

提升證券商資通安全說明

證交所
劉保鈞專員
112年11月2日

一、證券商資安治理架構

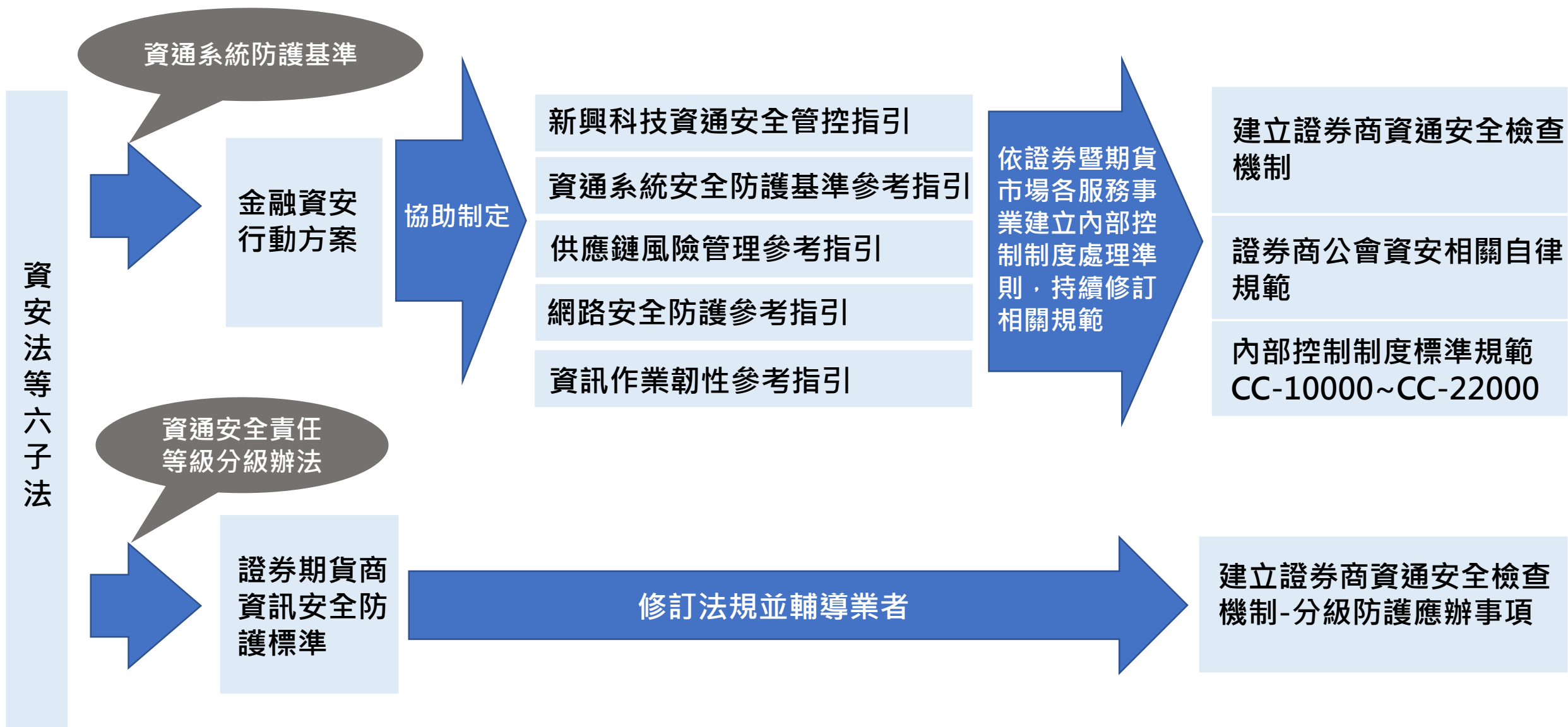
二、證券商資安防護藍圖

三、近期資安案例分享

四、重要事項宣導

五、未來資安治理策略

一、證券商資安治理架構



二、證券商資安防護藍圖

主動式防禦推動策略



網路攻擊狙殺鏈(Cyber Kill Chain)

偵查 (Reconnaissance)	武裝 (Weaponization)	遞送 (Delivery)	攻擊 (Exploitation)	安裝 (Installation)	發令與控制 (Command and Control)	採取行動 (Actions on Objectives)
研究、識別及選擇目標，可以在網際網路上搜尋相關資訊，或是利用工具掃描或探測目標環境。	針對特定的安全漏洞，設計遠端存取木馬程式，包裹在可選送的資料中，多數以自動化工具產生，且利用常見資料檔案進行偽裝。	設法將惡意程式傳送到目標環境，如電子郵件附件、網站及可移動的USB 碟等遞送管道。	惡意程式遞送到目標主機後，將觸發內部的程式碼，以應用程式或作業系統的安全弱點為目標，開始進行攻擊。	於受駭主機安裝遠端存取的木馬或後門程式，而攻擊者可繼續隱藏於受駭環境中。	受駭主機須向外連結網際網路上的控制伺服器，以建立控制通道，攻擊者便可利用此通道遠端操控受駭主機。	攻擊者開始採取行動，如竊取資料、破壞資料的完整性與可用性，或是做為入侵其他系統的跳板。



縱深防禦



資料來源：NCCST

撞庫事件

事件說明

證券商遭受撞庫攻擊(國內外均有)，惟網頁下單部分已導入多因子驗證，網路攻擊之撞庫未果，但造成部分客戶帳號因密碼錯誤過多遭到鎖定。

處理措施

- 該公司暫時停止網路下單服務
- 調整資安設備防護規則

改善預防措施

- 調整登入之檢核機制，初步檢核客戶所帶憑證之有效性
- 分析單一IP於固定時間區間之登入頻率

駭客滲透攻擊

事件說明

證券商之委外廠商遭駭客滲透攻擊，致該委外廠商所提供之系統亦遭攻擊，且同網段之其它主機亦遭嘗試登入。

處理措施

- 停止相關主機之運作
- 委請外部資安單位協助檢視

改善預防措施

- 落實網段分割
- 強化異常監控及避免使用預設帳號、密碼
- 委外廠商維運經覆核後始得建立連線

委外管理失當

事件說明

委外廠商進行維護作業，誤使用營運環境系統進行測試交易。

處理措施

- 恢復正常狀態
- 停止相關帳號使用

改善預防措施

- 管控高權限帳號之使用
- 正式系統與測試系統應分割
- 委外廠商之維運作業應俟業者同意後始得建立連線

交易系統異常

事件說明

近期成交量大，客戶線上交易需求量增加，致系統無法負荷，造成服務中斷，影響客戶權益。

處理措施

- 調整系統資源參數
- 引導客戶使用其它下單管道

改善預防措施

- 定期進行系統優化
- 加強故障復原作業及持續營運演練
- 辦理全量(前中後台)壓力測試

疑似暗網事件

事件說明

有暗網指稱握有某業者客戶資料，並在暗網進行兜售。

處理措施

- 請第三方公正單位進行鑑識
- 委請會計師事務所進行個資查核，並出具確信報告

改善預防措施

- 管控高權限帳號之使用
- 內部系統不應透過網際網路提供服務
- 建置資料外洩防護機制

加重事件處置措施

強化經理人問責制度

- 重大資安缺失對**經理人**予以警告或暫停1~6個月之處置
- 視需要請**經理人**與**資安長**至本公司訪談

提高違約金上限額度

- 由**100萬元**提高為**200萬元**
- 最近半年內再次發生違規，上限由**200萬元**提高為**400萬元**

四、重要事項宣導

落實資安通報

初步通報

知悉事件30
分鐘內辦理

取消通報

釐清事件
確認誤報

正式通報

於查明事件
後儘速辦理

解除通報

事件處理
完成後

資安事件通報，於**初步通報**後，**24小時**內完成正式通報。

如資安事件符合特定態樣，依「證券商通報大資安事件之範圍申報程序及其他應遵循事項」辦理。

強化持續營運

- 證券商如發生當機致無法下單時，應向投資人公告替代下單方式，並協助投資人妥適處理下單問題，避免發生糾紛。
- 落實備援演練，降低營運中斷風險

證交所精進管理

優化查核品質

- 配合調整查核工作底稿
- 運用監理科技聚焦重要議題，進行精準查核
- 加強查核人員教育訓練

掌握市場脈動

- 資安通報事件之後續追蹤控管
- 蒐集證券商資安輿情、新聞資訊

新興議題善用 專家職能

- 研議證券商治理成熟度相關法規
- 研析證券商與銀行業資安法規比較
- 研析AI新興科技運用之法規修訂

精實資安防護韌性

精實 資安治理

- 發生重大資安缺失證券商所提改善計畫，視需要委託**第三方驗證機構**出具驗證報告
- 改善計畫及驗證報告提報**董事會**，函報**本公司**並副知**主管機關**

提升 資安聯防能力

- 透過**SF-CERT**提供資料，達到**資安聯防**
- 充足**備援量能**
- 落實**壓力測試**
- 完備**監控預警**

強化 查核及輔導

- **即時查核**
發生**嚴重系統異常**、**重大資安攻擊事件**等
- **年度查核**
頻繁通報資安事件、**資安缺失較多**

持續辦理資安專案

資安總體檢

- 持續辦理證券商資安**總體檢**作業

資安治理成熟度

- 協助及鼓勵證券商辦理**資安治理成熟度自評**作業

作業委託他人

- 研訂「證券商作業委託他人處理應注意事項」申報格式及申報資料方式
- 施行緩衝期**1年內**，輔導完成委外作業調整

可容忍中斷時間

- 依市占率**規模分級**，研訂各級證券商核心系統可容忍中斷時間**最低標準**

監理科技應用

- 導入**大數據**分析工具
- 精進差異化管理
- 健全資安防護網

簡報結束
敬請指導