國泰金控
Cathay Financial Holdings

數位轉型時代之資安思維

林佩靜
2021/5/6

國泰金融集團

國泰世華銀行
Cathay United Bank

國泰人壽
Cathay Life Insurance

國泰創投
Cathay Venture

國泰產險
Cathay Century Insurance

國泰投信
Cathay Securities Investment Trust

國泰金控
Cathay Financial Holdings

國泰綜合證券
Cathay Securities Corporation

- 集團一致性的資安政策及藍圖
- 各子公司設立資安專責單位

組織推動進程

組織 (2018)

- 資安專責組織

防禦 (2019)

- 電腦安全評估
- ……

聯防 (2020)

- 集團資安監控中心 (SOC)
- …..

韌性 (2021 – 2022)

- **建立營運持續**
- **……**

產業遭受入侵期間

公用事業	高科技產業	政府單位	金融業
平均 1719天	平均 773天	平均 755天	平均 391天
最高 3339天	最高 5865天	最高 4150天	最高 1656天

資料來源：趨勢科技

威脅無所不在

遠距工作

遠距工作連線，增加未授權存取以及外部入侵等風險

BEC 詐騙

攻擊者掌握郵件往來內容並進行操控

供應鏈安全

委外廠商恐成為入侵企業的跳板

物聯網(IoT)

IoT廠商眾多且設備重功能輕安全，許多舊設備也已無法修補

雲端安全

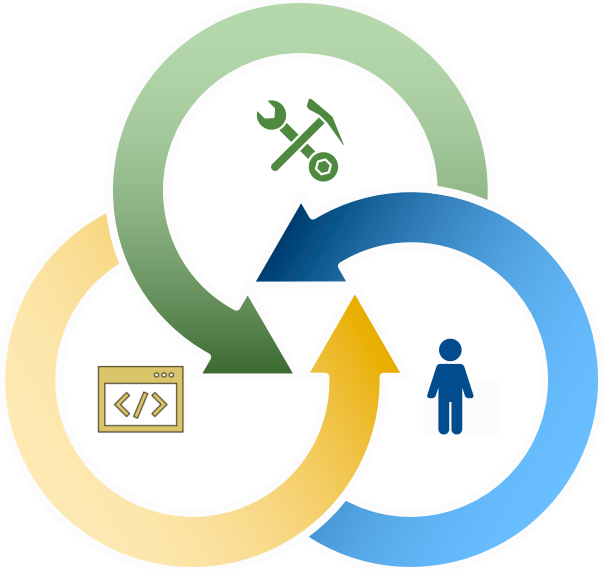
現行地端防護機制無法滿足雲端管控

Goal

- ✓ **不要發生重大**資安事件
- ✓ 發生了，**不可以影響營運**
- ✓ 影響營運，也要**快速恢復**

Strategy

System



Application

People

System

Mindset

Objective

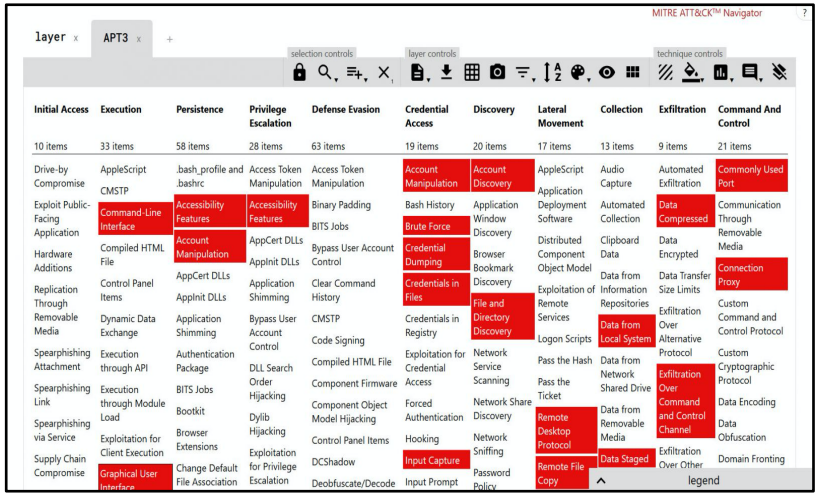
架構 工具 管控

資安框架

✓資安防禦機制基準

✓有一致性的標準可供遵循及管控

ATT&CK®



ISO27001：2013

1. 適用範圍	2. 引用標準	3. 用語及定義
4. 組織全景		
5. 領導作為	6. 規劃	7. 支援	8. 運作
9. 績效評估		10. 改善

A.5資訊安全政策 (2)			
A.6資訊安全之組織 (7)			
A.8資產管理 (10)			
A.7人力資源安全 (6)	A.9存取控制 (14)	A.10密碼學 (2)	A.14系統獲取、開發及維護 (13)
A.11實體及環境安全(15)	A.12運作安全 (14)	A.13通訊安全 (7)	
A.15供應者關係 (5)			
A.16資訊安全事故管理 (7)			
A.17營運持續管理之資訊安全層面 (4)			
A.18遵循性 (8)			

PDCA Process

Security is a process, not a product.

透過檢測及演練
確認完整及有效性

- 電腦系統資訊安全評估
- 紅藍隊攻防演練
- 模擬DDoS攻擊、ATM入侵
- 成熟度評估

集團SOC

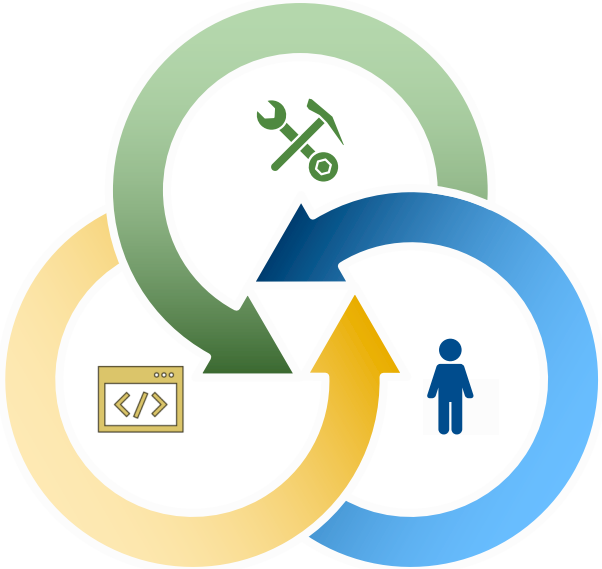
7x24 監控集團資安狀態，掌握資安風險

✓ **2020 年底正式運作**

- 海內外子公司
- 資安及系統設備納入監控
- 上百條監控規則
- 資安儀表板主動預警
- 高中低風險通報
- 每則事件專人回報

Strategy

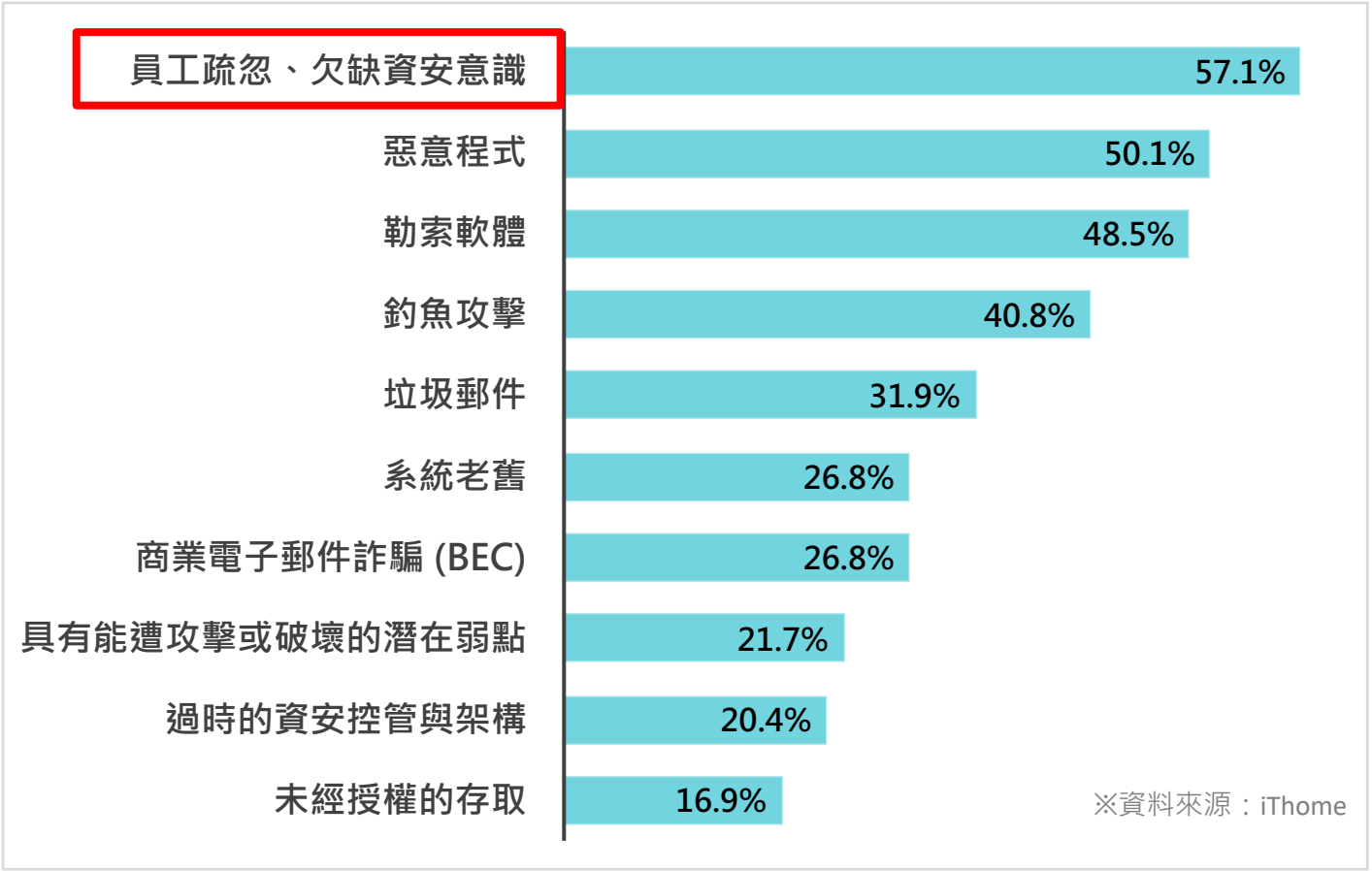
System



Application

People

2020 年台灣企業面臨的十大資安風險



※資料來源：iThome

Mindset

Trust **but** Verify

員工

Zero Trust **and** Verify

非員工

Awareness

常民資安

員工工作式

定義邊界

- 終端設備的安全：WFH 政策，公發筆電
- 人員作業的識別：集團統一帳號
- 資料不落地：VDI
- 內部即時通訊：Cathay TEAM+
- 協同作業平台與檔案交換：Cathay DRIVE

資安投資仍有極限

員工資安意識才是防護關鍵

安全 vs 效率

自律 vs 自由

資安人才

- 設定資安目標、資安策略、可接受風險
- 設立職缺、職涯路徑
- 培育領域專業、鼓勵考證照
- 信任及培養當責團隊

客戶

降低客戶被詐騙機會

- 提供客戶**短網址**
- 透過 **APP推播**

防堵錯的人拿對的鑰匙開鎖

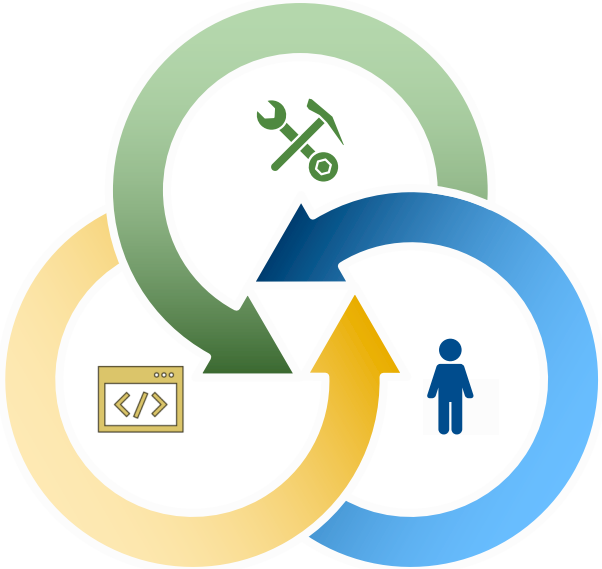
- 導入**多因子認證**
- 建立**安全性提問**
- 重要交易強制採用**生物辨識**

減少客戶損害

- 解除綁定裝置時**通知客戶**
- 異常交易分析機制

Strategy

System



Application

People

Mindset

Security by Design

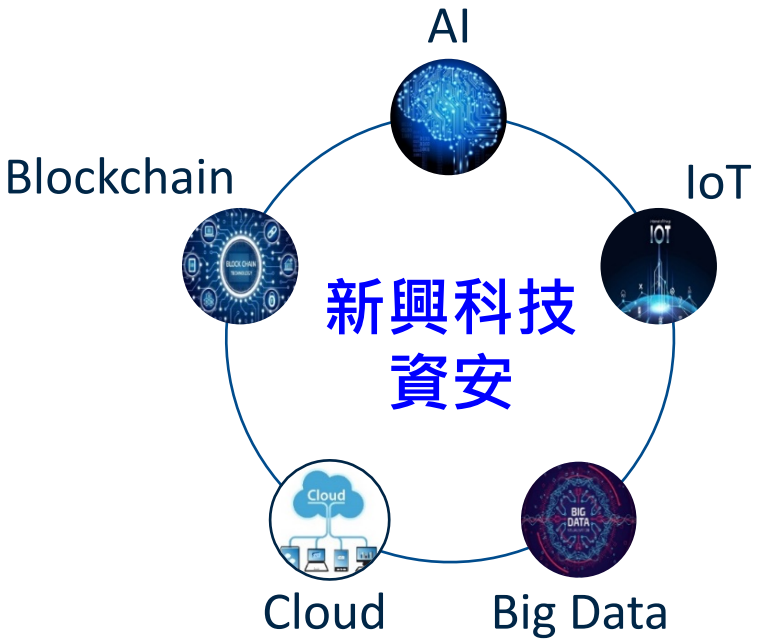
“SHIFT LEFT”，以協助業務推動為思維，來思考

資安要如何設計

高築牆之外

預防勝於治療

數位轉型



- ✓ **軟體開發標準**
  開發初期就要把安全考量進去
- ✓ **軟體 vs 服務模式 vs 商業模式**
- ✓ **資料生命週期**

Application

APP

- APP檢測
- 資料不落地

API

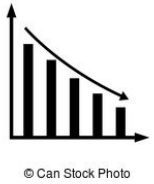
- 傳輸過程加密
- 權限管控

Supplier

- 合作對象
- 開發標準規範

Cloud

- 客戶資料不上雲端
- 雲端控管標準



Data

- 資料安全分級
- 資料使用

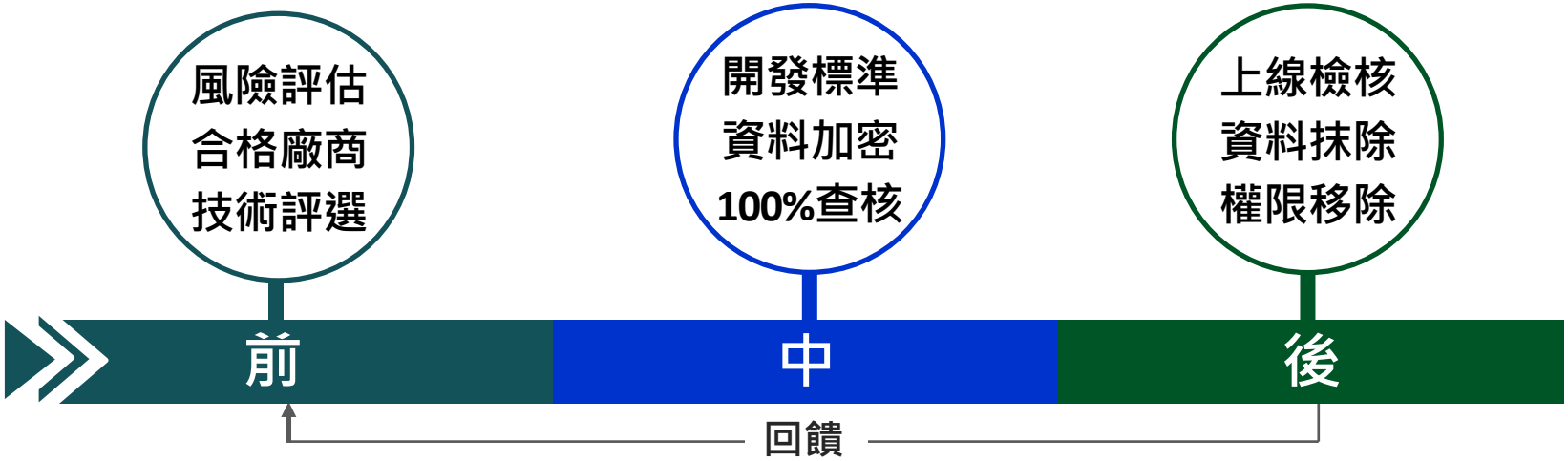
Open Source

- 最新版本
- Kernel安全來源

規範　檢測　查核

Supplier

產業生態圈成員共同建立防衛力



IoT

多功能事務機
(6%)

網路電話機
(60%)

數位錄影機
(23%)

影印機
(4%)

5G

其他
(4%)

電子白板
(1%)

電話交換機
(1%)

錄音設備
(1%)

Cloud

存取控制
Access Control

✓ 防止未經授權的使用者、裝置及應用程式存取雲端環境

金鑰管理
Key Management

✓ 確保雲端環境中資料的機密性與完整性

組態管理
Configuration management

✓ 妥適的組態設定能更有效的強化管理並增加雲端環境的安全性

持續監控
Continuous Monitoring

✓ 透過雲端各種監控機制，完整掌握基礎架構及應用程式的效能、可用性和運作狀態

Tips

- ✓ **策略思維**
  比買硬體工具重要
  風險降低 vs 業務促進
- ✓ **動態管理**
  用攻擊者角度思考風險
  不知不覺 vs 後知後覺 vs 先知先覺
- ✓ **產業聯防**
  遠端工作 網網相連 邊界定義

國泰金控
Cathay Financial Holdings

Thanks