變的鑑識證據要求(詰問)

認可的證據

Generative Future

路卡交換原理 (Locard's Exchange Principle)



Every contact leaves a trace.

兩物接觸，必有微量證物相互交換

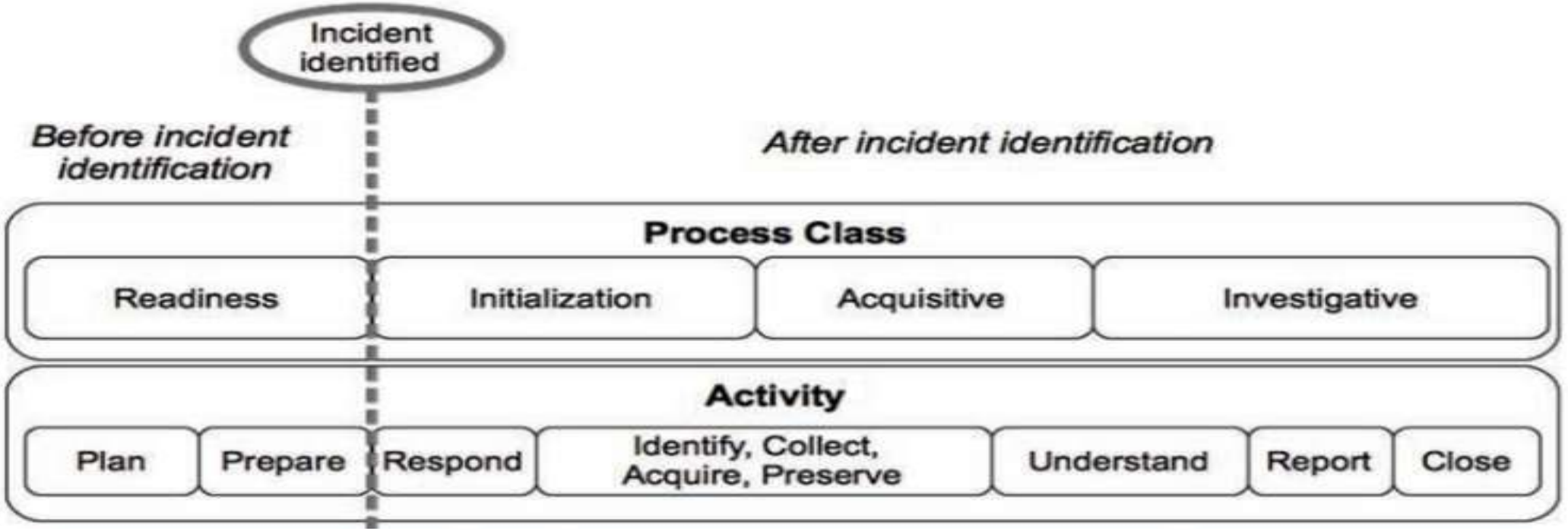
追查嫌犯稽核紀錄四要件

編號	要件	理由	目標
1	來源網址 (IP addresses)	追查來源電腦帳號或電話號碼	鎖定涉案嫌犯的犯罪行為
2	時間戳記 (timestamp)		
3	數位動作 (digital action)	檢查犯罪構成要件的該當或合致	
4	系統訊息 (system response)		

ISO/IEC 27043:2015資安事件調查原則與程序

Generative Future

階段程序



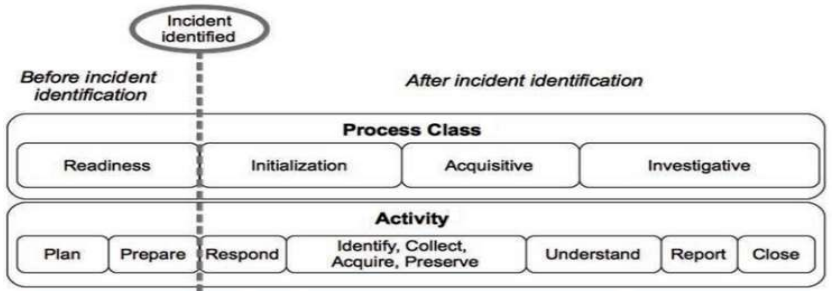
活動

同時進行程序

1.獲取授權(Obtaining Authorization)
2.資料文件化(Documentation)
3.管理資訊流(Managing Information Flow)
4.維持證物監管鏈(Preserving Chain-of-custody)
5.保存數位證據(Preserving Digital Evidence)
6.與實體調查相互參考(Interaction with Physical Investigation)

數位鑑識程序與分析：資安事件的應變程序

不同面向的思考



Information Security (NIST CSF)

Digital Forensics (ISO/IEC 27043:2015)

1 Plan

2 Prepare

Digital forensic toolkits

Incident Response (Resilient Governance)

- Experience Feedback
- Information Sharing

Law Enforcement (Forensic Evidence)

- Support
- Refuse the accused

4 Identify 1

Protect 2

Detect 3

3 Respond 4

Recover 5

10 Close

5 Collect

6 Acquire

7 Preserve

8 Understand

9 Report

Chain of Custody and Evidence Integrity

4.企業實踐資安事件應變的機遇、案例分享及因應策略(未來)

個資外洩：歷史資料的甜蜜負擔

販售個資之暗網檸檬市場

賣家：知桃子或檸檬

- 加工處理：轉賣歷史資料、資料切割(欄位少)、整併內容(來源多)
- 格式不一：全(半)形、數字、空白、缺誤

買家：無法區分品質高低 只願支付固定價格

個資外洩之真假議題

民眾求償

- ◆ 企業須證明盡善良管理人注意義務
- ✓ 恐受詐欺團體不法利用
- ✓ 難證詐騙損失與外洩個資的因果關係

檢警調查

- ◆ 人員約談筆錄的錄音、錄影(電腦稽核/系統)
- ✓ 調閱系統(查詢紀錄、需求處理流程)
- ✓ 內外部查核(含完整備份、有效查核)
- ✓ 品質數量(獨特、完整)

潛在後果

- ◆ 媒體曝光、要求採訪，處理不當導致
- ✓ 罰款
- ✓ 財務股價損失
- ✓ 損害聲譽
- ✓ 其他後遺症

最壞的打算：法庭交互詰問演練

犯罪

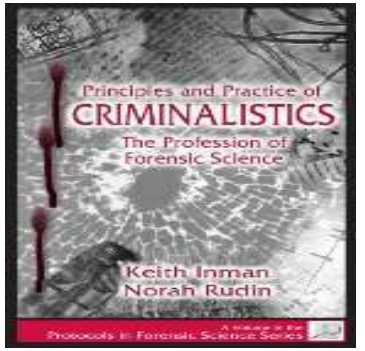
現場　證據

嫌犯/被告　被害者

四面向理論
(證物)

Inman-Rudin Paradigm

2000



6W1H(人事時地物、原因、手法)

路卡交換原理
(觸物留痕)

Divisible Matter

(Matter) Transfer

Transfer (traits)

1 識別

2 類化

Identification

Classification

Individualization

Recognition

evidence collection

APPEARANCE

COMPOSITION

3 個化

SOURCE

CONTACT

EVENT

Association

Reconstruction

Eoghan Casey
犯罪分析

4 關聯

5 重建

CRIME

可分割性　轉移性

證據的產生　鑑識科學的實作

Generation of Evidence

Practice of Forensic Science

The origin of evidence, https://jihwan4862.tistory.com/47

5.結語

人生差別：做好/做完

Generative Future

用心做好

- 溝通滿意結果
- 舉一反三解決
- 思考真正做好
- 100%付出努力

Just do it?

1

- 無差不多心態
- 樹立自我品牌
- 執行到位價值

2

用力做完

- 純粹被動執行
- 說一動做一動
- 有問題慢回報
- 99.9%過場了事

升遷看志業（喜樂心）

試用看態度（軟實力）

面試看專業（硬實力）

(來源：https://www.gvm.com.tw/article/106648)

鄰家草分外青的職業迷失

The Grass Is Not Always Greener on the Other Side.

當下工作，努力爭取幸福和滿足感

減少員工流動

(1) 職業道路，熱情投入
(2) 擴充邊界，以終為始

(3) 薪資福利，維持業界水準
(4) 員工流動，帶來維運風險
(5) 初中級人員，至少4或5年

讓錢自動跟著

下份工作的幸福和滿意是海市蜃樓