

**CYBERSEC 2025**

臺灣資安大會



國泰金控

Cathay Financial Holdings

# 金融資安韌性：實踐與挑戰

國泰金控 資安長 陳明環

2025.4.17

# Agenda

01

何謂金融資安韌性

韌性 / 威脅現狀

02

安全框架

N I S T / 待強化

03

國泰強化策略

零信任 / AI / 雲端 / 供應鏈

04

挑戰與優化

資料分級 / 防詐 / 監控 / 軟體安全

# 何謂資安韌性

## 攻不進來、服務中斷很快恢復

NIST美國國家標準技術研究所

### 應具備主動防禦和恢復能力



NIST Special Publication (SP) 800-160, Volume 2

金融監督管理委員會

### 安全便利不中斷的金融服務



金融資安行動方案

### 銀行公會

為確保金融機構核心資通系統因意外事故、人為破壞或重大設備故障等而出現服務中斷時，能有效執行應變措施，將損害降低至可承受範圍。

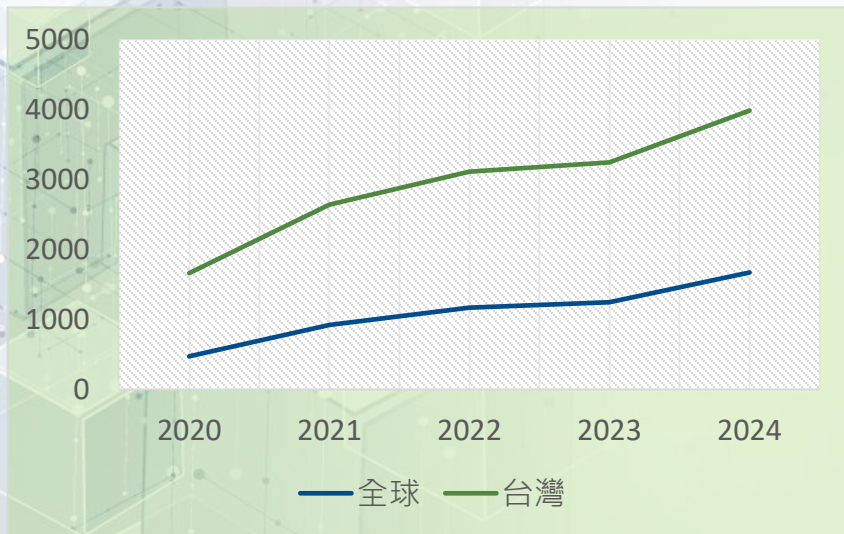
金融機構資訊作業韌性規範



國泰金控

Cathay Financial Holdings

# 面臨的威脅持續上升



※資料來源：Check Point Research統計(平均每周網路攻擊次數)

## 近年常見資安威脅



DDOS



惡意入侵



勒索軟體



供應鏈資安



國泰金控

Cathay Financial Holdings

# 從NIST CSF看資安韌性



## 執行演練

找出弱點、深化防禦

## 迅速復原

確保業務能從攻擊中恢復，  
並提升系統韌性

## 即時應變

快速應對安全事件，  
減少損害並控制風險

辨識  
(IDENTIFY)

## 戰場在哪？

確定資產、風險與業務環境，  
建立有效的安全策略

保護  
(PROTECT)

## 建造城牆

實施安全措施，  
如存取控制與數據保護，  
以防止攻擊影響

治理

領導階層重視及推動、  
安全管理符合業務目標與法規要求

回應  
(RESPOND)

偵測  
(DETECT)

## 全面監控

持續監測與分析異常活動，  
及早發現潛在威脅

復原  
(RECOVER)



國泰金控

Cathay Financial Holdings

※ NIST CSF : NIST Cybersecurity Framework 網路安全框架

## 2024 掌握現況

1. 符合主管機關期待  
對標「金融業導入零信任架構參考指引」，釐清與現況的差距
2. 對標美國CISA框架  
參考美國框架建立集團零信任成熟度評估方法論
3. 產出共通性強化項目  
與第三方顧問共同合作，產出集團共通性強化項目

## 2025-2027 強化規劃

1. 三年強化計畫  
依據2024年評估結果，各公司依其業務需求、資源配置進行三年計畫，確保各公司自行評估項目依序達標
2. 整合集團資源  
對於集團**共通性強化項目**，藉由項目分工，發揮集團綜效，共同評估機制有效性，確保效益最大化

## 目標

主要風險項目  
達到「進階」等級

# AI資安治理

## 整體治理架構



## 資安關注焦點

- 1 資料安全性與隱私保護
- 2 模型與系統安全
- 3 存取與權限管理
- 4 治理架構與政策制定
- 5 透明性與可解釋性
- 6 合規與標準對齊

# 雲端資安治理

雲端治理規劃

兼顧法規及實務面

應用系統上雲

整合實作案例及參考業界經驗

雲端資安防護

搭建安全的資安架構

IAM權限控管、資料加密、機敏資料保護、端到端的安全防護

雲端技術架構

從資安面考量整體基礎設施及維運開發框架

雲端人才培育

多元化培訓計畫，強化團隊雲實力

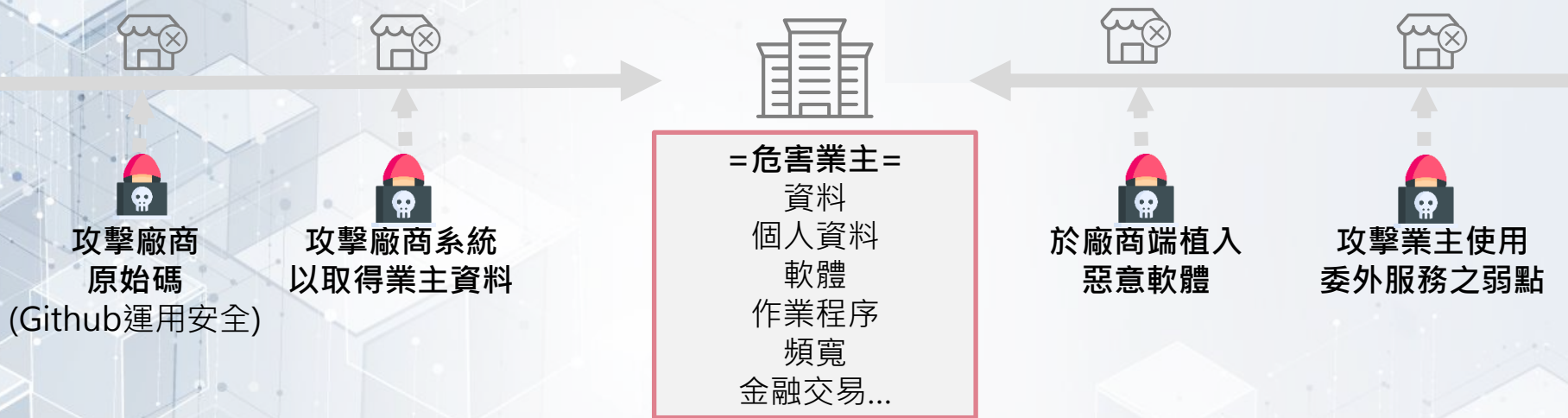


五大策略



# 供應鏈管理(委外)

綜觀近期資安事件，供應鏈資安攻擊近年大幅提升，攻擊樣態如下：



因應委外廠商、軟硬體供應商為跳板攻擊的案例逐漸增多，供應鏈恐成企業資安破口  
以「合規面」、「國際標準」、「風險面」考量，

推動資訊供應商管理機制強化專案，規劃委外前中後整體資安機制

應對新興威脅，基本功才是關鍵



威脅瞬息萬變，應  
建立完善的資安運作制度  
確保業務的持續和安全



01

### 應變與災難復原

沒有攻不破的牆，除了持續加強防禦能力  
也要強化應變與災難復原

### 執行演練

持續演練，發掘可能漏洞與威脅  
強化防禦機制

02

03

### 強化監控

定期梳理監控結果、更新監控原則及閾值  
精準回應告警

### 資安人才培育

因應外部威脅趨勢及內部流程更新  
進行員工培訓，提升員工的認知與能力

04

# Thank you for listening



國泰金控

Cathay Financial Holdings