證券商資通安全的挑戰與因應

臺灣證券交易所 券商輔導部

2019年10月24日

簡報大綱

- 強敵壓境－新科技的挑戰
- 運籌帷幄－提升資安防護能力
- 眾志成城－強化資安韌性

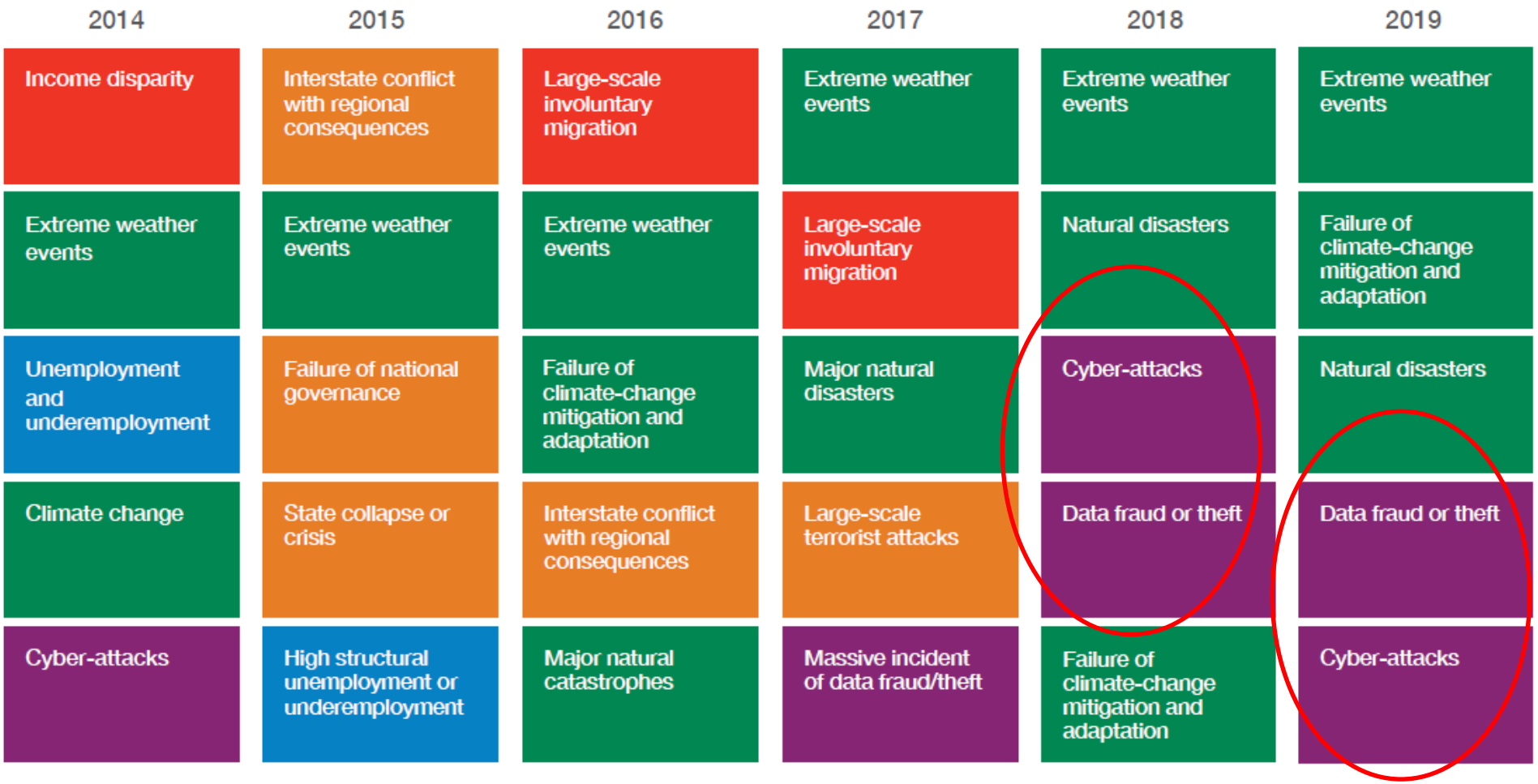
科技帶來的議題—資訊安全

世界經濟論壇(WEF)全球風險趨勢關聯圖

- 資料詐欺或竊盜 ❹
- 網路攻擊 ❺
- 關鍵資訊基礎設施崩潰
- 科技進步的負面效應

資料來源：The Global Risks Report 2019 (14th Edition)

2014-2019 全球風險因素排名前五名



資料來源：The Global Risks Report 2019 (14th Edition)

近年來台灣金融業遭受網路攻擊事件頻傳

2016.07

- 第一銀行遭駭客盜領8,300萬元

2016.09

- 第一金證券及第一銀行通報遭受DDoS攻擊

2017.02

- 臺灣證券商遭受勒索及大規模DDoS攻擊，多家業者受害

2017.10

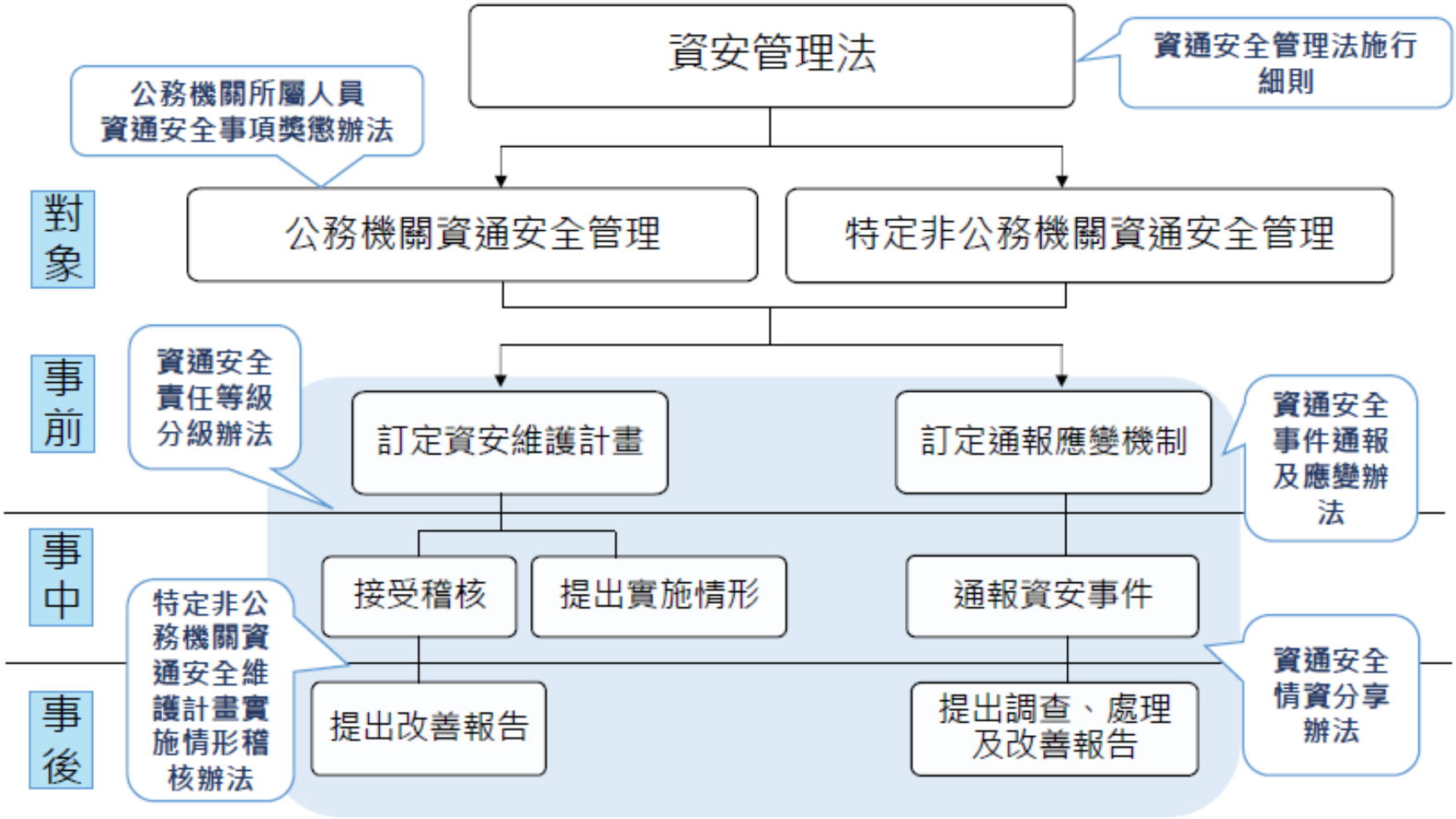
- 遠東銀行遭駭，遭駭客利用SWIFT轉帳約18億台幣

簡報大綱

- 強敵壓境－新科技的挑戰
- 運籌帷幄－提升資安防護能力
- 眾志成城－強化資安韌性

資安即國安 (2016國家戰略目標)

- **資通安全管理法已於2019年元旦實施**



資料來源：行政院資通處

強化證券期貨市場資安防護能力

- 證券期貨業採行之資安防護強化措施：

市場緊急事件應變

- 資安通報系統
- 金融資安資訊分享與分析中心

強化業者體質

- 強化證券期貨業者DDoS防護水準
- 配置資訊專責人力
- 擴大查核資安深度及廣度
- **研提證券期貨業者資通安全防護標準**

證券期貨市場
資通安全事件通報系統

- 訂定證券業者資安通報規範，並建置通報系統，以及時掌握資安事件

初步通報

知悉事件30分鐘內

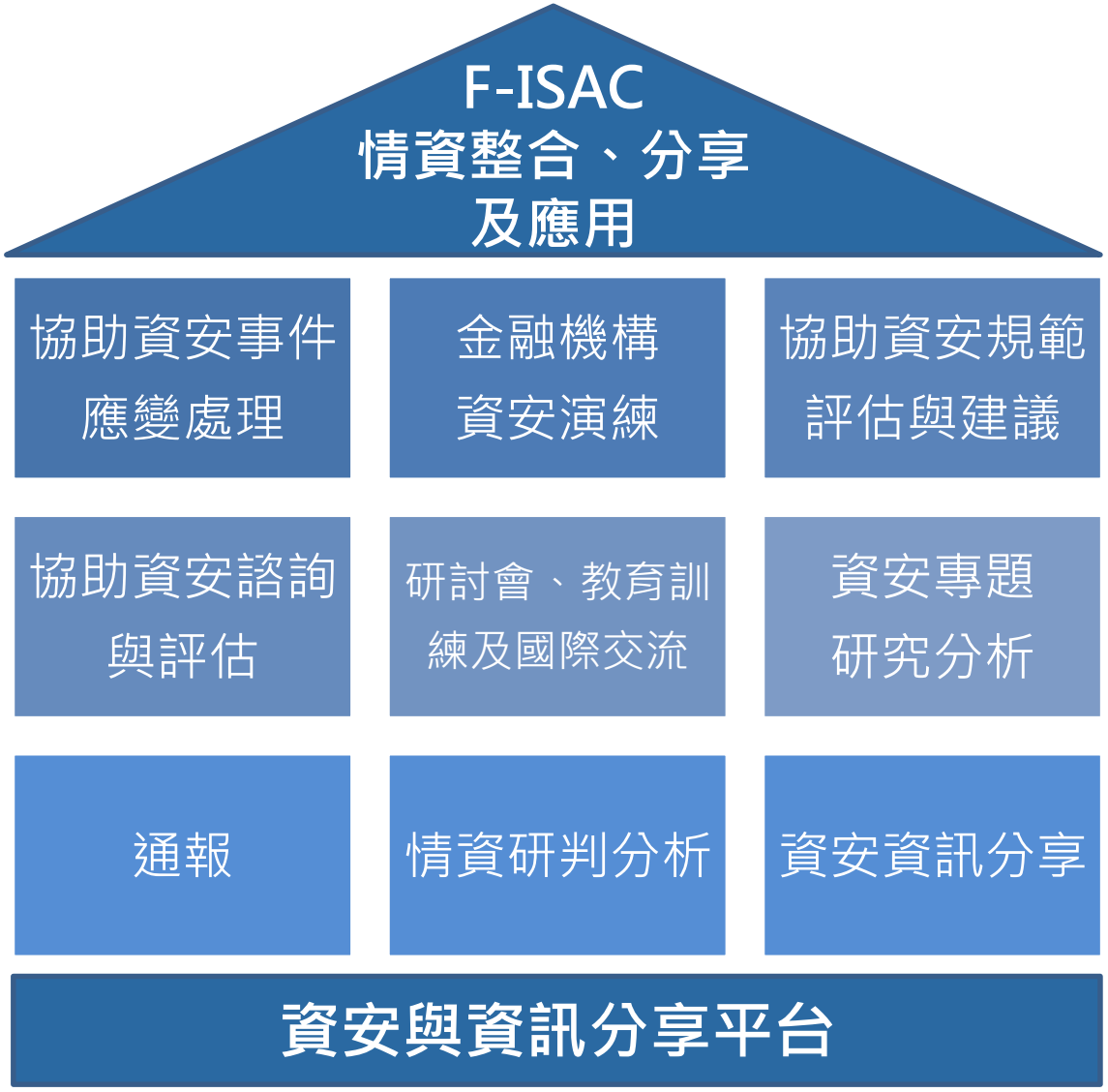
正式通報

查明事件後儘速辦理

解除通報

事件處理完成後

金融資安資訊分享與分析中心



2016 成立證券期貨市場資安資訊中心(SF-ISAC)

2017 成立金融資安資訊分享與分析中心(F-ISAC)

規劃建置金融網路危機處理中心(F-CERT)

- 政府聯手金融業者建構金融資安聯防體系

擴大查核資安深度及廣度(1)

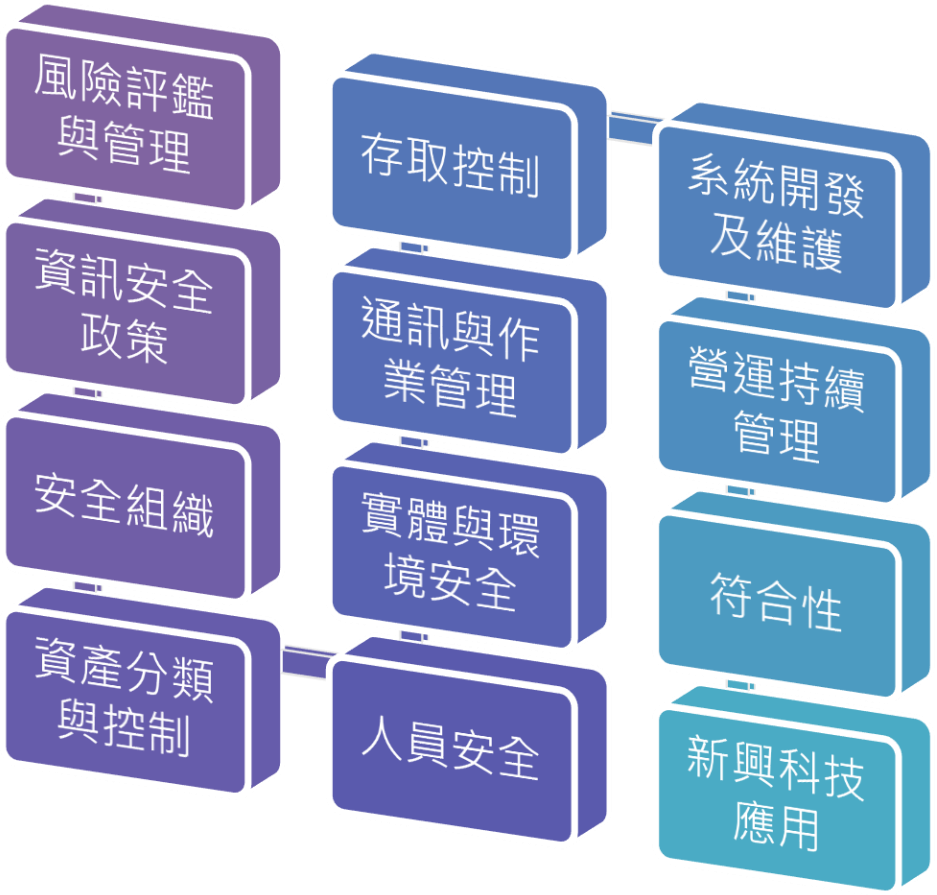
- 證券期貨各服務事業應設置資訊安全專責單位及主管，負責資安制度之規劃、監控及執行。
- 針對不同規模設置資訊安全專責單位及主管，以進行差異化管理

分級標準	資安單位暨人力編制
資本額200億以上	應設資安專責單位，資安主管及至少2名資安人員(參照一般銀行)
資本額100億以上，未達200億	資安主管及至少2名資安人員
資本額40億以上，未達100億	資安主管及至少1名資安人員
資本額未達40億	至少1名資安人員

擴大查核資安深度及廣度(1)

持續輔導證券商落實執行「建立證券商資通安全檢查機制」

- 每年由證交所對證券商進行資安外部稽核
- 參考近期證券業重大資安事件，訂定年度資通安全重要查核項目



擴大查核資安深度及廣度(2)

- 查核作業採差異化分級管理
- 持續輔導，強化業者資安防護能力

分級標準	查核重點
資本額未達40億	建立證券商資通安全檢查機制
資本額40億以上，未達100億	1. 建立證券商資通安全檢查機制 2. 社交工程、網路釣魚、個資去識別化等
資本額100億以上	1. 建立證券商資通安全檢查機制 2. 社交工程、網路釣魚、個資去識別化等 3. 滲透測試、資安健診、資安監控中心等

資安防護、人人有責

駭客攻擊方式改變

目標攻擊
公司網站、系統

埋伏攻擊
社交工程、社群網站

強化資安教育
提升資安防護能力

新興科技影響

業務模式改變
線上開戶

法令遵循風險
防制洗錢、打擊資恐

落實對客戶KYC

業務防線

遭遇資安事故
DDoS 攻擊

線上業務停擺
電子式交易系統故障

人工接單
降低營運衝擊

強化資安危機意識、提升資安防護能力

資安危機就在身旁

社交工程

變臉詐騙攻擊

勒索軟體

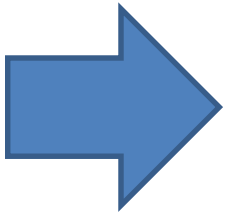
社交工程

社交工程 (Social Engineering)

- 係利用人性弱點以影響力或說服力來進行詐騙，是一種非全面技術性的資訊安全攻擊方式，藉由人際關係的互動，來突破資安防護，遂行其非法存取、破壞行為，以獲取帳號、密碼或其他機敏性資料。

➢社交工程手法

- 電子郵件
- 釣魚網站
- 社群網站
- 即時通訊



➢防範方法

- 不下載不明檔案及非法軟體
- 不瀏覽及登入未經確認的網站
- 不開啟來路不明的電子郵件及附加檔案
- 應確認後始提供資料

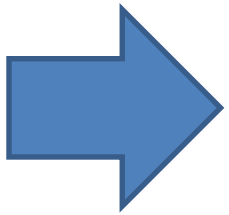
變臉詐騙攻擊

變臉詐騙攻擊(Business Email Compromise)

- 為駭客竄改企業間往來的郵件內容，誤導企業轉帳至詐騙帳號，是近年來常見的駭客攻擊手法之一。

➢變臉詐騙手法

- 假造寄件者地址
- 利用相似的網域名稱



➢防範方法

- 不直接回覆
- 電話確認
- 設定交易控管機制

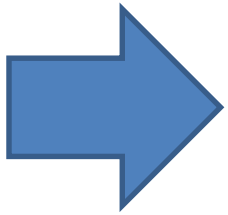
勒索軟體

勒索攻擊

- 勒索軟體是一種讓受害者不能夠存取他們電腦的惡意軟體。它的目的是要威脅受害者付出贖金來讓系統或資料復原。

➢勒索攻擊手法

- 釣魚信件



➢防範方法

- 不點擊不明電子郵件提供網址或夾帶附件
- 不點擊不明網路廣告
- 勤備份
- 勤更新防毒等防護程式

簡報大綱

- 強敵壓境－新科技的挑戰
- 運籌帷幄－提升資安防護能力
- 眾志成城－強化資安韌性

眾志成城

強化資安韌性

由上而下

由下而上

THE END

謝謝您的聆聽

臺灣證券交易所